Fraud Examiners Manual

2016 International Edition

Select a section below to view its chapters:

SEARCH

ACFE™
Association of Certified Fraud Examiners

Fraud Examiners Manual

2016 International Edition

financial transactions & fraud schemes

ACFE™
Association of Certified Fraud Examiners

Fraud Examiners Manual

2016 International Edition

law

ACFE™
Association of Certified Fraud Examiners

Fraud Examiners Manual

2016 International Edition

investigation

ACFE™
Association of Certified Fraud Examiners

Fraud Examiners Manual

2016 International Edition

fraud prevention & deterrence

ACFE™
Association of Certified Fraud Examiners

ISBN 978-1-889277-56-8

716 West Avenue
Austin, Texas 78701
United States of America
(800) 245-3321/(512) 478-9000
www.ACFE.com

DISCLAIMER

No publication could cover all of the rules and regulations applicable for every country around the globe. The editors of this work have attempted to provide general information about concepts and methods of fraud detection, investigation, and prevention that are commonly used worldwide. Because this publication is a compendium of information from various countries and jurisdictions, the specific laws, rules, regulations, and terminology may (and probably will) vary in your area.

Every effort has been made to ensure that the contents of this publication are accurate and free from error. However, it is possible that errors exist, both typographical and in content. Therefore, the information provided herein should be used only as a guide and not as the only source of reference.

This publication is not intended to be a legal or accounting reference, and nothing contained herein is to be considered as the rendering of legal or accounting advice for specific subjects or areas. Readers are responsible for obtaining such advice from legal or accounting professionals in their jurisdictions. This publication and any forms or samples within are intended for educational and informational purposes only.

Descriptions of products, software programs, organizations, service organizations, etc., are provided as a convenience to the reader. Readers are advised to obtain further information from the provider of the product or service before purchasing.

The author, advisors, and publishers shall have neither liability nor responsibility to any person or entity with respect to any loss, damage, or injury caused or alleged to be caused directly or indirectly by any information contained in or omitted from this publication.

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

TABLE OF CONTENTS

VOLUME I

SECTION 1
FINANCIAL TRANSACTIONS AND FRAUD SCHEMES

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

FINANCIAL TRANSACTIONS AND FRAUD SCHEMES

ASSET MISAPPROPRIATION: INVENTORY AND OTHER ASSETS

BRIBERY AND CORRUPTION

THEFT OF INTELLECTUAL PROPERTY

FINANCIAL INSTITUTION FRAUD

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

FINANCIAL TRANSACTIONS AND FRAUD SCHEMES

CHECK AND CREDIT CARD FRAUD

INSURANCE FRAUD

HEALTH CARE FRAUD

CONSUMER FRAUD

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

FINANCIAL TRANSACTIONS AND FRAUD SCHEMES

COMPUTER AND INTERNET FRAUD

CONTRACT AND PROCUREMENT FRAUD

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

SECTION 2
LAW

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

LAW

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

LAW

TESTIFYING

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

VOLUME II

SECTION 3
INVESTIGATION

PLANNING AND CONDUCTING A FRAUD EXAMINATION

ANALYZING DOCUMENTS

INTERVIEW THEORY AND APPLICATION

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

INVESTIGATION

INTERVIEW THEORY AND APPLICATION (CONT.)

INTERVIEWING SUSPECTS AND SIGNED STATEMENTS

COVERT EXAMINATIONS

SOURCES OF INFORMATION

DATA ANALYSIS AND REPORTING TOOLS

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

INVESTIGATION

DATA ANALYSIS AND REPORTING TOOLS (CONT.)

DIGITAL FORENSICS

TRACING ILLICIT TRANSACTIONS

REPORT WRITING

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

INVESTIGATION

MENU

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

SECTION 4
FRAUD PREVENTION AND DETERRENCE

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

FRAUD PREVENTION AND DETERRENCE

FRAUD EXAMINERS MANUAL
(INTERNATIONAL EDITION)

FRAUD PREVENTION AND DETERRENCE

PREFACE

More than two decades ago, the First Edition of the *Fraud Examiners Manual* postulated that "…fraud will be the crime of choice for the 21st century."

The truth of that prophetic prediction has been borne out in the events of the last decade. According to estimates by the Association of Certified Fraud Examiners, global losses from occupational fraud and abuse may exceed $3.5 trillion each year. If we add together the various confidence schemes, check and credit card frauds, and securities swindles, the total may run even higher. Enron, WorldCom, Satyam, Olympus, Bernie Madoff, and the rest of a rogue's gallery—as devastating as these frauds were—are only a microcosm of the problem.

One difficult aspect of fraud and white-collar crime is that it is hidden—we only know about the ones that surface. Whatever the true cost of this problem, it is a staggering social and economic sum. But there is hope.

When the First Edition of the *Fraud Examiners Manual* was released, there were less than a thousand Certified Fraud Examiners. The ACFE now has more than 75,000 members in more than 150 countries. These members bring true hope to understanding and, eventually, controlling the problem of white-collar crime. It will not be easy, nor will it be accomplished quickly.

The *Fraud Examiners Manual* is but one weapon to fight fraud. Like all weapons, it is useless except in the hands of someone trained to use it. You, the individual fraud examiner, are the real key. Study the enclosed information carefully, then add this knowledge to your arsenal. It represents the common body of knowledge in the fraud examination field. But auditors, forensic accountants, attorneys, law enforcement personnel, regulatory examiners, investigators, and other anti-fraud professionals will find much useful information, too.

The ACFE offers two editions of the *Fraud Examiners Manual*—the *International Edition* and the *U.S Edition.* Both editions discuss thousands of fraud schemes and the relevant prevention, detection, and investigation techniques. The primary difference is that the *International Edition* contains a more generalized discussion regarding accounting and legal rules and regulations. Consequently, it will be up to the individual user to seek out additional information or professional advice when needed.

The *Fraud Examiners Manual* is organized into four sections. The first section, Financial Transactions and Fraud Schemes, describes thousands of fraud schemes and the techniques

that can be used to prevent and detect them. This section begins with an overview of basic accounting concepts. It then contains several chapters on occupational fraud schemes (i.e., asset misappropriations, corruption, and fraudulent financial statements), orgainized in a taxonomy originally developed for the book *Occupational Fraud and Abuse* (now *The Corporate Fraud Handbook*). The later part of this section details a number of other fraud schemes ranging from financial institution fraud to health care fraud.

The Investigation Section provides the basic tools and techniques necessary to develop information and evidence when conducting a fraud examination and identifying the perpetrators. It describes how to gather evidence through the examination of documents and through interview techniques. It also contains information about using data analysis techniques, computer forensics, public records, and the Internet to locate evidence and other resources.

The Law Section discusses some of the common legal principles fraud examiners are faced with; the legal nuances involved in examining several specific categories of fraud, such as money laundering and securities fraud; and the legal pitfalls you may encounter in conducting an investigation. It also contains information about how to testify as a witness.

The Fraud Prevention and Deterrence Section reflects a concrete approach to preventing and deterring fraud. It not only discusses why people commit crime, but also contains practicable advice about how to use that knowledge to prevent fraud through proactive policies, formal fraud risk assessment and fraud risk management initiatives, corporate governance practices, and compliance programs. It also includes a number of meaningful statistics about fraud, as well as a discussion of the types and impact of organizational and occupational crime. This section concludes with a discussion of the ACFE Code of Professional Ethics and its meaning for fraud examiners.

We would like to acknowledge the assistance of the following experts in contributing material to this publication: Derek Baldwin, Lesley Baldwin, Paul Barnes, Bob Bauman, Neil Bebbington, Charlotte J. Bell, Thomas Bell, Tasha Bollinger, Dick Brodfuehrer, Chris Campos, Larry Cook, Dave Cotton, Tom Creelman, Don Dame, Bruce Dean, Joe Dervaes, Chris Dorman, Stuart Douglas, Ron Durkin, Dennis Dycus, David Elzinga, Bryan Farrell, John Francolla, Paul French, Sunder Gee, Mason Haynesworth, Jim Healy, Steve Hendrix, Dick Hollinger, Frank Howatt, Bethmara Kessler, Mike Kline, Mike Lawrence, Frank Leggio, Jim Lile, Bob Lindquist, Kathleen Lower, Tony Maceo, Judge Frank Maloney, Walt

PREFACE

Manning, John McLaren, Bob Miller, Frank Nasuti, Dick Nossen, Joan Norvelle, Brett Holloway-Reeves, Ric Rowe, William N. Rudman, Mike Ryman, Ken Sibley, Craig Starr, Bill Thornhill, Don Wall, and John Fisher Weber.

Final thanks go to the staff of the Association of Certified Fraud Examiners. We are especially appreciative of the efforts of John Warren, Andi McNeal, Amy Scott, Mark Scott, Valerie Caldwell, Jacob Parks, Zach Capers, Misty Carter, Ron Cresswell, Laura Hymes, Yasmin Vazquez, Mark Blangger, Jennifer Liebman, and Jeanette LeVie.

The following pages will provide you with detailed references. But remember, no procedure can replace good judgment. The detection and deterrence of fraud is difficult. But if you learn the information in this book, your task will be immeasurably easier.

Authors:
Joseph T. Wells, CFE, CPA
Nancy S. Bradford, CFE, CPA, CIA
Gilbert Geis, Ph.D.
John D. Gill, J.D., CFE
W. Michael Kramer, J.D., CFE
James D. Ratley, CFE
Jack Robertson, Ph.D., CFE, CPA

Austin, Texas
February 2016

MENU

TABLE OF CONTENTS

MENU

FINANCIAL STATEMENT FRAUD (CONT.)

ASSET MISAPPROPRIATION: CASH RECEIPTS

MENU

ASSET MISAPPROPRIATION: FRAUDULENT DISBURSEMENTS

BRIBERY AND CORRUPTION

MENU

THEFT OF INTELLECTUAL PROPERTY (CONT.)

THEFT OF INTELLECTUAL PROPERTY (CONT.)

FINANCIAL INSTITUTION FRAUD

MENU

FINANCIAL INSTITUTION FRAUD (CONT.)

MENU

FINANCIAL INSTITUTION FRAUD (CONT.)

MENU

FINANCIAL INSTITUTION FRAUD (CONT.)

CHECK AND CREDIT CARD FRAUD

CHECK AND CREDIT CARD FRAUD (CONT.)

INSURANCE FRAUD

MENU

INSURANCE FRAUD (CONT.)

INSURANCE FRAUD (CONT.)

HEALTH CARE FRAUD

MENU

HEALTH CARE FRAUD (CONT.)

MENU

HEALTH CARE FRAUD (CONT.)

CONSUMER FRAUD

CONSUMER FRAUD (CONT.)

MENU

CONSUMER FRAUD (CONT.)

CONSUMER FRAUD (CONT.)

COMPUTER AND INTERNET FRAUD

MENU

COMPUTER AND INTERNET FRAUD (CONT.)

MENU

COMPUTER AND INTERNET FRAUD (CONT.)

CONTRACT AND PROCUREMENT FRAUD

MENU

CONTRACT AND PROCUREMENT FRAUD (CONT.)

CONTRACT AND PROCUREMENT FRAUD (CONT.)

The material in the Financial Transactions section is divided into three principal topic areas. First, general accounting concepts are illustrated, including the basics of debits and credits, as well as the contents of financial statements. Second, employee defalcation schemes are detailed. This section includes discussion on fraudulent financial statement schemes, asset misappropriation schemes, and bribery and corruption. Finally, other fraud schemes, primarily external frauds, ranging from securities violations to health care frauds, are covered and explained.

ACCOUNTING CONCEPTS

Fraudulent acts are usually of a financial nature. The fraud examiner must therefore understand the essential nature of financial transactions and how they affect records. Additionally, the fraud examiner should have a grasp of both financial terminology and accounting theory.

Accounting Basics

Accounting can be defined as the identification, accumulation, measurement, and communication of economic data about an enterprise for decision makers and other interested parties. The measurement and recording of this data are accomplished through keeping a balance of the accounting equation. The accounting model or accounting equation, as shown below, is the basis for all double-entry accounting:

Assets = Liabilities + Owners' Equity

By definition, *assets* consist of the net resources owned by an entity. Examples of assets include cash, receivables, inventory, property, and equipment, as well as intangible items of value such as patents, licenses, and trademarks. To qualify as an asset, an item must (1) be owned by the entity and (2) provide future benefit.

Liabilities are the obligations of an entity or outsider's claims against a company's assets. Liabilities usually arise from the acquisition of assets or the incurrence of operational expenses. Examples of liabilities include accounts payable, notes payable, interest payable, and long-term debt.

Owners' equity represents the investment of a company's owners plus accumulated profits (revenues less expenses). Owners' equity is equal to assets minus liabilities.

This equation has been the cornerstone of accounting since Luca Pacioli developed it in 1494. Balance is the key of this equation. If a company borrows from a bank, cash (an asset) and notes payable (a liability) increase to show the receipt of cash and an obligation owed by the company. Since both assets and liabilities increase by the same amount, the equation stays in balance.

Accounts and the Accounting Cycle

The major components of the accounting equation consist of numerous detail accounts. An account is nothing more than a specific accounting record that provides an efficient way to categorize similar transactions. All transactions are recorded in accounts that are categorized as asset accounts, liability accounts, owners' equity accounts, revenue accounts, and expense accounts. Account format occurs in a number of ways. The simplest, most fundamental format is the use of a large letter *T,* often referred to as a *T account.*

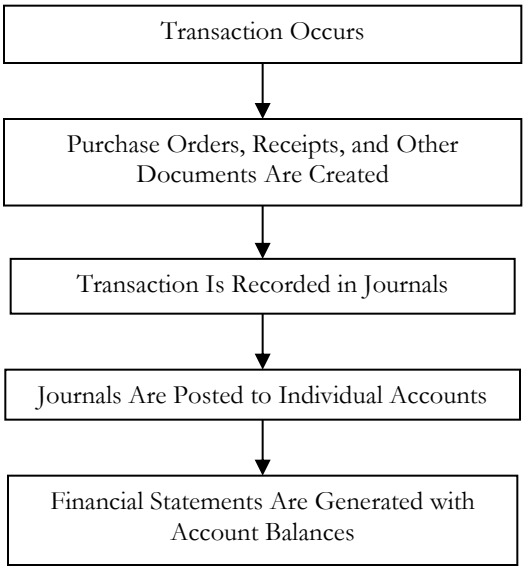
Entries to the left side of an account are *debits* (dr), and entries to the right side of an account are *credits* (cr). Debits increase asset and expense accounts, while credits decrease them. Conversely, credits increase liability, owners' equity, and revenue accounts; debits decrease them. Every transaction recorded in the accounting records has both a debit and a credit, thus the term *double-entry accounting*. The debit side of an entry always equals the credit side so that the accounting equation remains in balance. The accounting equation, in the form of T accounts, looks like the following:

Assets		Liabilities		Owners' Equity
dr | cr	=	dr | cr	+	dr | cr

Fraud investigation often requires an understanding of the debit-and-credit process. For example, a fraud examiner who is investigating the disappearance of $5,000 in cash finds a debit in the legal expense account and a corresponding credit in the cash account for $5,000, but cannot find genuine documentation for the charge. The fraud examiner can then reasonably suspect that a perpetrator might have attempted to conceal the theft by labeling the misappropriated $5,000 as a legal expense.

Discovering concealment efforts through a review of accounting records is one of the easier methods of detecting internal fraud; usually, one needs only to look for weaknesses in the various steps of the accounting cycle. Legitimate transactions leave an audit trail. They start with a source document such as an invoice, check, receipt, or receiving report. These source documents become the basis for journal entries, which are chronological listings of transactions with their debit and credit amounts. Entries are made in various accounting journals. Then, entries are posted to the appropriate general ledger accounts. The summarized account amounts become the basis for a particular period's financial statements.

To help explain how transactions affect the financial statements, this flow of transactional information through the accounting records is illustrated below, followed by examples of typical accounting transactions:



Journal Entries

As transactions occur, they are recorded in a company's books via *journal entries*. Each journal entry serves as a record of a particular transaction and forms an audit trail that can be retraced later to obtain an understanding of a company's operations. Journal entries that are not prompted by a transaction, called *adjusting journal entries*, are also made periodically for items such as depreciation expense and accounts receivable write-offs.

EXAMPLE

XYZ Company completed the following transactions during its first year of operations, 20XX.

Transaction	Analysis	Journal Entry Account	Debit	Credit	Balance Sheet Effect Assets = Liabilities + Owners' Assets	Liabilities	Equity
Enterprise established, Owner invests $192,000	Cash increased Liabilities no effect Equity increased	Cash Common Stock	192,000	192,000	192,000		192,000
Cumulative Balance			192,000	192,000	192,000	-	192,000
Company borrowed $80,000 on a note payable	Cash increased Liabilities increased Equity no effect	Cash Notes Payable	80,000	80,000	80,000	80,000	
Cumulative Balance			272,000	272,000	272,000	80,000	192,000
Purchase business equipment for $70,000	Cash decreased Assets increased Liab & Equity no effect	Equipment Cash	70,000	70,000	70,000 (70,000)		
Cumulative Balance			342,000	342,000	272,000	80,000	192,000
Services rendered to client $40,000, $15,000 collected in advance	Cash increased A/R increased Equity increased	Cash Accounts Receivable Sales Revenue	15,000 25,000	40,000	15,000 25,000		40,000
Cumulative Balance			382,000	382,000	312,000	80,000	232,000
Operating expenses incurred $25,000, 14,000 paid in cash	Cash decreased Liabilities increased Equity decreased	Operating Expenses Cash Accounts Payable	25,000	14,000 11,000	(14,000)	11,000	(25,000)
Cumulative Balance			407,000	407,000	298,000	91,000	207,000
Paid $5,000 on a note payable	Cash decreased Liabilities decreased	Notes Payable Cash	5,000	5,000	(5,000)	(5,000)	
Cumulative Balance			412,000	412,000	293,000	86,000	207,000
Depreciated equipment for 1 yr, estimated life 10yr ($70,000/10) = $7,000	Asset decreased Equity decreased	Depreciation expense Accum. Depreciation	7,000	7,000	(7,000)		(7,000)
Cumulative Balance			419,000	419,000	286,000	86,000	200,000

Accounting Methods

There are two primary methods of accounting: cash-basis and accrual-basis. Cash-basis accounting involves recording revenues and expenses based on when a company pays or receives cash. For example, sales are recorded when a company receives payment for goods, regardless of when the goods are delivered. If a customer purchases goods on credit, the company does not book the sale until the cash is received for the sale. Likewise, if a customer prepays for a sale, the company records the sales revenue immediately rather than when the goods are passed off to the customer. The same holds true with expenses: They are recorded when paid, without consideration to when they are incurred.

Conversely, accrual-basis accounting requires revenues to be recorded when they are earned (generally, when goods are delivered or services are rendered to a customer), without regard

to when cash exchanges hands. Expenses are recorded in the same period as the revenues to which they relate. For example, employee wages are expensed in the period during which the employees provided services, which might not necessarily be the same period in which they were paid.

Under cash accounting, a company may decide to delay paying some expenses so they are not recorded in the current period, resulting in an artificially inflated bottom line. Conversely, accrual accounting requires expenses to be matched to revenues; therefore, it provides a truer picture of a company's financial situation. Generally accepted accounting principles mandate the use of accrual-basis accounting.

Financial Statements

The results of the accounting process are summarized and consolidated reports, or financial statements, that present the financial position and operating results of an entity. It is important to have a basic understanding of how financial statements work because they are often the vehicles through which fraud occurs.

Financial statements are presentations of financial data and accompanying notes prepared in conformity with either generally accepted accounting principles (GAAP)—such as International Financial Reporting Standards (IFRS) or a country's specific accounting standards—or some other comprehensive basis of accounting. The following is a list of typical financial statements:

- Statement of financial position ("balance sheet")
- Statement of profit or loss and other comprehensive income for the period ("income statement")
- Statement of changes in owners' equity or statement of retained earnings
- Statement of cash flows

Financial statements might also include other financial data presentations, such as:

- Statement of assets and liabilities that does not include owners' equity accounts
- Statement of revenue and expenses
- Summary of operations
- Statement of operations by product lines
- Statement of cash receipts and disbursements
- Prospective financial information (forecasts)

- Proxy statements
- Interim financial information (for example, quarterly financial statements)
- Current value financial presentations
- Personal financial statements (current or present value)
- Bankruptcy financial statements

Other comprehensive bases of accounting include:

- Government or regulatory agency accounting
- Tax-basis accounting
- Cash receipts and disbursements, or modified cash receipts and disbursements
- Any other basis with a definite set of criteria applied to all material items, such as the price-level basis of accounting

Consequently, the term *financial statements* includes almost any financial data presentation prepared in accordance with generally accepted accounting principles or another comprehensive basis of accounting. Throughout this section, the term *financial statements* will include the aforementioned forms of reporting financial data, including the accompanying footnotes and management's discussion. For most companies, however, a full set of financial statements comprises a statement of financial position ("balance sheet"), a statement of profit or loss and other comprehensive income ("income statement"), a statement of changes in owners' equity or a statement of retained earnings, and a statement of cash flows, as well as the supplementary notes to the financial statements. Therefore, fraud examiners should be familiar with the purpose and components of each of these financial statements.

Balance Sheet

The *balance sheet,* or *statement of financial position,* shows a "snapshot" of a company's financial situation at a specific point in time, generally the last day of the accounting period. The balance sheet is an expansion of the accounting equation, *assets = liabilities + owners' equity*. That is, it lists a company's assets on one side and its liabilities and owners' equity on the other side. The nature of the accounting equation means that the two sides of the statement should balance.

The following balance sheet, derived from the journal entries in the aforementioned example, shows the financial position of XYZ Company on the last day of its first year of operations.

XYZ Company
Balance Sheet
December 31, 20XX

Assets			**Liabilities**		
Current Assets			Current Liabilities		
Cash	$ 198,000		Accounts Payable	$ 11,000	
Accounts Receivable	25,000		Total Current Liabilities		$ 11,000
Total Current Assets		$ 223,000			
			Long-term Liabilities		
Fixed Assets			Notes Payable	75,000	
Equipment	70,000		Total Long-Term Liabilities		75,000
Less: Accum. Depreciation	(7,000)		Total Liabilities		86,000
Total Fixed Assets		63,000			
			Owners' Equity		
			Common Stock	192,000	
			Retained Earnings	8,000	
			Total Owners' Equity		200,000
Total Assets		$ 286,000	Total Liabilities and Equity		$ 286,000

As mentioned previously, assets are the resources owned by a company. Generally, assets are presented on the balance sheet in order of liquidity, or how soon they are expected to be converted to cash. The first section on the assets side, *current assets*, includes all those assets that are expected to be converted to cash, sold, or used up within one year. This category usually includes cash, accounts receivable (the amount owed to a company by customers for sales on credit), inventory, and prepaid items. Following the current assets are the *long-term assets*, or those assets that will likely not be converted to cash in the near future, such as fixed assets (e.g., land, buildings, equipment) and intangible assets (e.g., patents, trademarks, goodwill). A company's fixed assets are presented net of accumulated depreciation, an amount that represents the cumulative expense taken for wear-and-tear on a company's property. Likewise, intangible assets are presented net of accumulated amortization, an amount that represents the collective expense taken for declines in value of the intangible property.

Liabilities are presented in order of maturity. Like current assets, *current liabilities* are those obligations that are expected to be paid within one year, such as accounts payable (the amount owed to vendors by a company for purchases on credit), accrued expenses (e.g.,

taxes payable or salaries payable), and the portion of long-term debts that will come due within the next year. Those liabilities that are not due for more than a year are listed under the heading *long-term liabilities*. The most common liabilities in this group are bonds, notes, and mortgages payable. The total balance of the note payable is listed under long-term liabilities on XYZ Company's balance sheet, indicating that it does not have to make any payments on the note during the next year. However, if a $5,000 payment was required during the next year, the company would have to reclassify $5,000 of the note balance to the current liabilities section and show the remaining $70,000 as a long-term liability. This adjustment would not change the total amount of the outstanding liability that was shown—all $75,000 would still appear on the balance sheet—but it would allow financial statement users to know that the company had an obligation to pay $5,000 during the next year rather than at some unspecified time in the future.

The owners' equity in a firm generally represents amounts from two sources—owner contributions (usually referred to as *common* or *capital stock* and *paid-in capital*) and undistributed earnings (usually referred to as *retained earnings*). The balance in the capital stock account increases when the owners of a company invest in it through the purchase of company stock. The retained earnings balance increases when a company has earnings and decreases when a company has losses. The retained earnings account is also decreased when earnings are distributed to a company's owners in the form of dividends. XYZ Company's balance sheet shows that the company's owners have contributed $192,000 to the company and that the company has retained $8,000 of earnings as of December 31, 20XX.

Income Statement

Whereas the balance sheet shows a company's financial position at a specific point in time, the *income statement*, or *statement of profit or loss and other comprehensive income,* details how much profit (or loss) a company earned during a period of time, such as a quarter or a year. The accounts reflected on the income statement are temporary; at the end of each fiscal year, they are reduced to a zero balance (closed), with the resulting net income (or loss) added to (or subtracted from) retained earnings on the balance sheet.

The following is the income statement for XYZ Company for its first year of operations based on the sample transactions previously listed.

XYZ Company
Income Statement
For the Year Ended December 31, 20XX

Revenue		
Net Sales	$ 400,000	
Less: Cost of Goods Sold	250,000	
Gross Profit		$ 150,000
Operating Expenses		
Payroll	77,000	
Supplies	4,000	
Utilities	19,000	
Taxes	15,000	
Depreciation	27,000	
Total Operating Expenses		142,000
Net Income		$ 8,000

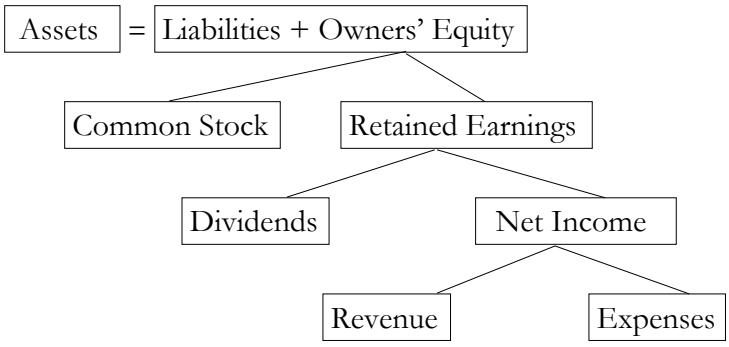
Two basic types of accounts are reported on the income statement—*revenues* and *expenses*. Revenues represent amounts received from the sale of goods or services during the accounting period. Most companies present *net sales* or *net service revenues* as the first line item on the income statement. The term *net* means that the amount shown is the company's total sales minus any sales refunds, returns, discounts, or allowances.

From net sales, an expense titled *cost of goods sold* or *cost of sales* is deducted. Regardless of the industry, this expense denotes the amount a company spent (in past, present, and/or future accounting periods) to produce the goods or services that were sold during the current period. For a company that manufactures goods, cost of goods sold signifies the amount the company spent on materials, labor, and overhead expenses to produce the goods that were sold during the accounting period. For a merchandise reseller, this expense is the amount the company has paid to purchase the goods that were resold during the period. For a service company, the cost of sales is typically the amount of salaries paid to the employees who performed the services that were sold. The difference between net sales and cost of goods sold is called *gross profit* or *gross margin*, which represents the amount left over from sales to pay the company's operating expenses.

Operating expenses are those costs that a company incurs to support and sustain its business operations. Generally, these expenses include items such as advertising, management's salaries, office supplies, repairs and maintenance, rent, utilities, depreciation, interest, and taxes. Accrual accounting requires that these items be included on the income statement in the period in which they are incurred, regardless of when they are paid.

A company's *net income* or *net earnings* for the period is determined after subtracting operating expenses from gross profit. If a company's total expenses were greater than its total revenues and the bottom line is negative, then it had a *net loss* for the period. Commonly, a profitable company will distribute some of its net income to its owners in the form of dividends. Whatever income is not distributed is transferred to the retained earnings account on the balance sheet. In the case of XYZ Company, net income for the year was $8,000. The company did not distribute any of these earnings, so the total amount—$8,000—is shown on the balance sheet as retained earnings. If the company is also profitable during its next year of operations, any net income that is not distributed as dividends will be added to the $8,000 balance in retained earnings. If expenses outperform revenues and XYZ Company shows a loss for its second year, the loss will be deducted from the $8,000 retained earnings balance at the end of the second year.

To summarize, the income statement ties to the balance sheet through the retained earnings account as follows:



Statement of Changes in Owners' Equity

The statement of changes in owners' equity details the changes in the total owners' equity amount listed on the balance sheet. Because it shows how the amounts on the income statement flow through to the balance sheet, it acts as the connecting link between the two statements. The balance of the owners' equity at the beginning of the year is the starting

point for the statement. The transactions that affect owners' equity are listed next and are added together. The result is added to (or subtracted from, if negative) the beginning-of-the-year balance, which provides the end-of-the-year balance for total owners' equity.

The statement of changes in owners' equity for XYZ Company would appear as follows:

XYZ Company
Statement of Changes in Owners' Equity
For the Year Ended December 31, 20XX

Owners' equity, January 1, 20XX		$ -
Investment by owners during the year	$ 192,000	
Net income for the year	8,000	
Increase in owners' equity		200,000
Owners' equity, December 31, 20XX		$ 200,000

XYZ Company completed two types of transactions that affected the owners' equity during 20XX: the $192,000 invested by the company's shareholders, and the revenue and expenses that resulted in the net income of $8,000. Had the company distributed any money to the shareholders in the form of dividends, that amount would be listed on the statement of changes in owners' equity as well. Notice that the $8,000 ties directly to the bottom line of the income statement, and the $200,000 owners' equity ties to the "total owners' equity" amount on the balance sheet.

Some companies present a statement of retained earnings rather than a statement of changes in owners' equity. Similar to the statement of changes in owners' equity, the statement of retained earnings starts with the retained earnings balance at the beginning of the year. All transactions affecting the retained earnings account are then listed and added to the beginning balance to arrive at the ending balance in the retained earnings account. The following is an example of the statement of retained earnings for XYZ Company:

XYZ Company
Statement of Retained Earnings
For the Year Ended December 31, 20XX

Retained earnings, January 1, 20XX		$ -
Net income for the year	$ 8,000	
Increase in owners' equity		8,000
Retained earnings, December 31, 20XX		$ 8,000

Statement of Cash Flows

The statement of cash flows reports a company's sources and uses of cash during the accounting period. This statement is often used by potential investors and other interested parties in tandem with the income statement to determine a company's true financial performance during the period being reported. The nature of accrual accounting allows (and often requires) the income statement to contain many noncash items and subjective estimates that make it difficult to fully and clearly interpret a company's operating results. However, it is much harder to falsify the amount of cash that was received and paid during the year, so the statement of cash flows enhances the financial statements' transparency.

The following is the statement of cash flows for XYZ Company:

XYZ Company
Statement of Cash Flows—Direct Method
For the Year Ended December 31, 20XX

Cash flows from operating activities		
Cash received from customers	$ 15,000	
Cash paid for merchandise	(14,000)	
Net cash flows from operating activities		$ 1,000
Cash flows from investing activities		
Cash paid for purchase of equipment	(70,000)	
Net cash flows from investing activities		(70,000)
Cash flows from financing activities		
Cash received as owners' investment	192,000	
Cash received from issuing note payable	80,000	
Cash paid on note payable	(5,000)	
Net cash flows from financing activities		267,000
Increase in cash		198,000
Cash balance at the beginning of the year		0
Cash balance at the end of the year		$ 198,000

The statement of cash flows is broken down into three sections: cash flows from operating activities, cash flows from investing activities, and cash flows from financing activities.

Cash Flows from Operations

The cash flows from operations section summarizes a company's cash receipts and payments arising from its normal business operations. Cash inflows included in this category commonly consist of payments received from customers for sales, and cash outflows include payments to vendors for merchandise and operating expenses and payments to employees for wages.

This category can also be summarized as those cash transactions that ultimately affect a company's operating income; therefore, it is often considered the most important of the three cash flow categories. If a company continually shows large profits per its income statement, but cannot generate positive cash flows from operations, then questionable

accounting practices might be to blame. On the other hand, net income that is supported by positive and increasing net cash flows from operations generally indicates a strong company.

There are two methods of reporting cash flows from operations. In the previous example, XYZ Company's statement of cash flows is presented using the *direct method*. This method lists the sources of operating cash flows and the uses of operating cash flows, with the difference between them being the net cash flow from operating activities.

In contrast, the *indirect method* reconciles net income per the income statement with net cash flows from operating activities; that is, accrual-basis net income is adjusted for noncash revenues and expenses to arrive at net cash flows from operations. The following is an example of XYZ Company's cash flows from operations using the indirect method:

XYZ Company
Statement of Cash Flows—Indirect Method
For the Year Ended December 31, 20XX

Cash flows from operating activities		
Net income, per income statement		$ 8,000
Add: Depreciation	$ 7,000	
Increase in accounts payable	11,000	18,000
		26,000
Subtract: Increase in accounts receivable	(25,000)	(25,000)
Net cash flows from operating activities		1,000

Note that the net cash flows from operating activities is the same amount—in this case, $1,000—regardless of the method that is used. The indirect method is usually easier to compute and provides a comparison of a company's operating results under the accrual and cash methods of accounting. As a result, most companies choose to use the indirect method, but either method is acceptable.

Cash Flows from Investing Activities

Cash inflows from investing activities usually arise from the sale of fixed assets (e.g., property and equipment), investments (e.g., the stocks and bonds of other companies), or intangible assets (e.g., patents and trademarks). Similarly, cash outflows from investing activities include any cash paid for the purchase of fixed assets, investments, or intangible assets.

Cash Flows from Financing Activities

Cash flows from financing activities involve the cash received or paid in connection with issuing debt and equity securities. Cash inflows in this category occur when a company sells its own stock, issues bonds, or takes out a loan. A company's cash outflows from financing activities include paying cash dividends to shareholders, acquiring shares of its own stock (called treasury stock), and repaying debt.

The total cash flows from all three categories are combined to arrive at the net increase or decrease in cash for the year. This total is then added to or subtracted from the cash balance at the beginning of the year to arrive at the cash balance at the end of the year, which ties back to the amount of cash reported on the balance sheet.

Users of Financial Statements

Financial statement fraud schemes are most often perpetrated by management against potential users of the statements. Financial statement users include company ownership and management, lending organizations, investors, regulatory agencies, vendors, and customers. The production of truthful financial statements plays an important role in an organization's continued success. However, fraudulent statements can be used for a number of reasons. The most common use is to increase an organization's apparent success in the eyes of potential and current investors. (For more information, see the chapter on "Financial Statement Fraud" in this section of the *Fraud Examiners Manual*.)

Generally Accepted Accounting Principles (GAAP)

In preparing financial statements, management, accountants, and auditors are charged with following the relevant standardized financial reporting practices known as *generally accepted accounting principles* (GAAP). GAAP are the rules by which a company's financial transactions are recorded into their appropriate account classifications and properly reported as part of the entity's financial statements.

Historically, each country has promulgated its own GAAP, which has led to a divergence of accounting practices throughout the globe. It has also contributed to some difficulties in comparing the financial performance of companies in different countries, as well as financial reporting challenges for multinational entities. Consequently, accounting standard-setters have been working toward a uniform set of accounting standards in an effort to enhance the transparency and comparability of financial reporting, facilitate cross-border commerce, and

encourage international investment. The resulting International Financial Reporting Standards have been adopted as the source of GAAP for reporting companies in many countries. However, some countries, such as the United States, have retained their own set of accounting standards that form GAAP for reporting companies in those jurisdictions.

International Financial Reporting Standards

The International Financial Reporting Standards (IFRS) Foundation was formed in 2001 with the goal of developing "a single set of high quality, understandable, enforceable, and globally accepted [reporting standards] through its standard-setting body, the International Accounting Standards Board (IASB)." For each accounting function, the IASB looks for the most appropriate principle for how transactions should be accounted for, or the most suitable method of reporting the results.

More than 120 countries permit or require IFRS for domestic reporting, and about 90 of those have fully conformed to IFRS as publicized by the IASB and include a statement acknowledging such conformity in their audit reports.[1]

Qualitative Characteristics of Useful Financial Information

Financial reports provide information about the reporting entity's economic resources, claims against the reporting entity, and the effects of transactions and other events and conditions that change those resources and claims. If financial information is to be useful, it must be relevant and faithfully represent what it purports to represent. The usefulness of financial information is enhanced by the following list of qualitative characteristics of useful financial information that accountants should use when creating financial statements in accordance with IFRS.

RELEVANCE

Any financial information that might affect a decision made by a user of the financial statements is considered relevant. Financial information is relevant if it has predictive value, confirmatory value, or both. *Predictive value* is present if the information can be used as an input to processes employed by users to predict future outcomes. *Confirmatory value* indicates the information provides feedback about previous evaluations.

[1] AICPA IFRS Resources, available at www.ifrs.com.

MATERIALITY

The amount of an item is *material* if its omission or misstatement would affect the judgment of a reasonable person who is relying on the financial statements. Materiality is an entity-specific aspect of relevance based on the nature or magnitude, or both, of the items to which the information relates in the context of an individual entity's financial report.

FAITHFUL REPRESENTATION

Financial information must faithfully represent the economic data of the enterprise that it purports to represent. Every effort shall be made to maximize the qualities of perfectly faithful representation: complete, neutral, and free from error. A *complete* depiction includes all information necessary to understand the data presented. A *neutral* depiction is without bias in the selection or presentation of financial information. *Free from error* means there are no material errors or omissions in the financial reporting data, and the process used to produce the reported information has been selected and applied with no errors.

COMPARABILITY AND CONSISTENCY

Users of financial statements base their decisions on comparisons between different entities and on similar information from a single entity for another reporting period. *Comparability* is the qualitative characteristic that enables users to identify and understand similarities and differences between such items. Information about a company is more useful if it is comparable with similar information about other entities and with similar information about the same entity for another period or another date. Although a single economic occurrence can be faithfully represented in multiple ways, permitting alternative accounting methods for the same economic occurrence diminishes comparability.

Consistency, although related to comparability, is not the same. *Consistency* refers to the use of the same methods for the same items, either from period to period within a reporting entity or in a single period across entities. Comparability is the goal; consistency helps to achieve that goal.

However, both comparability and consistency do not prohibit a change in an accounting principle previously employed. An entity's management is permitted to change an accounting policy only if the change either:

- Is required by a standard or interpretation
- Results in the financial statements providing more reliable and relevant information about the effects of transactions; other events; or conditions on the entity's financial position, financial performance, or cash flows

The entity's financial statements must include full disclosure of any such changes.

VERIFIABILITY

Verifiability helps assure users that information is accurate and faithfully represents the financial position of the entity. Verifiability means that different knowledgeable and independent observers could reach consensus, although not necessarily complete agreement, that a particular depiction is a faithful representation.

TIMELINESS

Timeliness means providing information to decision makers in time to be capable of influencing their decisions. In general, the older information is, the less useful it is.

UNDERSTANDABILITY

Classifying, characterizing, and presenting information clearly and concisely makes it understandable. However, some economic data are fundamentally complex. Therefore, enough information should be provided about such events so that a reasonable financial statement user can understand what took place. An entity's financial statements should include all information necessary for users to make valid decisions and must not mislead them.

GOING CONCERN

A company's management is required to provide disclosures when existing events or conditions indicate that it is more likely than not that the entity might be unable to meet its obligations within a reasonable period of time after the financial statements are issued. There is an assumption that an entity will continue as a going concern; that is, the life of the entity will be long enough to fulfill its financial and legal obligations. Any evidence to the contrary must be reported in the entity's financial statements.

Recognition of the Elements of Financial Statements

Recognition is the process of incorporating an item that meets the definition of an element and satisfies the criteria for recognition into the balance sheet or income statement. It involves the depiction of the item in words and by a monetary amount and the inclusion of that amount in the balance sheet or income statement totals. Items that satisfy the recognition criteria should be recognized in the balance sheet or income statement. The failure to recognize such items is not rectified by disclosure of the accounting policies used nor by notes or explanatory material.

An item that meets the definition of an element should be recognized if:

- It is probable that any future economic benefit associated with the item will flow to or from the entity; and
- The item has a cost or value that can be measured with reliability.

THE PROBABILITY OF FUTURE ECONOMIC BENEFIT

The concept of probability is used in the recognition criteria to refer to the degree of uncertainty that the future economic benefits associated with the item will flow to or from the entity. The concept is in keeping with the uncertainty that characterizes the environment in which an entity operates. Assessments of the degree of uncertainty attaching to the flow of future economic benefits are made on the basis of the evidence available when the financial statements are prepared.

For example, when it is probable that a receivable owed to an entity will be paid, it is then justifiable, in the absence of any evidence to the contrary, to recognize the receivable as an asset. For a large population of receivables, however, some degree of non-payment is normally considered probable; hence an expense representing the expected reduction in economic benefits is recognized. This expense is known as *bad debt expense*, and the corresponding liability is the provision for doubtful debts.

RELIABILITY OF MEASUREMENT

The second criterion for the recognition of an item is that it possesses a cost or value that can be measured with reliability. In many cases, cost or value must be estimated; the use of reasonable estimates is an essential part of the preparation of financial statements and does not undermine their reliability. When, however, a reasonable estimate cannot be made, the item is not recognized in the balance sheet or income statement.

For example, the expected proceeds from a lawsuit might meet the definitions of both an asset and income, as well as the probability criterion for recognition; however, if it is not possible for the claim to be measured reliably, it should not be recognized as an asset or as income; the existence of the claim, however, would be disclosed in the footnotes, explanatory material, or supplementary schedules.

RECOGNITION OF ASSETS

An asset is recognized in the balance sheet when it is probable that the future economic benefits will flow to the entity and the asset has a cost or value that can be measured reliably.

RECOGNITION OF LIABILITIES

A liability is recognized in the balance sheet when it is probable that an outflow of resources embodying economic benefits will result from the settlement of a present obligation and the amount at which the settlement will take place can be measured reliably.

RECOGNITION OF INCOME

Income is recognized in the income statement when an increase in future economic benefit related to an increase in an asset or a decrease of a liability has arisen that can be measured reliably. This means, in effect, that recognition of income occurs simultaneously with the recognition of increases in assets or decreases in liabilities (for example, the net increase in assets arising on a sale of goods or services or the decrease in liabilities arising from the waiver of a debt payable).

In general, revenue is recognized or recorded when it becomes realized or realizable, and earned. According to accrual accounting, revenue should not be recognized for work that is to be performed in subsequent accounting periods, even though the work might currently be under contract. In general, revenue should be recognized in the period in which the work is performed.

The procedures normally adopted in practice for recognizing income, such as the requirement that revenue should be earned, are applications of the recognition criteria previously discussed. Such procedures are generally directed at restricting the recognition as income to those items that can be measured reliably and have a sufficient degree of certainty.

RECOGNITION OF EXPENSES

Expenses are recognized in the income statement when a decrease in future economic benefit related to a decrease in an asset or an increase of a liability has arisen that can be measured reliably. This means, in effect, that recognition of expenses occurs simultaneously with the recognition of an increase in liabilities or a decrease in assets (for example, the accrual of employee entitlements or the depreciation of equipment).

Expenses are recognized in the income statement on the basis of a direct association between the costs incurred and the earning of specific items of income. This process, commonly referred to as the *matching principle*, involves the simultaneous or combined recognition of revenues and expenses that result directly and jointly from the same transactions or other events; for example, the various components of expense making up

the cost of goods sold are recognized at the same time as the income derived from the sale of the goods.

When economic benefits are expected to arise over several accounting periods and the association with income can only be broadly or indirectly determined, expenses are recognized in the income statement on the basis of systematic and rational allocation procedures. This is often necessary in recognizing the expenses associated with using up assets such as property, plant, and equipment; goodwill; and patents and trademarks. In such cases, the expense is referred to as *depreciation* or *amortization*. These allocation procedures are intended to recognize expenses in the accounting periods in which the economic benefits associated with these items are consumed or expire.

An expense is recognized immediately in the income statement when an expenditure produces no future economic benefits or when, and to the extent that, future economic benefits do not qualify, or cease to qualify, for recognition in the balance sheet as an asset.

Measurement of the Elements of Financial Statements

A number of different measurement bases are employed to different degrees and in varying combinations in financial statements. They include the following:

- Historical cost—Assets are recorded at the amount of cash or cash equivalents paid or the fair value of the consideration given to acquire them at the time of their acquisition. Liabilities are recorded at the amount of proceeds received in exchange for the obligation, or in some circumstances (for example, income taxes), at the amounts of cash or cash equivalents expected to be paid to satisfy the liability in the normal course of business.
- Current cost—Assets are carried at the amount of cash or cash equivalents that would have to be paid if the same or an equivalent asset were acquired currently. Liabilities are carried at the undiscounted amount of cash or cash equivalents that would be required to settle the obligation currently.
- Realizable (settlement) value—Assets are carried at the amount of cash or cash equivalents that could currently be obtained by selling the asset in an orderly disposal. Liabilities are carried at their settlement values; that is, the undiscounted amounts of cash or cash equivalents expected to be paid to satisfy the liabilities in the normal course of business.
- Present value—Assets are carried at the present discounted value of the future net cash inflows that the item is expected to generate in the normal course of business. Liabilities

are carried at the present discounted value of the future net cash outflows that are expected to be required to settle the liabilities in the normal course of business.

The measurement basis most commonly adopted by entities in preparing their financial statements is historical cost. This is usually combined with other measurement bases. For example, inventories are usually carried at the lower of cost and net realizable value; marketable securities can be carried at market value; and pension liabilities are carried at their present value. Furthermore, some entities use the current cost basis as a response to the inability of the historical cost accounting model to deal with the effects of changing prices of non-monetary assets.

Departures from Generally Accepted Accounting Principles

As with rules for most things, departures from GAAP are sometimes required. It was impossible for GAAP developers to anticipate all circumstances to which the principles are applied. It can be assumed that adherence to GAAP almost always results in financial statements that are fairly presented. However, the standard-setting bodies recognize that, upon occasion, there might be an unusual circumstance when the literal application of GAAP would render the financial statements misleading. In these cases, a departure from GAAP is the proper accounting treatment.

The question of when it is appropriate to stray from GAAP is a matter of professional judgment; there is no clear-cut set of circumstances that justify such a departure. However, the fact that complying with GAAP would be more expensive or would make the financial statements look weaker is not a reason to use a non-GAAP method of accounting for a transaction.

Departures from GAAP can be justified in the following circumstances:

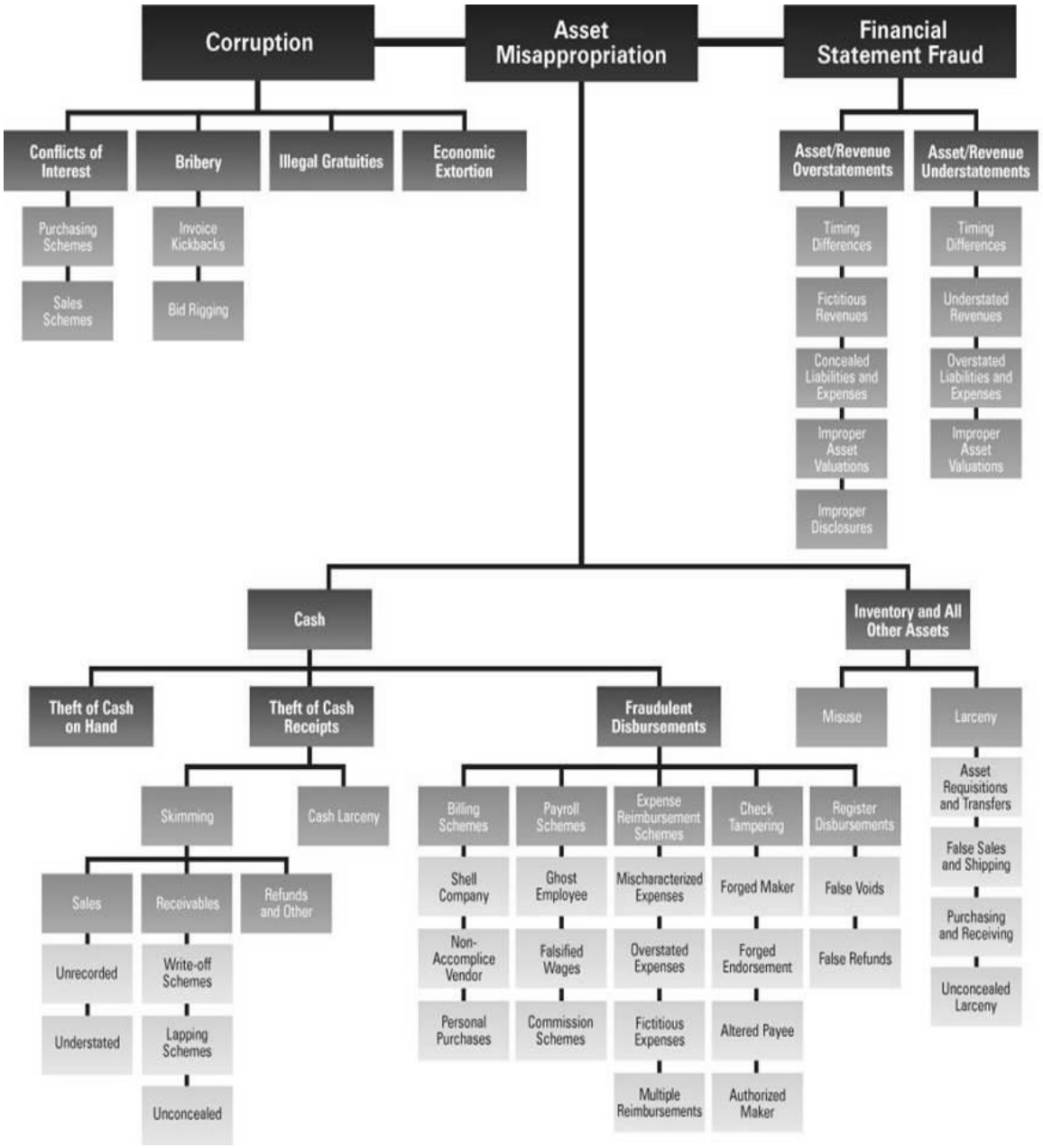
- It is common practice in the entity's industry for a transaction to be reported a particular way.
- The substance of the transaction is better reflected (and, therefore, the financial statements are more fairly presented) by not strictly following GAAP.
- If a transaction is considered immaterial (i.e., it would not affect a decision made by a prudent reader of the financial statements), then it need not be reported.
- There is concern that assets or income would be overstated (the conservatism constraint requires that when there is any doubt, one should avoid overstating assets and income).

- The results of departure appear reasonable under the circumstances, especially when strict adherence to GAAP would produce unreasonable results and the departure is properly disclosed.

FINANCIAL STATEMENT FRAUD

Financial statement schemes are one of a large category of frauds that fall under the heading of *Occupational Fraud and Abuse*, which is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets." Simply stated, occupational frauds are those in which an employee, manager, officer, or owner of an organization commits fraud to the organization's detriment. The three major types of occupational fraud are corruption, asset misappropriation, and financial statement fraud. The following diagram shows the complete classification of occupational fraud, frequently referred to as the *Fraud Tree*.

(NOTE: The discussions pertaining to accounting rules and standards in the following sections are generalized, and are based on accounting practices common to many countries. However, required accounting treatments vary among regions and organization types. Therefore, it is important to consult the applicable accounting standards governing the organization being examined to determine whether a particular accounting treatment is correct.)



The Fraud Tree

What Is Financial Statement Fraud?

Financial statement fraud is the *deliberate misrepresentation* of the financial condition of an enterprise accomplished through the *intentional misstatement* or *omission* of amounts or disclosures in the financial statements to *deceive* financial statement users.

Note that financial statement fraud, much like all types of fraud, is an intentional act. As stated in the International Standard on Auditing (ISA) 240, *The Auditor's Responsibility Relating to Fraud in an Audit of Financial Statements,* "misstatements in the financial statements can arise from error or fraud. The distinguishing factor between error and fraud is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional."

Financial statement fraud is usually a means to an end rather than an end in itself. When people "cook the books," they might be doing it to "buy more time" to quietly fix business problems that prevent their company from achieving its expected earnings or complying with loan covenants. It might also be done to obtain or renew financing that would not be granted, or would be smaller, if honest financial statements were provided. People who are intent on profiting from crime might commit financial statement fraud to obtain loans they can then siphon off for personal gain or to inflate the price of the company's shares, allowing them to sell their holdings or exercise stock options at a profit, or even obtain bonus money calculated based on sales or profits. However, in many past financial statement fraud cases, the perpetrators have gained little or nothing personally in financial terms. Instead, the focus appears to have been preserving their status as the organizations' leaders—a status that might have been lost had the real financial results been published promptly.

Financial statement fraud almost always involves overstating assets, revenues, and profits and understating liabilities, expenses, and losses. However, sometimes the opposite result is desired. For example, understating assets or revenue might lead to a smaller tax liability for the company. Alternatively, a fraudster might wish to minimize over-budget results in a good year in order to help make up for any shortcomings during the subsequent year.

Financial statements are the responsibility of the organization's management. Accordingly, financial statement fraud is typically committed by someone in a managerial role who not only has the ability to alter the financial statements, but also has an incentive to do so. Since fraud investigations are typically conducted or overseen by management, financial

statement fraud cases often persist for a long time before the whistle is blown and the fraud is discovered.

The Cost of Financial Statement Fraud

Financial statement fraud frequently has a devastating effect on an organization's reputation and financial position, as well as on the people involved. The stock market capitalization of companies affected by financial statement fraud might fall substantially almost overnight, losing billions of dollars for investors. Even if the balance sheet and income statement do not change substantially, a restatement is likely to damage investors' confidence in the reporting ability of the company's management and its auditors, and the company's stock price will decrease accordingly.

Many jobs might be lost as companies restructure to restore profitability. Financial statement fraud can influence the well-being of employees, who might lose their jobs, retirement funds, any savings invested in their employer's stock, and health care and other benefits. The company's auditors are likely to be sued for the amount of investors' losses, which could mean billions of dollars for large public companies. For large and small companies alike, financial statement fraud can be costly and potentially destroy the company.

Why Financial Statement Fraud Is Committed

There are a number of reasons why individuals commit financial statement fraud. Most commonly, financial statement fraud is used to make a company's earnings look better on paper. Financial statement fraud occurs through a variety of methods, such as valuation judgments and fine points of timing the recording of transactions. These more subtle types of fraud are often dismissed as either mistakes or errors in judgment and estimation. Some of the more common reasons why people commit financial statement fraud include:

- To encourage investment through the sale of stock
- To demonstrate increased earnings per share or partnership profits interest, thus allowing increased dividend/distribution payouts
- To cover inability to generate cash flow
- To avoid negative market perceptions
- To obtain financing, or to obtain more favorable terms on existing financing
- To receive higher purchase prices for acquisitions
- To demonstrate compliance with financing covenants

- To meet company goals and objectives
- To receive performance-related bonuses

This limited list of reasons shows that the motivation for financial statement fraud does not always involve direct personal financial gain. Sometimes, the cause of fraudulent financial reporting is the combination of situational pressures on either the company or the manager and the opportunity to commit the fraud without the perception of being detected. These pressures are known as "red flags." That is to say, if red flags (situational pressures and opportunity) are present, then the risk of financial reporting fraud increases significantly.

Examples of situational pressures include:

- Sudden decreases in revenue or market share experienced by a company or an industry
- Unrealistic budget pressures, particularly for short-term results (the pressures become even greater with arbitrarily established budgets that are without reference to current conditions)
- Financial pressures resulting from bonus plans that depend on short-term economic performance (these pressures are particularly acute if the bonus is a significant component of the individual's total compensation)

Opportunities to commit fraud most often arise gradually. Generally, these opportunities can come from a lack of adequate oversight functions within the company. The existence of an oversight function does not, in and of itself, guarantee the detection of fraudulent acts; the oversight function must also respond effectively. The perception of detection, not internal control by itself, is arguably the strongest deterrent to fraud.

Some of the more obvious opportunities for the existence of fraud are:

- Absence of a board of directors or audit committee
- Improper oversight or other neglectful behavior by the board of directors or audit committee
- Weak or nonexistent internal controls, including an ineffective internal audit staff and a lack of external audits
- Unusual or complex transactions (an understanding of the transactions, their component parts, and their effect on financial statements is paramount to fraud deterrence)
- Financial estimates that require significant subjective judgment by management

Trends in Financial Statement Fraud

According to the ACFE's 2014 *Report to the Nations on Occupational Fraud and Abuse*, financial statement fraud comprised 9 percent of the frauds reported in the study, with a median loss of $1 million. However, it is important to note that quoted losses resulting from financial statement fraud are often measuring lost market capitalization or lost shareholder value rather than direct loss of financial assets. This does not make the scheme any less harmful; in fact, the lost shareholder value resulting from financial statement fraud can have devastating effects on even the largest companies. It can also have a tremendous impact on the organization's shareholders.

Financial Statement Fraud Schemes

Fraud in financial statements typically takes the form of:

- Overstated assets or revenue
- Understated liabilities and expenses

Overstating assets or revenue falsely reflects a financially stronger company by inclusion of fictitious asset costs or artificial revenues. Understated liabilities and expenses are shown through exclusion of costs or financial obligations. Both methods result in increased equity and net worth for the company. This manipulation results in increased earnings per share or partnership profit interests, or a more stable picture of the company's true situation.

However, in some cases, financial statement fraud takes the opposite form:

- Assets and revenues are understated
- Liabilities and expenses are overstated

To demonstrate the over- and understatements typically used to fraudulently enhance the financial statements, the schemes have been divided into five classes. Because the maintenance of financial records involves a double-entry system, fraudulent accounting entries always affect at least two accounts and, therefore, at least two categories on the financial statements. While the following areas reflect their financial statement classifications, keep in mind that the other side of the fraudulent transaction exists elsewhere. The five classifications of financial statement schemes are:

- Fictitious revenues
- Timing differences (including improper revenue recognition)
- Improper asset valuations

- Concealed liabilities and expenses
- Improper disclosures

As discussed in the following example, financial statement frauds can entail a combination of these schemes.

EXAMPLE OF MULTIPLE FRAUD SCHEMES

In February of 2008, the U.S. Securities and Exchange Commission (SEC) filed financial fraud charges against Bally Total Fitness Holding Corporation (Bally), a nationwide commercial operator of fitness centers, alleging that Bally violated the antifraud, reporting, books and records, and internal control provisions of the federal securities laws (United States Securities and Exchange Commission v. Bally Total Fitness Holding Corporation). According to the SEC, from at least 1997 through 2003, Bally's financial statements were compromised by more than two dozen accounting improprieties. The alleged improprieties caused Bally to overstate its originally reported year-end 2001 stockholders' equity by $1.8 billion, or more than 340 percent; to understate its originally reported 2002 net loss by $92.4 million, or 9341 percent; and to understate its originally reported 2003 net loss by $90.8 million, or 845 percent. Bally settled the charges with the SEC in February of 2008 and emerged from bankruptcy proceedings under new, private ownership.

Later, in December of 2009, the former Bally CFO and former controller were charged for their roles in the accounting violations, as were Bally's independent auditor, Ernst & Young, LLP (E&Y), and six E&Y partners. According to the SEC, Bally's former CFO and former controller were responsible for the fraudulent financial accounting and disclosures, and the unqualified audit opinions issued by E&Y were false and misleading, as the auditors knew or should have known about the fraud. All parties charged settled with the SEC without admitting or denying the charges.

Bally's alleged improprieties involved fictitious revenues, timing differences, concealed liabilities and expenses, improper disclosures, and improper asset valuations. The following is a summary of just some of the many financial statement schemes employed by Bally.

Bally employed a number of inappropriate accounting tricks to overstate its revenue:

- *Rather than recognize revenue from initiation fees over the entire estimated gym membership life, as was required by U.S. GAAP, Bally chose to inappropriately recognize these fees over a shorter period of time.*

- *Bally elected, in violation of U.S. GAAP, to recognize as revenue the entire amount of prepaid dues in the month payment was received, instead of deferring the prepaid dues and recognizing them as earned.*
- *Bally recognized hypothetical membership reactivation fees as revenue anticipated (up to three years in the future). U.S. GAAP prohibited Bally from recognizing revenue from reactivation fees until after the reactivating members had entered into binding contracts.*
- *Bally recognized revenue from unpaid dues on inactive memberships, a practice that was in violation of U.S. GAAP.*
- *Under U.S. GAAP, Bally was to account for revenue from its bundled packages (consisting of gym memberships, nutritional products, and personal training services) as a single element, unless it met certain exceptions (which Bally did not meet). Bally failed to comply with U.S. GAAP, accounting for each item in the package as a separate element and prematurely recording revenue.*
- *U.S. GAAP required that revenue from prepaid personal training services be recognized when earned; that is, when the services were actually provided. Bally recognized revenue related to prepaid personal training services before it was actually earned.*
- *Bally prematurely recognized revenue from the sale of future receivables by accounting for these sales as sales of financial assets. Under U.S. GAAP, Bally was required to account for these transactions as debt.*

Bally was equally creative when it came to using accounting improprieties to understate its expenses and liabilities:

- *Bally deferred as "membership acquisition costs" costs that were not directly related to the acquisition of membership contracts. Under U.S. GAAP, these costs were to be expensed as incurred.*
- *Bally failed to include interest expense associated with a liability on bonds, in addition to improperly removing the bond obligation from its balance sheet. Both actions were in violation of U.S. GAAP.*
- *Under U.S. GAAP, Bally was to expense advertising expenses no later than the first time the advertising took place. Bally violated U.S. GAAP by deferring recognition of the production costs of its advertisements over the estimated life of the advertisements.*
- *When Bally acquired other health clubs, it was required under U.S. GAAP to allocate a portion of the purchase price to certain separately identifiable intangible assets and to conduct impairment analysis of goodwill. Bally failed to do either, which resulted in an overstatement of goodwill and an understatement of expenses.*

Additionally, Bally carried out various improprieties to understate its accumulated deficit:

- *In accounting for its leased facilities, Bally was not in compliance with U.S. GAAP for several reasons: (1) Bally improperly failed to recognize rent expense on club leases with escalating rental obligations using the required straight-line rent method; (2) Bally improperly reflected tenant allowances as a reduction of property and equipment on the balance sheet and improperly amortized these amounts and the related leasehold improvements to depreciation expense; (3) Bally improperly reflected tenant allowances as a component of cash flows from investing activities in its statement of cash flows; and (4) Bally improperly failed to depreciate leasehold improvements over the lesser of the asset's economic life, with a maximum of 15 years, or the contractual term of the lease, excluding all renewal options.*
- *At times, Bally temporarily closed various clubs while it undertook construction and remodeling in preparation for use by members. Bally still incurred rent costs during the construction periods, which, under U.S. GAAP, Bally was to recognize as expenses when incurred unless certain requirements were met. Bally didn't meet those requirements, but nonetheless improperly deferred recognition of the rent costs.*
- *While clubs were closed for remodeling and construction, Bally incurred certain internal compensation costs, which, under U.S. GAAP, were required to be expensed when services were rendered. Bally improperly capitalized and deferred these costs and recognized them as expenses in later periods.*

Under U.S. GAAP, Bally was required to periodically analyze whether the value of its fixed assets had been impaired, and if it had, to recognize the amount of the impairment as an expense. Bally failed to identify the existence of events that should trigger an asset impairment analysis, and failed to measure the related impairment charges.

Fictitious Revenues

Fictitious or fabricated revenues involve the recording of sales of goods or services that did not occur. Fictitious sales most often involve fake customers, but can also involve legitimate customers. For example, a fictitious invoice can be prepared (but not mailed) for a legitimate customer even though the goods are not delivered or the services are not rendered. At the end of the accounting period, the sale will be reversed, which will help conceal the fraud. However, the artificially high revenues of the period might lead to a revenue shortfall in the new period, creating the need for more fictitious sales. Another method is to use legitimate customers and artificially inflate or alter invoices to reflect higher amounts or quantities than are actually sold.

The challenge with both of these methods is balancing the other side of the entry. A credit to revenue increases the revenue account, but the corresponding debit in a legitimate sales transaction typically either goes to cash or accounts receivable. Since no cash is received in a fictitious revenue scheme, increasing accounts receivable is the easiest way to get away with recording the entry. However, accounts receivable stay on the books as an asset until they are collected. If the outstanding accounts never get collected, they will eventually need to be written off as bad debt expense. Mysterious accounts receivable on the books that are long overdue are a common sign of a fictitious revenue scheme.

EXAMPLE OF FICTITIOUS REVENUES

In one case, a foreign subsidiary of a U.S. company recorded several large fictitious sales to a series of companies. It invoiced the sales but did not collect any of the accounts receivable, which became severely past due. The manager of the foreign subsidiary arranged for false confirmations of the accounts receivable for audit purposes and even hired actors to pretend to be the customers during a visit from U.S. management. Background checks on the customers would have revealed that some of the companies were fictitious while others either were undisclosed related parties or operated in industries that would have no need for the goods supposedly supplied. An investigation revealed that the manager of the foreign subsidiary directed the scheme to record fictitious revenues to meet unrealistic revenue goals set by U.S. management.

In some cases, companies go to great lengths to conceal fictitious sales. A sample journal entry from such a case is detailed here. To record an alleged purchase of fixed assets, a fictional entry is made by debiting fixed assets and crediting cash for the amount of the alleged purchase:

Date	Description	Ref.	Debit	Credit
12/01/X1	Fixed Assets	104	350,000	
	Cash	101		350,000

A fictitious sales entry is then made for the same amount as the false purchase, debiting accounts receivable and crediting the sales account. The cash outflow that supposedly paid for the fixed assets is "returned" as payment on the receivable account, though in practice the cash might never have moved if the fraudsters didn't bother to falsify that extra documentary support.

Date	Description	Ref.	Debit	Credit
12/01/X1	Accounts Rec	120	350,000	
	Sales	400		350,000
12/15/X1	Cash	101	350,000	
	Accounts Rec	120		350,000

The result of this completely fabricated sequence of events is an increase in both fixed assets and revenue. The debit could alternatively have been directed to other accounts, such as inventory or accounts payable, or simply left in accounts receivable if the fraud were committed close to the year's end and the receivable could be left outstanding without attracting undue attention. The subsequent case describes yet another approach to revenue fabrication.

EXAMPLE OF REVENUE FABRICATION INVOLVING
DECEPTIVE SALES AND CUSTOMERS

In what has become India's largest corporate scandal, Satyam Computer Services Limited (Satyam) founder and chairman, B. Ramalinga Raju, suddenly quit in January 2009, confessing that he had falsified company accounts for years. In his four-and-a-half page resignation letter, Raju revealed he had overstated the company's reported cash balance by $1 billion.

Satyam (renamed Mahindra Satyam in 2009), a foreign private issuer, is a large information technology services company incorporated in the Republic of India that provides back office support functions to organizations around the world.

In April of 2011, the company agreed to a $10 million penalty to settle the SEC's charges in U.S. Securities and Exchange Commission v. Satyam Computer Services Limited d/b/a Mahindra Satyam.

According to the SEC, a complete failure of internal controls over Satyam's invoice management system, books of account, and financial reporting enabled the company's then-senior managers to intentionally overstate revenue, income, earnings per share, cash, and interest-bearing deposits from 2003 through September 2008 by over $1 billion, or more than half of the company's total assets.

More specifically, the SEC alleged that Satyam's then-senior management falsified the company's reported revenues by creating more than 6,000 false invoices for services never provided and also for nonexistent customers. Certain employees were given administrative

logins and passwords to the invoice management system so that they could record the false invoices, ensuring that the invoices were used in the calculation of revenue but concealed from Satyam's business unit heads so they would not spot the suspicious invoices. Forged bank statements were created by Satyam's employees to reflect "payment" on the false invoices, inflating the company's cash balances.

In confirming Satyam's cash balance, the auditors relied on management to send confirmation requests to the company's banks and to return alleged confirmation responses from the banks to the auditors. This was in direct conflict with standard audit procedures, which require that (1) cash balances be independently confirmed with the financial institutions in which the accounts are held, and (2) the auditors retain control over the confirmation documents to reduce the risk of tampering. Had this basic procedure been performed in accordance with standards, it is likely that the auditors would have caught the fraud themselves.

Fictitious sales schemes are not always elaborate, however. Less complex methods include shipments of false or defective products. In one instance, a company shipped goods to a customer and recorded revenue, even though the customer had agreed only to evaluate the product, not purchase it. In some extreme cases, goods are shipped and booked as revenue to customers who did not order them.

Fraud examiners should be skeptical about large revenue transactions recorded near the end of the period. Because the company might be trying to meet sales targets, careful examination of supporting documentation is essential to determine the sales are legitimate.

In reviewing purchase orders, auditors should look for cancellation clauses that could contradict the sale. Auditors should read sales contracts and look for cancellation privileges and lapse dates. Revenue should not be recorded until the cancellation privilege lapses. The absence of a requested shipping date on a purchase order might indicate that the customer will notify the seller when shipment is to occur, which might mean that no exchange is presently being requested.

What Red Flags Are Associated with Fictitious Revenues?

The following red flags are associated with fictitious revenues:

- An unusually large amount of long overdue accounts receivable
- Outstanding accounts receivable from customers that are difficult or impossible to identify and contact

- Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Significant transactions with related parties or special purpose entities not in the ordinary course of business or where those entities are not audited or are audited by a separate firm
- Significant, unusual, or highly complex transactions, especially those close to the period's end that pose difficult "substance over form" questions
- Unusual growth in the days' sales in receivables ratio (receivables/average daily sales)
- A significant volume of sales to entities whose substance and ownership is not known
- An unusual increase in sales by a minority of units within a company or in sales recorded by corporate headquarters

Timing Differences (Including Improper Revenue Recognition)

Financial statement fraud might also involve timing differences—that is, the recording of revenues or expenses in improper periods. This can be done to shift revenues or expenses between one period and the next, increasing or decreasing earnings as desired. This practice is also referred to as *income smoothing*.

Premature Revenue Recognition

In general, revenue should be recognized in the accounting records when a sale is complete—that is, when title is passed from the seller to the buyer. This transfer of ownership completes the sale and is usually not final until all obligations surrounding the sale are complete.

Under IFRS, revenue is generally recognized or recorded under IFRS when it becomes realized or realizable, and earned. According to accrual accounting, revenue should not be recognized for work that is to be performed in subsequent accounting periods, even though the work might currently be under contract. In general, revenue should be recognized in the period in which the work is performed.

EXAMPLE

ABC, Inc. sells products that require engineering and adapting work before they are acceptable to customers. However, the company records sales revenue before completing the engineering, testing, evaluation, and customer acceptance stages of production. In some cases,

sales do not take place for weeks or months. In other cases, the sales are specifically contingent upon the customer's trial and acceptance of the product.

EXAMPLE

Another company is engaged in the design, development, manufacture, marketing, and servicing of computer peripheral subsystems. The company recognized revenue prior to a time when collection of the sales price was reasonably assured and at a time prior to completion of the underlying sales transaction.

It was the company's policy to recognize revenue when the products were shipped. However, the sales were not complete as of the time of shipment because customers were not obligated to pay for the equipment until it had been installed; the company had substantial obligations to the customers for installation and adjustments; and there remained major uncertainties concerning the customers' true willingness to complete the transaction because of the volatile nature of the high-tech product.

In May 2014, the U.S. FASB and the IASB issued a converged standard on revenue recognition, *Revenue from Contracts with Customers*. For IFRS, the new statement has been issued as IFRS 15; for U.S. GAAP, the new standard will be codified in ASC 606 and will replace ASC 605. Companies adhering to U.S. GAAP or IFRS will be required to apply the revised standard as follows:

- Companies using IFRS: For annual reporting periods beginning on or after January 1, 2018
- Public companies using U.S. GAAP: For annual reporting periods beginning on or after January 1, 2018
- Nonpublic companies using U.S. GAAP: For annual reporting periods beginning on or after January 1, 2018

The core principle of the revised revenue recognition standard is that an entity should recognize revenue to depict the transfer of promised goods or services to customers in an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services. To achieve compliance with this revised standard, an entity should apply the following steps:

1. Identify the contract(s) with a customer. A contract is an agreement between two or more parties that creates enforceable rights and obligations.

2. Identify the performance obligations in the contract. A contract includes promises to transfer goods or services to a customer. If those goods or services are distinct, the promises are performance obligations and are accounted for separately.
3. Determine the transaction price. The transaction price is the amount of consideration in a contract to which an entity expects to be entitled in exchange for transferring promised goods or services to a customer.
4. Allocate the transaction price to the performance obligations in the contract. An entity usually allocates the transaction price to each performance obligation based on the comparative standalone selling prices of each distinct good or service promised in the contract. If a standalone selling price is not easily observable, it must be estimated.
5. Recognize revenue when (or as) the entity satisfies a performance obligation. An entity recognizes revenue when (or as) it satisfies a performance obligation by transferring a promised good or service to a customer (which is when the customer obtains control of that good or service). The amount of revenue recognized is the amount allocated to the satisfied performance obligation.

Sales with Conditions

Sales with conditions are those that have terms that have not been completed and those with rights and risks of ownership that have not passed to the purchaser. In most cases, such sales cannot be recorded as revenue. These types of sales are similar to schemes involving the recognition of revenue in improper periods, since the conditions for sale might become satisfied in the future, at which point revenue recognition would become appropriate.

External pressures to succeed that are placed on business owners and managers by bankers, stockholders, families, and even communities often provide the motivation to commit fraud. For example, in addition to other charges, General Electric (GE) was alleged by the U.S. Securities and Exchange Commission (SEC) to have manipulated earnings for two years in a row (2002 and 2003) to meet performance targets by recording $381 million in "sales" of locomotives to financial partners. Since GE had not relinquished ownership of the assets and had agreed to maintain and secure them on its property, the transactions were, in reality, more like loans than sales. GE settled the SEC's charges in 2009 for $50 million, neither admitting nor denying guilt.

Long-Term Contracts

Long-term contracts can cause special problems for revenue recognition. In many countries, for example, revenues and expenses from long-term construction contracts can be recorded

using either the completed-contract method or the percentage-of-completion method, depending partly on the circumstances. The completed-contract method does not record revenue until the project is 100 percent complete. Construction costs are held in an inventory account until completion of the project. The percentage-of-completion method recognizes revenues and expenses as measurable progress on a project is made, but this method is particularly vulnerable to manipulation. Managers can often easily manipulate the percentage-of-completion and the estimated costs to complete a construction project to recognize revenues prematurely and conceal contract overruns.

Multiple Deliverables

Product and service sales sometimes involve multiple deliverables (or multiple-element arrangements). For example, a cell phone company provides a discounted or free cell phone to a customer who signs up for a two-year service agreement; in this situation, the deliverables include both the product (cell phone) and the service, which spans two years. In multiple-element arrangements, the seller completes the earnings process—and thus must recognize revenue—over a period of time.

Financial reporting fraud risks associated with multiple-element revenue arrangements include:

- Falsely claiming that the criteria for a multiple-element revenue arrangement have been met
- Manipulating the allocation of revenue among the individual components of the arrangement to accelerate revenue recognition (by allocating more to the components to be recognized early and less to components that must be deferred to future periods)

Channel Stuffing

A challenging area of revenue recognition is *channel stuffing*. This term refers to the sale of an unusually large quantity of a product to distributors who are encouraged to overbuy through the use of deep discounts or extended payment terms. This practice is especially attractive to industries with high gross margins—such as tobacco, pharmaceuticals, perfume, soda concentrate, and branded consumer goods—because it can increase short-term earnings. On the downside, however, stealing from future periods' sales makes it harder to achieve sales goals in those future periods. The pressure to meet sales goals can, in turn, lead to increasingly disruptive levels of channel-stuffing and, ultimately, to a restatement. Although orders are received, the terms of the order might raise questions about the collectibility of the accounts receivable, and any existing side agreements that grant a right of return might,

effectively, turn the sales into consignment sales. Also, there might be a greater risk of returns for certain products if they cannot be sold before their shelf life ends.

This is particularly a problem for pharmaceuticals because retailers will not accept drugs with a short shelf life remaining. As a result, "channel stuffing" should be viewed skeptically, since in certain circumstances it may constitute fraud. For example, the U.S. Securities and Exchange Commission filed a complaint against Bausch & Lomb, indicating that the company's internal estimates showed that it might take distributors up to two years to sell the quantity of contact lenses the company was trying to get them to purchase in the last two weeks of its fiscal year.

Recording Expenses in the Wrong Period

The timely recording of expenses is often compromised due to pressures to meet budget projections and goals, or due to lack of proper accounting controls. As the expensing of certain costs is pushed into periods other than the ones in which they actually occur, they are not properly matched against the income that they help produce. For example, revenue might be recognized on the sale of certain items, but the cost of goods and services that went into the items sold might intentionally not be recorded in the accounting system until the following period. This might make the sales revenue from the transaction almost pure profit, inflating earnings. In the next period, earnings would have fallen by a similar amount.

What Red Flags Are Associated with Timing Differences (Including Improper Revenue Recognition)?

- Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Significant, unusual, or highly complex transactions, especially those close to the period's end, that lead to difficult "substance over form" questions
- Unusual increase in gross margin or gross margin in excess of industry peers
- Unusual growth in the days' sales in receivables ratio (receivables/average daily sales)
- Unusual decline in the days' purchases in accounts payable ratio (accounts payable/average daily purchases)

Improper Asset Valuation

One way to commit financial statement fraud is to manipulate the valuation of a company's assets. Typically, a fraudster artificially increases asset accounts to strengthen the company's balance sheet and its financial ratios. In some cases, however, a fraudster might want to record false revenues, and overstated assets are simply a by-product of that scheme.

With the exception of certain securities, asset values are generally not increased to reflect current market value. It is often necessary to use estimates in accounting. For example, estimates are used in determining the residual value and the useful life of a depreciable asset, the uncollectible portion of accounts receivable, or the excess or obsolete portion of inventory. Whenever estimates are used, there is an additional opportunity for fraud by manipulating those estimates.

Many schemes are used to inflate current assets at the expense of long-term assets. In the case of such schemes, the net effect is seen in the current ratio, which divides current assets by current liabilities to evaluate a company's ability to satisfy its short-term obligations. By misclassifying long-term assets as short-term, the current ratio increases. This type of misclassification can be of critical concern to lending institutions that often require the maintenance of certain financial ratios. This is of particular consequence when the loan covenants are on unsecured or under-secured lines of credit and other short-term borrowings. Sometimes these misclassifications are referred to as "window dressing."

Most improper asset valuations involve the fraudulent overstatement of inventory or receivables, again with the goal being to strengthen the appearance of the balance sheet. Other improper asset valuations include manipulation of the allocation of the purchase price of an acquired business to inflate future earnings, misclassification of fixed and other assets, or improper capitalization of inventory or start-up costs.

Improper asset valuations usually take the form of one of the following classifications:

- Inventory valuation
- Accounts receivable
- Business combinations
- Fixed assets

Inventory Valuation

Under many countries' accounting standards, as well as IFRS, inventory should be recorded at the lower of cost or net realizable value. This means that inventory must be valued at its acquisition cost, except when the cost is determined to be higher than the net realizable value, in which case it should be written down to its net realizable value or written off altogether if it has no value. Failing to write down or write off inventory results in overstated assets and the mismatching of cost of goods sold with revenues.

Other methods by which inventory can be improperly stated include manipulation of the physical inventory count, inflation of the unit costs used to price out inventory, and failure to adjust inventory for the costs of goods sold. Fictitious inventory schemes usually involve the creation of fake documents, such as inventory count sheets and receiving reports. Many inventory reports are kept electronically, which allows the fraud examiner to total columns and perform data analysis techniques to detect these types of inventory fraud schemes.

In some instances, friendly co-conspirators claim to be holding inventory for companies in question. Other times, companies falsely report large values of inventory in transit, knowing that it would be nearly impossible for the auditors to observe. "Bill and hold" items that have already been recorded as sales might be included in the physical inventory count, as might goods owned by third parties but held by companies on consignment or for storage. There have been cases of fraudsters assembling pallets of inventory with hollow centers, placing bricks in sealed boxes instead of high-value products, and shuttling inventory overnight between locations being observed by auditors on different days so as to double count the inventory. Another possible inventory inflation strategy is for companies to insert phony count sheets during the inventory observation or change the quantities on the count sheets.

Accounts Receivable

Accounts receivable are subject to manipulation in the same manner as sales and inventory, and, in many cases, the schemes are conducted together. The two most common schemes involving overstated accounts receivable are recording fictitious receivables and the failure to properly account for uncollectible customer accounts.

FICTITIOUS ACCOUNTS RECEIVABLE

Fictitious accounts receivable go hand-in-hand with fictitious sales, as discussed in the previous section. They are common among companies with financial problems, as well as

with managers who receive a commission based on sales. The typical entry under fictitious accounts receivable is to debit (increase) accounts receivable and credit (increase) sales. Of course, these schemes are more common around the end of the accounting period, since accounts receivable are expected to be paid in cash within a reasonable time. Fraudsters commonly attempt to conceal fictitious accounts receivable by providing false confirmations of balances to auditors. They get the audit confirmations because the mailing address they provide for the phony customers is typically either a mailbox under their control, a home address, or the business address of a co-conspirator. Such schemes can be detected by using satellite imaging software, business credit reports, public records, or even the telephone book to identify customers who have no physical existence or no apparent business need for the product sold to them.

FAILURE TO ACCOUNT FOR UNCOLLECTIBLE ACCOUNTS

In general, accounts receivable should be reported at net realizable value—that is, the amount of the receivable less the amount expected not to be collected. As such, companies generally are required to write off uncollectible receivables as bad debt expense.

Managers can overstate their company's accounts receivable balance by failing to record bad debt expense. Bad debt expense is recorded to account for any uncollectible accounts receivable. The debit side of the entry increases bad debt expense, and the credit side of the entry increases the allowance (or provision) for doubtful accounts, which is a contra account that is recorded against accounts receivable. Therefore, if the controller fails to record bad debt expense, the allowance (or provision) for doubtful accounts will be understated.

For example, suppose ABC Company has total accounts receivable of $500,000. However, management has learned one of the company's debtors is filing for bankruptcy and will likely default on its $15,000 loan. ABC Company would need to record the following journal entry to establish the allowance (or provision) for doubtful accounts:

Date	Description	Debit	Credit
12/31/X1	Bad debt expense	15,000	
	Allowance for doubtful accounts		15,000

Once this journal entry is made, accounts receivable is reported at net realizable value. The allowance (or provision) for doubtful accounts represents the amount expected not to be

collected. It is a contra-account to accounts receivable. These two accounts are deducted to arrive at the net realizable value of accounts receivable. The net realizable value of ABC Company's receivables would be $500,000 less $15,000 or $485,000.

Business Combinations

Companies are required to allocate the purchase price they have paid to acquire another business to the tangible and intangible assets of that business. Any excess of the purchase price over the value of the acquired assets is treated as goodwill. In many countries, changes in required methods of accounting for goodwill have decreased the incentive for companies to minimize the amount allocated to goodwill that previously was required to be amortized against future earnings. However, companies might still be tempted to over-allocate the purchase price to in-process research and development assets so that they can then write them off immediately. Alternatively, they might establish excessive reserves for various expenses at the time of acquisition, intending to release those excess reserves into earnings at a future date.

Fixed Assets

Fictitious fixed assets can be created by a variety of methods. They are subject to manipulation through several different schemes. Some of the more common schemes involve booking fictitious assets, misrepresenting asset values, and capitalizing non-asset costs.

BOOKING FICTITIOUS ASSETS

One of the easiest methods of asset misrepresentation is the recording of fictitious assets. This false creation of assets affects account totals on a company's balance sheet. The corresponding account commonly used is the owners' equity account. Because company assets are often physically found in many different locations, this fraud can sometimes be easily overlooked. One of the most common fictitious asset schemes is to simply create fictitious documents. In other instances, the equipment is leased, not owned, and this fact is not disclosed during the audit of fixed assets. Fictitious fixed assets can sometimes be detected because the fixed asset addition makes no business sense.

MISREPRESENTING THE VALUE OF FIXED ASSETS

Fixed assets should be recorded at cost. Although assets might appreciate in value, this increase in value should generally not be recognized on company financial statements. Many financial statement frauds involve the reporting of fixed assets at higher market values rather

than the lower historical (acquisition) costs, or at even higher inflated values with unreasonable valuations to support them. Misrepresentation of asset values frequently goes hand in hand with other schemes.

EXAMPLE

In October 2002, the U.S. Securities and Exchange Commission (SEC) filed a civil enforcement action against former Enron CFO Andrew S. Fastow, who also faced criminal charges, relating to an alleged self-enriching scheme to defraud Enron's security holders through the use of certain off-balance sheet entities. One of the six transactions in the SEC's complaint against Andrew Fastow involved Raptor I and Avici. According to the complaint, Enron and the Fastow-controlled partnership LJM2 engaged in complex transactions with an entity called Raptor I. Raptor I was used to manipulate Enron's balance sheet and income statement and to generate profits for LJM2 and Fastow at Enron's expense. In September 2000, Fastow and others used Raptor I to create a fraudulent hedging transaction and thus avoid a decrease in the value of Enron's investment in the stock of a public company called Avici Systems Inc. Specifically, Fastow and others back-dated documents to make it appear that Enron had locked in the value of its investment in Avici in August of 2000, when Avici's stock was trading at its all-time high price.

CAPITALIZING NON-ASSET COSTS

Interest and finance charges incurred in the purchase are excluded from the recorded cost of a purchased asset. For example, when a company finances a capital equipment purchase, monthly payments include both principal liability reduction and interest payments. On initial purchase, only the original cost of the asset should be capitalized. The subsequent interest payments should be charged to interest expense and not to the asset. Without a reason for intensive review, this type of fraud can go unchecked.

Understating Assets

In some cases, as with some government-related or government-regulated companies, it is advantageous to understate assets. Additional funding is often based on asset amounts. This understatement can be done directly or through improper depreciation.

Misclassifying Assets

To meet budget requirements—and for various other reasons—assets are sometimes misclassified into general ledger accounts in which they don't belong. For example, fixed

assets might be fraudulently reclassified as current assets. The manipulation can create misleading financial ratios and help the company comply with loan covenants or other borrowing requirements.

What Red Flags Are Associated with Improper Asset Valuation?

The following red flags commonly indicate improper asset valuation schemes:

- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Significant declines in customer demand and increasing business failures in either the industry or the overall economy
- Assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to support
- Nonfinancial management's excessive participation in or preoccupation with the selection of accounting principles or the determination of significant estimates
- Unusual increase in gross margin or margin in excess of industry peers
- Unusual growth in the number of days' sales in receivables ratio
- Unusual growth in the number of days' purchases in inventory ratio
- Reduction in allowances (or provision) for bad debts, excess inventory, and obsolete inventory especially if relevant ratios are out of line with those of industry peers
- Unusual change in the relationship between fixed assets and depreciation
- Adding to assets while competitors are reducing capital tied up in assets

Concealed Liabilities and Expenses

Understating liabilities and expenses is one of the ways financial statements can be manipulated to make a company appear more profitable than it actually is. Because pre-tax income will increase by the full amount of the expense or liability not recorded, this financial statement fraud method can significantly affect reported earnings with relatively little effort by the fraudster. It is much easier to commit this scheme than to falsify sales transactions. Missing transactions can also be harder for auditors to detect than improperly recorded ones since the missing transactions leave no audit trail.

There are three common methods for concealing liabilities and expenses:

- Liability/expense omissions
- Improperly capitalizing costs rather than expensing them
- Failure to disclose warranty costs and product-return liabilities

Liability/Expense Omissions

The preferred and easiest method of concealing liabilities or expenses is to simply fail to record them. Large monetary judgments against a company from a recent court decision might be conveniently ignored. Vendor invoices might be thrown away or stuffed into drawers rather than posted into the accounts payable system, thereby increasing reported earnings by the full amount of the invoices. In a retail environment, debit memos might be created for chargebacks to vendors, supposedly to claim permitted rebates or allowances, but sometimes solely to create additional income. Whether these items are properly recorded in a subsequent accounting period does not change the fraudulent nature of the current financial statements.

Often, perpetrators of liability and expense omissions believe they can conceal their frauds in future periods. They frequently plan to compensate for their omitted liabilities with visions of other income sources, such as profits from future price increases.

Just as they are easy to conceal, omitted liabilities are probably one of the most difficult schemes to uncover. A thorough review of all post-financial-statement-date transactions, such as accounts payable increases and decreases, can aid in the discovery of omitted liabilities in financial statements, as can a computerized analysis of expense records. Additionally, if the auditor requested and was granted unrestricted access to the client's files, a physical search could turn up concealed invoices and unposted liabilities. Investigative interviews of accounts payable and other personnel can reveal unrecorded or delayed items as well.

EXAMPLE

In July 2002, the U.S. Securities and Exchange Commission (SEC) filed suit in the United States District Court for the Southern District of New York, charging major cable television producer Adelphia Communications Corporation ("the Company" or "Adelphia"); its founder John J. Rigas; his three sons, Timothy J. Rigas, Michael J. Rigas, and James P. Rigas; and two senior executives at Adelphia, James R. Brown and Michael C. Mulcahey, in one of the most extensive financial frauds ever to take place at a public company. The SEC charged that Adelphia, at the direction of the individual defendants, (1) fraudulently excluded over $2.3 billion in liabilities from its consolidated financial statements by hiding them in off-balance sheet affiliates; (2) falsified operations statistics and inflated Adelphia's earnings to meet Wall Street's expectations; and (3) concealed rampant self-dealing by the Rigas Family, including the undisclosed use of

corporate funds for Rigas Family stock purchases and the acquisition of luxury condominiums in New York and elsewhere.

With respect to the concealed liabilities, the complaint alleged that between mid-1999 and the end of 2001, John J. Rigas, Timothy J. Rigas, Michael J. Rigas, James P. Rigas, and James R. Brown, with the assistance of Michael C. Mulcahey, caused Adelphia to fraudulently exclude from the Company's annual and quarterly consolidated financial statements over $2.3 billion in bank debt by deliberately shifting those liabilities onto the books of Adelphia's off-balance sheet, unconsolidated affiliates. Failure to record this debt violated financial reporting requirements and precipitated a series of misrepresentations about those liabilities by Adelphia and the defendants, including the creation of (1) sham transactions backed by fictitious documents to give the false appearance that Adelphia had actually repaid debts when, in truth, it had simply shifted them to unconsolidated Rigas-controlled entities, and (2) misleading financial statements by giving the false impression through the use of footnotes that liabilities listed in the Company's financials included all outstanding bank debt.

In November 2002, in exchange for his testimony against the Rigas men, James Brown was released from prosecution by consenting to an entry of a permanent injunction against him for U.S. securities law violations. Additionally, Brown has been permanently barred from becoming an officer or director of a public corporation.

In July 2004, after a three-month trial, a federal jury convicted John and Timothy Rigas of conspiracy, securities fraud, and bank fraud. John Rigas received a 15-year prison sentence and was fined $2,300, and Timothy Rigas was sentenced to 20 years in prison. James Rigas was never criminally charged by the Court. In November 2005, Michael Rigas pleaded guilty to a charge of making a false entry in a financial record.

In April 2005, the SEC filed permanent injunctions against John, Timothy, Michael, and James Rigas, as well as James Brown, Michael Mulcahey, and Adelphia Communications Corporation. The defendants were charged with violating anti-fraud, periodic reporting, recordkeeping, and internal control provisions of U.S. securities laws. In addition, the Rigas family members were barred from ever holding officer or director positions in a public company.

Improperly Capitalized Costs

All organizations incur costs. How to record these costs on the books, however, is not always clear. Suppose ABC Company has a piece of property in need of some repairs. If the work performed simply fixes any problems and brings the property back to its original state, then the costs associated with the repair would appear as an expense on the income statement in the year they were incurred. Net income would be reduced by this amount, and the balance sheet would remain unaffected.

However, suppose work is done that not only repairs but increases the value of the property. Any expenditures made that increase the book value of the property would need to be capitalized. In other words, these costs would be added to the asset value on ABC's balance sheet and then depreciated as an expense over time.

Either way, the costs associated with repairs or improvements are on ABC's income statement as an expense. The difference is in the timing. Capitalizing an expenditure and depreciating it over a number of years makes a significant difference in the bottom line of the financial statements in the year the work was done. Conversely, expensing the same amount of costs in the same year results in a much lower net income that year.

Improperly capitalizing expenses is another way to increase income and assets and make the entity's financial position appear stronger. If expenditures are capitalized as assets and not expensed during the current period, income will be overstated. As the assets are depreciated, income in following periods will be understated.

EXAMPLE

In November 2002, the U.S. Securities and Exchange Commission (SEC) filed an amended complaint against WorldCom, Inc., broadening its charges to allege that WorldCom misled investors from at least as early as 1999 through the first quarter of 2002. The complaint stated that the company had acknowledged that during that period WorldCom materially overstated the income it reported on its financial statements by approximately $9 billion, mainly using two methods. First, WorldCom reduced its operating expenses by improperly releasing as a credit to operating expenses certain provisions previously established for line costs and for taxes. Second, the company improperly reduced its operating expenses by reassigning certain expenses as capital assets. Much of the $9 billion related to improper accounting for "line costs," which were among WorldCom's major operating expenses. The SEC complaint alleges that, in a scheme

directed and approved by members of senior management, WorldCom concealed the true extent of its "line costs." By improperly reducing provisions held against "line costs" and by transferring certain "line costs" to its capital asset accounts, WorldCom falsely portrayed itself as a profitable business when it was not and concealed large losses. These improper accounting practices were designed to inflate income to correspond with estimates by Wall Street analysts and to support the price of WorldCom's stock.

In March 2005, former WorldCom CEO Bernard Ebbers was convicted of one count of conspiracy, one count of securities fraud, and seven counts of false regulatory filing, and was later sentenced to 25 years in prison. He also agreed to forfeit nearly all of his personal assets to settle a civil suit filed by angry WorldCom investors.

Scott Sullivan, the former CFO under Ebbers and "the architect" behind the fraud scheme, pled guilty to fraud charges and agreed to testify against Ebbers. Due to his cooperation during the investigation, he was sentenced to only five years in prison. He also agreed to forfeit the proceeds from the sale of his $10 million home, along with his investment holdings, to settle the civil suit brought by shareholders.

Former WorldCom Controller David F. Myers and former Director of General Accounting Buford "Buddy" Yates, Jr., pled guilty to criminal charges prosecuted by the U.S. Attorney's Office for the Southern District of New York. Myers received a sentence of one year and one day in prison. Yates was also sentenced to one year and one day in prison and ordered to pay a $5,000 fine. Additionally, each man was permanently enjoined from acting as an officer or director of any public company and was suspended from practicing before the SEC as an accountant, under Rule 102(2) of the Commission's Rules of Practice.

The SEC also brought civil actions against Betty L. Vinson, CPA, and Troy M. Normand, former members of the WorldCom General Accounting Department. Both were permanently charged with securities violations. Vinson was suspended from appearing or practicing before the SEC as an accountant. In addition, she pled guilty to one count of securities fraud and one count of conspiracy to commit securities fraud, and was sentenced to five months in prison and five months of house arrest. Normand pled guilty to similar charges and received three years of probation for his role in the fraud.

EXPENSING CAPITAL EXPENDITURES

Just as capitalizing expenses is improper, so is expensing costs that should be capitalized. The organization might want to minimize its net income due to tax considerations or to increase earnings in future periods. Expensing an item that should be depreciated over a period of time helps to accomplish just that—net income is lower and, therefore, so are taxes.

Unrecorded and Undisclosed Warranty Costs and Product-Return Liabilities

Improper recording of warranty and product-return liabilities occurs when a company fails to accrue the proper expenses and related liabilities for potential product returns or warranty repairs. It is inevitable that a certain percentage of products sold will, for one reason or another, be returned. When this happens, management must recognize a provision for the best estimate of the costs of making good under the warranty products sold before the end of the reporting period (see IAS 37 14 Recognition Provisions and IAS 37 24 Probable outflow for a class of obligations). The provision may be estimated based on an analysis of historical data (relation between types of products sold and warranty expenses) or on a subsequent review of quality issues around the reporting date.

Likewise, when a company offers a warranty on product sales, it must estimate the amount of warranty expense it reasonably expects to incur over the warranty period and accrue a liability for that amount. In warranty liability fraud, the warranty liability is usually either omitted altogether or substantially understated. Another similar area is the liability resulting from defective products (product liability).

What Red Flags Are Associated with Concealed Liabilities and Expenses?

The following red flags are indicators of concealed liabilities and expenses schemes:

- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to support
- Nonfinancial management's excessive participation in or preoccupation with the selection of accounting principles or the determination of significant estimates
- Unusual increase in gross margin or margin in excess of industry peers
- Allowances/provisions for sales returns, warranty claims, etc., that are shrinking in percentage terms or are otherwise out of line with industry peers

- Unusual reduction in the number of days' purchases in accounts payable ratio
- Reducing accounts payable while competitors are stretching out payments to vendors

Improper Disclosures

Accounting principles require that financial statements include all the information necessary to prevent a reasonably discerning user of the financial statements from being misled. Clearly, this principle is subject to the professional judgment of the accountants and management preparing the financial statements. Events, transactions, and policy changes that are likely to have a material impact on the entity's financial position must be disclosed. The financial statement notes should include narrative disclosures, supporting schedules, and any other information required to avoid misleading potential investors, creditors, or any other users of the financial statements.

Management has an obligation to disclose all significant (material) information appropriately in the financial statements and in management's discussion and analysis. In addition, the disclosed information must not be misleading. Improper disclosures resulting in financial statement fraud usually involve the following:

- Liability omissions
- Subsequent events
- Management fraud
- Related-party transactions
- Accounting changes

Liability Omissions

Typical omissions include the failure to disclose loan covenants or contingent liabilities. Loan covenants are agreements, in addition to or as part of a financing arrangement, that a borrower has promised to keep as long as the financing is in place. The agreements can contain various types of covenants, including certain financial ratio limits and restrictions on other major financing arrangements. Contingent liabilities are potential obligations that will materialize only if certain events occur in the future. A corporate guarantee of personal loans taken out by an officer or a private company controlled by an officer is an example of a contingent liability. Under generally accepted accounting principles, the company's potential liability must be disclosed if it is material.

Subsequent Events

Events occurring or becoming known after the close of the period that could have a significant effect on the entity's financial position must be disclosed. Fraudsters typically avoid disclosing court judgments and regulatory decisions that undermine the reported values of assets, that indicate unrecorded liabilities, or that adversely reflect upon management's integrity. A review of subsequent financial statements, if available, might reveal whether management improperly failed to record a subsequent event that it had knowledge of in the previous financial statements. Public record searches can also help reveal this information.

Management Fraud

Management has an obligation to disclose to the shareholders significant frauds committed by officers, executives, and others in positions of trust. Withholding such information from auditors would likely also involve lying to auditors, an illegal act in itself.

Related-Party Transactions

Related-party transactions occur when a company does business with another entity whose management or operating policies can be controlled or significantly influenced by the company or by some other party in common. There is nothing inherently wrong with related-party transactions, as long as they are fully disclosed. If the transactions are not fully disclosed, the company might injure shareholders by engaging in economically harmful dealings without their knowledge.

The financial interest that a company official might have might not be readily apparent. For example, common directors of two companies that do business with each other, any corporate general partner and the partnerships with which it does business, and any controlling shareholder of the corporation with which he/she/it does business may be related parties. Family relationships can also be considered related parties, such as all direct descendants and ancestors, without regard to financial interests. Related-party transactions are sometimes referred to as *self-dealing*. While these transactions are sometimes conducted at arm's length, often they are not.

EXAMPLE

In September 2002, the U.S. Securities and Exchange Commission (SEC) charged former top executives of Tyco International Ltd., including former CEO L. Dennis Kozlowski, with violating the U.S. securities laws by failing to disclose to shareholders

hundreds of millions of dollars of low-interest and interest-free loans they took from the company, and in some cases, never repaid. The SEC complaint, which also charged former Tyco CFO Mark H. Swartz and Chief Legal Officer Mark A. Belnick, alleges that the three former executives also sold shares of Tyco stock valued at millions of dollars while their self-dealing remained undisclosed. The complaint alleges numerous improper transactions, such as Kozlowski's use of $242 million of loans for unauthorized purposes that included funding an extravagant lifestyle. With these undisclosed loans, Kozlowski allegedly amassed millions of dollars in fine art, yachts, and estate jewelry, as well as a $31 million Park Avenue apartment and a lavish estate in Nantucket. Kozlowski and Swartz allegedly engaged in undisclosed non-arm's-length real estate transactions with Tyco or its subsidiaries and received undisclosed compensation and perquisites, including forgiveness of multimillion-dollar loans, rent-free use of large New York apartments, and use of corporate aircraft for personal purposes at little or no cost.

In July 2004, Belnick was acquitted of all the charges brought against him. In a separate trial, Kozlowski and Swartz were each found guilty of 22 charges, including grand larceny, falsifying business records, conspiracy, and securities fraud, and were sentenced to eight and one-third to 25 years in prison.

Accounting Changes

In general, three types of accounting changes must be disclosed to avoid misleading the user of financial statements: accounting principles, estimates, and reporting entities. Although the required treatment for these accounting changes varies for each type and across jurisdictions, they are all susceptible to manipulation. For example, fraudsters might fail to properly retroactively restate financial statements for a change in accounting principle if the change causes the company's financial statements to appear weaker. Likewise, they might fail to disclose significant changes in estimates such as the useful lives and estimated salvage values of depreciable assets, or the estimates underlying the determination of warranty or other liabilities. They might even secretly change the reporting entity by adding entities owned privately by management or by excluding certain company-owned units to improve reported results.

Backdating Stock Options

As a supplement to salary, companies frequently offer employees stock options, which grant the recipient the privilege to purchase a share of the company's stock at a future date for a specific price called the *strike price*. A strike price is the value of a share at a particular date.

Generally, the strike price is set at the price of the underlying stock on the day the option is granted; therefore, the option becomes valuable only with future increases in the stock price. In this way, companies grant stock options as an incentive for employees to enhance company performance and thus raise the stock price. The practice of backdating stock options, however, gives the employee a chance to profit by purchasing stock at past low prices, providing an immediate payoff. Backdating stock options occurs when a company alters the date of the grant to a time when the stock was trading at a lower price in the interest of making the option instantly valuable and further increasing the employee's gain if the stock price continues to rise.

EXAMPLE

On June 1, 20X1, Company XYZ grants its CEO a stock option that provides the executive the right to purchase 100 shares of XYZ stock on January 1, 20X2 for the strike price. Per its usual policy, the strike price is set at the price of the company stock on the date of the option grant. On June 1, 2008 (the grant date), XYZ stock was trading at $40 per share. Therefore, if the stock price increases to $45 per share by January 1, 20X2, the CEO could exercise the option and purchase the shares for $40 per share, and then sell them immediately on the market for $45 per share, resulting in a gain of $5 per share. However, the company has recently experienced a dramatic increase in its share price. On May 24, 20X1, the stock was trading for $15 per share. To provide the CEO with an opportunity to exploit this increase in share price, the company chooses to backdate the stock options to make it appear that they were granted on May 24, 20X1. Because the strike price is set at the price of the stock on the option grant date, the strike price is effectively changed to $15 per share. As a result, the CEO now has the option to buy 100 shares of XYZ stock on January 1, 20X2 for $15 per share. Thus, the CEO has immediately gained $25 per share (the difference between the stock price on the actual grant date of June 1 and the stated grant date of May 24) based solely on the manipulation of the grant date used.

Backdating is not necessarily illegal, but can be if not handled appropriately. To be legal, the practice typically must be explicitly reported to shareholders and the government; failure to do so could constitute securities fraud. To help address the possibility of this type of illegal activity, auditors should assess the information obtained from the audit to determine if there is a need for further audit procedures to test for stock option backdating.

What Red Flags Are Associated with Improper Disclosures?

The following red flags might indicate improper disclosures:

- Domination of management by a single person or small group (in a nonowner-managed business) without compensating controls
- Ineffective board of directors or audit committee oversight over the financial reporting process and internal control
- Ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management or the communication of inappropriate values or ethical standards
- Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
- Significant, unusual, or highly complex transactions, especially those close to a period's end that pose difficult "substance over form" questions
- Significant related-party transactions not in the ordinary course of business or with related entities either not audited or audited by a different firm
- Significant bank accounts or subsidiary or branch operations in tax-haven jurisdictions for which there appears to be no clear business justification
- Overly complex organizational structure involving unusual legal entities or managerial lines of authority
- Known history of violations of securities laws or other laws and regulations, or claims against the entity, its senior management, or board members alleging fraud or violations of laws and regulations
- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality
- Formal or informal restrictions on the auditor that inappropriately limit access to people or information, or limit the auditor's ability to communicate effectively with the board of directors or audit committee

What Red Flags Are Associated with Financial Statement Fraud in General?

Red flags associated with particular financial statement fraud schemes have been discussed previously. There are many red flags associated with financial statement fraud generally. An extensive list of such red flags can be found in the appendix to both AU Section 240, *Consideration of Fraud in a Financial Statement Audit*, and ISA 240, *The Auditor's Responsibility Relating to Fraud in an Audit of Financial Statements,* where they are called "fraud risk factors."

Some red flags indicate increased vulnerability to financial statement fraud; others indicate a greater likelihood that financial statement fraud has occurred.

Some of the more significant red flags are:

- Domination of management by a single person or small group (in a nonowner-managed business) without compensating controls
- Profitability or trend level expectations of investment analysts, institutional investors, significant creditors, or other external parties (particularly expectations that are unduly aggressive or unrealistic), including expectations created by management in, for example, overly optimistic press releases or annual report messages
- Ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management, or the communication of inappropriate values or ethical standards
- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
- Significant, unusual, or highly complex transactions, especially those close to a period's end that pose difficult "substance over form" questions
- Significant related-party transactions not in the ordinary course of business or with related entities not audited or audited by another firm
- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality
- Formal or informal restrictions on the auditor that inappropriately limit access to people or information, or limit the ability of the auditor to communicate effectively with those charged with governance

Detection of Fraudulent Financial Statement Schemes

To better understand basic accounting concepts and to see how an analysis of accounting records and procedures can reveal a fraud, consider the following example:

EXAMPLE

Jackson Hardware Supply is a medium-sized plumbing and electrical wholesale distributor. On December 31, the balance sheet and income statement were as follows:

Jackson Hardware Supply
Balance Sheet
As of December 31

Assets		Liabilities & Owners' Equities	
Cash	$2,427,000	**Liabilities**	
Accounts Receivable	300,000	Accounts Payable	$ 300,000
Inventory	300,000	Salaries Payable	70,000
Supplies	11,000	Rent Payable	50,000
Prepaid Insurance	44,000	Deferred Taxes Payable	438,000
Equipment	440,000	Total Liabilities	858,000
		Owners' Equities	
		Common Stock	$2,000,000
		Retained Earnings	664,000
		Total Owners' Equity	2,664,000
Total Assets	$3,522,000	Total Liabilities & Owners' Equity	$3,522,000

Jackson Hardware Supply
Income Statement
For the year ending December 31

Revenues		
Sales Revenue	$3,470,000	
Cost of Goods Sold	(2,100,000)	
Gross Profit from Sales	1,370,000	
Rent Revenue	10,000	
Gross Profit		$ 1,380,000
General and Administrative Expenses		
Insurance Expense	$4,000	
Salary Expense	220,000	
Supplies Expense	14,000	
Rental Expense	40,000	
Total General and Administrative Expenses		(278,000)
Net Income Before Taxes		1,102,000
Income Taxes		(438,000)
Net Income		$ 664,000

An anonymous tip was received that the paymaster, a long-time trusted employee, is stealing cash from the company. Lately, he has been seen driving a new BMW and has taken expensive vacations. The president of the company wants to follow up on the tip and asks the fraud examiner to determine if the paymaster has been stealing. Although there are several ways to proceed with the investigation, the fraud examiner with accounting knowledge decides to first compare this year's total salary expense with last year's balance. He theorizes that if the paymaster is dishonest, he might be concealing the theft in the salaries expense account. Past experience has taught the fraud examiner to look in the most obvious place first.

The fraud examiner notes that the balance of $220,000 in the salary expense account this year is significantly larger than the $180,000 balance last year. He asks the owner if there was an increase in the number of employees and how large across-the-board raises were this year. He discovers that the workforce did not increase and all employees, including the owner, received 10 percent raises. He recalculates this year's salaries by increasing last year's salaries 10 percent and determines that the balance in the salary expense account should be approximately $198,000 ($180,000 × 1.10 = $198,000). He now believes that excess salaries went to someone.

The next step is to follow the overstatement in salary expense backward from the income statement through the accounts and journal entries to the source documents—the payroll checks, in this case. He finds that there are 12 checks payable to John Doe, an employee who quit in January of last year. He compares the endorsements on John Doe's checks with those on the paymaster's checks and notices distinct similarities in the signatures. Armed with this evidence, he interviews the paymaster, who confesses that he has stolen $22,000 and concealed the theft by issuing payroll checks to a nonexistent employee, checks that he subsequently endorsed and cashed.

Obviously, this example is relatively simple; but most fraud schemes are simple, especially for a fraud examiner who understands concealment techniques and accounting concepts.

Other detection techniques are available for determining if the paymaster is stealing. These include running a report of all employees who do not elect insurance coverage and other payroll withholdings (withholdings on fictitious employees create additional concealment problems for perpetrators), having someone else distribute the checks, and examining identification numbers of all active employees. Any of these methods might have revealed

the false paychecks to John Doe. The approach shows, however, how an understanding of accounting can be invaluable for detecting fraud.

Financial Statement Analysis

Comparative financial statements provide information for current and past accounting periods. Accounts expressed in whole dollar amounts yield a limited amount of information. The conversion of these numbers into ratios or percentages allows the reader of the statements to analyze them based on their relationship to each other; in addition, it allows the reader to more readily compare current performance with past performance. In fraud detection and investigation, the determination of the reasons for relationships and changes in amounts can be important. These determinations are the red flags that point a fraud examiner in the direction of possible fraud. If large enough, a fraudulent misstatement can affect the financial statements in such a way that relationships between the numbers become questionable. Many schemes are detected because the financial statements do not make sense when analyzed closely. Financial statement analysis includes the following:

- Vertical analysis
- Horizontal analysis
- Ratio analysis

Vertical Analysis

There are traditionally two methods of percentage analysis of financial statements: horizontal and vertical analysis. *Vertical analysis* is a technique for analyzing the relationships among the items on an income statement, balance sheet, or statement of cash flows by expressing components as percentages of a specified base value. This method is often referred to as *common sizing* financial statements because it allows an analyst to compare entities of different sizes more easily. In the vertical analysis of an income statement, net sales is the base value and is assigned 100 percent. On the balance sheet, total assets is assigned 100 percent on the asset side, and total liabilities and equity are expressed as 100 percent. All other items in each of the sections are expressed as a percentage of these numbers.

Vertical analysis emphasizes the relationship of statement items within each accounting period. These relationships can be used with historical averages to determine statement anomalies.

Horizontal Analysis

Horizontal analysis is a technique for analyzing the percentage change in individual financial statement line items from one period to the next. The first period in the analysis is considered the base period, and the changes in the subsequent period are computed as a percentage of the base period. If more than two periods are presented, each period's changes are computed as a percentage of the preceding period. The resulting percentages are then studied in detail. As is the case with vertical analysis, this technique does not work for small, immaterial frauds.

The following is an example of financial statements that are analyzed using both horizontal and vertical analysis:

BALANCE SHEET	Vertical Analysis				Horizontal Analysis	
	Year One		Year Two		Change	%Change
Assets						
Current Assets						
Cash	45,000	14%	15,000	4%	(30,000)	-67%
Accts Receivable	150,000	45%	200,000	47%	50,000	33%
Inventory	75,000	23%	150,000	35%	75,000	100%
Fixed Assets (net)	60,000	18%	60,000	14%	-	0%
Total	330,000	100%	425,000	100%	95,000	29%
Acc'ts Payable	95,000	29%	215,000	51%	120,000	126%
Long-term Debt	60,000	18%	60,000	14%	-	0%
Stockholder's Equity					-	
Common Stock	25,000	8%	25,000	6%	-	0%
Paid-in Capital	75,000	23%	75,000	18%	-	0%
Retained Earnings	75,000	23%	50,000	12%	(25,000)	-33%
Total	330,000	100%	425,000	100%	95,000	29%

INCOME STATEMENT	Vertical Analysis				Horizontal Analysis	
	Year One		Year Two		Change	%Change
Net Sales	250,000	100%	450,000	100%	200,000	80%
Cost of Goods Sold	125,000	50%	300,000	67%	175,000	140%
Gross Margin	125,000	50%	150,000	33%	25,000	20%
Operating Expenses						
Selling Expenses	50,000	20%	75,000	17%	25,000	50%
Administrative Expenses	60,000	24%	100,000	22%	40,000	67%
Net Income	15,000	6%	(25,000)	-6%	(40,000)	-267%
Additional Information						
Average Net Receivables	155,000		210,000			
Average Inventory	65,000		130,000			
Average Assets	330,000		425,000			

In the example, we can observe that accounts payable makes up 29 percent of total liabilities in Year One. Historically, we might find that this account averages slightly over 25 percent of total liabilities. In Year Two, accounts payable, as a percentage of total liabilities, increased to 51 percent. Although this increase might be explainable through a correlation with a rise in sales, such a significant increase could also be the starting point of a fraud examination.

Source documents should be examined to determine the reason for the rise in this percentage. With this type of examination, fraudulent activity might be detected. The same type of change can be seen as selling expenses decline as a percentage of sales in Year Two from 20 percent to 17 percent. Again, this change might be explainable, but close examination could point a fraud examiner to uncover fictitious sales since there was not a corresponding increase in selling expenses.

It is important to consider the dollar amount of change as well as the percentage when conducting a horizontal analysis. A 5 percent change in an account with a very large dollar amount could actually be much more of a change than a 50 percent change in an account with much less activity.

In the example, it is obvious that the 80 percent increase in sales has a much greater corresponding increase in cost of goods sold, which rose 140 percent. These accounts are often used to hide fraudulent expenses, withdrawals, or other illegal transactions.

Ratio Analysis

Ratio analysis is a means of measuring the relationship between two different financial statement amounts. The relationship and comparison are the keys to the analysis. Many professionals, including bankers, investors, and business owners, as well as major investment firms, use this method. Ratio analysis allows for internal evaluations using financial statement data. Traditionally, financial statement ratios are compared to an entity's industry averages. The ratios and comparisons can be very useful in detecting red flags for a fraud examination.

If the financial ratios present a significant change from one year to the next or over a period of years, it becomes obvious that there could be a problem. As in all other analyses, specific changes are often explained by changes in the business operations. If a change in specific ratios is detected, the appropriate source accounts should be researched and examined in detail to determine if fraud has occurred. For instance, a significant decrease in a company's current ratio might point to an increase in current liabilities or a reduction in assets, both of which could be used to cover fraud.

In financial statement analysis, each reader of a statement will determine which portions are most important. Like the financial statement analysis discussed previously, the analysis of ratios is limited by its inability to detect fraud on a smaller, immaterial scale. Some of the types of financial ratio comparisons are shown in the following section.

Many of the possible ratios are used in industry-specific situations, but the nine comparisons described here are ratios that might lead to the discovery of fraud. The following calculations are based on the financial statement example presented earlier:

Common Financial Ratios

CURRENT RATIO

$$\frac{\text{Current Assets}}{\text{Current Liabilities}}$$

The current ratio—current assets to current liabilities—is probably the most commonly used ratio in financial statement analysis. This comparison measures a company's ability to meet present obligations from its liquid assets. The number of times that current assets exceed current liabilities has long been a quick measure of financial strength.

In detecting fraud, this ratio can be a prime indicator that the accounts involved have been manipulated. Embezzlement will cause the ratio to decrease, and liability concealment will cause a more favorable ratio.

In the case example, the drastic change in the current ratio from Year One (2.84) to Year Two (1.70) should cause a fraud examiner to look at these accounts in more detail. For instance, a check-tampering scheme will usually result in a decrease in cash, a current asset, which will in turn decrease the ratio.

QUICK RATIO

$$\frac{\text{Cash+Securities+Receivables}}{\text{Current Liabilities}}$$

The quick ratio, often referred to as the acid test ratio, compares the most liquid assets to current liabilities. This calculation divides the total of cash, securities, and receivables by current liabilities to yield a measure of a company's ability to meet sudden cash requirements. The quick ratio is a conservative measurement of liquidity that is often used in turbulent economic times to provide an analyst with a worst-case scenario of a company's working capital situation.

A fraud examiner will analyze the quick ratio for fraud indicators. In Year One of the example, the company balance sheet reflects a quick ratio of 2.05. This ratio drops to 1.00 in Year Two. In this situation, a closer review of accounts receivable shows it is increasing at an unusual rate, which could indicate that fictitious accounts receivable have been added to inflate sales. Of more concern, perhaps, is the increase in accounts payable, which at a minimum might require a closer review to determine why this increase took place.

ACCOUNTS RECEIVABLE TURNOVER

$$\frac{\text{Net Sales on Account}}{\text{Average Net Receivables}}$$

Accounts receivable turnover is defined as net sales on account divided by average net receivables. It measures the number of times accounts receivable is turned over during the accounting period. In other words, it measures the time between on-account sales and collection of funds. This ratio is one that uses both income statement and balance sheet accounts in its analysis. If the fraud includes fictitious sales, this fraudulent income will never be collected. As a result, the turnover of receivables will decrease.

COLLECTION RATIO

$$\frac{365}{\text{Receivable Turnover}}$$

Accounts receivable aging is measured by the collection ratio. It divides 365 days by the receivable turnover ratio to arrive at the average number of days to collect receivables. In general, the lower the collection ratio, the faster receivables are collected. A fraud examiner might use this ratio as a first step in detecting fictitious receivables or larceny and skimming schemes. Normally, this ratio will stay fairly consistent from year to year, but changes in billing policies or collection efforts could cause a fluctuation. The example shows a favorable reduction in the collection ratio from 226.3 in Year One to 170.33 in Year Two. This means that the company is collecting its receivables more quickly in Year Two than in Year One.

INVENTORY TURNOVER

$$\frac{\text{Cost of Goods Sold}}{\text{Average Inventory}}$$

The relationship between a company's cost of goods sold and average inventory is shown through the inventory turnover ratio. This ratio measures the number of times inventory is sold during the period. This ratio is a good determinant of purchasing, production, and sales efficiency. In general, a higher inventory turnover ratio is considered more favorable. For example, if cost of goods sold has increased due to theft of inventory (ending inventory has declined, but not through sales), then this ratio will be abnormally high. In the case example, inventory turnover increases in Year Two, signaling the possibility that an embezzlement is buried in the inventory account. A fraud examiner should investigate the changes in the ratio's components to determine where to look for possible fraud.

AVERAGE NUMBER OF DAYS INVENTORY IS IN STOCK

$$\frac{365}{\text{Inventory Turnover}}$$

The average number of days inventory is in stock ratio is a restatement of the inventory turnover ratio expressed in days. This rate is important for several reasons. An increase in the number of days that inventory stays in stock causes additional expenses, including

storage costs, risk of inventory obsolescence, and market price reductions, as well as interest and other expenses incurred due to tying up funds in inventory stock. Inconsistency or significant variance in this ratio is a red flag for fraud investigators. Fraud examiners might use this ratio to examine inventory accounts for possible larceny schemes. Purchasing and receiving inventory schemes can affect the ratio. Understating the cost of goods sold will result in an increase in the ratio as well. Significant changes in the inventory turnover ratio are good indicators of possible fraudulent inventory activity.

DEBT-TO-EQUITY RATIO

$$\frac{\text{Total Liabilities}}{\text{Total Equity}}$$

The debt-to-equity ratio is computed by dividing total liabilities by total equity. This ratio is one that is heavily considered by lending institutions. It provides a clear picture of the relative risk assumed by the creditors and owners. The higher the ratio, the more difficult it will be for the owners to raise capital by increasing long-term debt. Debt-to-equity requirements are often included as borrowing covenants in corporate lending agreements. The example displays a very favorable Year One ratio of 0.89. Year Two, however, shows a ratio of 1.84, which indicates that debt is greatly increasing. In this case, the increase in the ratio corresponds with the rise in accounts payable. Sudden changes in this ratio might signal a fraud examiner to look for fraud.

PROFIT MARGIN

$$\frac{\text{Net Income}}{\text{Net Sales}}$$

The profit margin ratio is defined as net income divided by net sales. This ratio is often referred to as the efficiency ratio in that it reveals profits earned per dollar of sales. This percentage of net income to sales relates not only the effects of gross margin changes, but also changes to sales and administrative expenses. As fraud is committed, net income will be artificially overstated, and the profit margin ratio will be abnormally high. False expenses and fraudulent disbursements will cause an increase in expenses and a decrease in the profit margin ratio. Over time, this ratio should be fairly consistent.

ASSET TURNOVER

$$\frac{\text{Net Sales}}{\text{Average Total Assets}}$$

The asset turnover ratio is used to determine the efficiency with which assets are used during the period. The asset turnover ratio is typically calculated by dividing net sales by average total assets (net sales / average total assets). However, average operating assets can also be used as the denominator (net sales / average operating assets). The case example displays a greater use of assets in Year Two than in Year One.

By performing a financial statement analysis, the fraud examiner might be directed toward the direct evidence to resolve an allegation of fraud. After the analysis, the fraud examiner can select statistical samples in the target account and eventually examine the source documents. If an irregularity of overstatement is suspected, the fraud examiner should begin the examination with the financial statements. If, however, an irregularity of understatement is suspected, the fraud examiner should begin the examination with a review of the source documents. This rule of thumb is especially effective in the area of omission of liabilities, such as litigation, contingent liabilities, leases, and some product warranties.

The asset turnover ratio is one of the more reliable indicators of financial statement fraud. A sudden or continuing decrease in this ratio is often associated with improper capitalization of expenses, which increases the denominator without a corresponding increase in the numerator.

Inflating revenue is the most common form of financial statement fraud. But, overstated sales most often are accompanied by inflated assets (e.g., phony accounts receivable). This adds equal amounts to both the numerator and denominator of the total asset turnover, which affects the ratio, but not as strongly as when just a numerator or denominator are affected. Accordingly, increases in the total asset turnover have less of a correlation with overstatement of sales than do decreases with false capitalization of costs.

Tax Return Review

Tax returns are good sources of additional and comparative information on the business's operations. A complete review and comparison to the financial statement could provide information unknown to the lender or disclose unexplained discrepancies. Again, the lack of properly prepared or timely filed tax returns could be a method of stalling by not providing the required information. Most perpetrators of fraud are reluctant to continue the deception and falsify a tax return. Year-after-year extensions and filing of the tax returns on the last possible date could be a ploy to cover up financial statement and tax return differences.

Interviews in Fraudulent Financial Statement Cases

For in-depth interviewing techniques, refer to the "Interview Theory and Application" chapter in the Investigation section of the *Fraud Examiners Manual*.

Financial statement fraud does not occur in an isolated environment. People in organizations who have both motive and opportunity are the prime candidates to commit fraudulent misstatement. In the overwhelming majority of situations, two key managers participate actively in the fraud: the chief executive officer and the chief financial officer. Others become involved largely out of necessity. Those who are not directly involved most often are not aware that anything is wrong.

Investigations of financial statement frauds are unique in that they almost always involve interviewing the executive management of the organization. To detect or deter financial statement fraud, it is absolutely necessary that top management be interviewed by a competent and experienced fraud examiner who possesses the ability to solicit honest answers to tough—but vital—questions about whether anyone has tampered with the books.

Interviewing Techniques

Situations in which accountants are tempted to misstate financial statements most often involve pressure connected with financial performance. The following is a fictitious conversation between upper managers of a corporation. The example shows how the pressure to commit financial statement fraud can greatly influence accounting personnel.

> *CFO: (To CEO) "Boss, it looks like we will not have a good year financially. We told the shareholders (or bank) that our earnings would be $4 a share, and it looks like we'll be very lucky to even make $3."*
>
> *CEO: "Well, what are we going to do about it? If we miss the earnings projections (or don't get the loan) it won't look good for the company; we'll both lose our jobs. We must get those earnings up to where they should be."*
>
> *CFO: "What do you mean?"*
>
> *CEO: "What I mean is that it is your job to bring in the numbers. You're going to have to find a way to get them up. I'm sure we can probably make up the difference next year, but for now, you get our earnings/assets/equity up however you have to. All financial statements are essentially estimates anyhow. So you figure out how to 'estimate' the numbers more in our favor. I don't know how to do it, and I don't want you to tell me. But get it done."*

The CFO faces a dilemma: cook the books or lose his job. The CFO's actions are very hard to predict. If he steps over the edge, chances are he will need to enlist the aid of accounting and clerical personnel to carry out the details, even if these employees do not know what they are actually doing. For example, the CFO might tell the chief accountant to book certain receivables and income, which would produce the needed effect—pumping up the equity. Such a scheme might only be apparent to the real insiders.

To detect financial statement frauds through interviews, management and key support staff must be interviewed. Fraud examiners and auditors (collectively referred to as "examiners") must consider many important issues when conducting interviews. One important issue examiners should keep in mind is that there is generally no liability in asking questions in which they have a legitimate interest, no matter how insulting the questions might be to the respondents. Examiners, therefore, have the legal right to be fearless in asking questions, as long as the questions are asked privately and under reasonable circumstances. This legal right doesn't extend to accusations—only to questions. "Are you still cooking the books?" is an accusation, whereas, "Are you cooking the books?" is a question. It is important to know the difference and to frame questions accordingly.

Examiners should also be sure to interview only one person at a time. Groups of people should not be interviewed together because members tend to influence each other. The interviews should always be conducted under private conditions, which permit the respondent to answer candidly.

It is important that examiners aim to be nonthreatening in their interview approaches. The less threatening the interviewer appears, the less reluctant the respondent will be to answer questions. An interviewer should not be judgmental or show surprise or disgust; such actions can inhibit the flow of information.

Examiners should warm up respondents thoroughly before asking sensitive questions. It is best to obtain all of the procedural information and information pertaining to internal controls prior to discussing fraud. Fraud should usually be the last thing covered in an interview.

To reduce the possibility of offending respondents, examiners can explain the nature of their interest before asking sensitive questions. For example, an examiner can say, "As you know, as an auditor, I am required to actively look for fraud. This means I must ask you some

direct questions about the subject. Do you understand?" Then, after obtaining a positive response, the examiner can proceed to ask questions about fraud. It is best to ask the least difficult questions first.

Another approach examiners can take to make tough interview questions more palatable is to phrase them hypothetically, especially during the beginning of the interview. For example, rather than asking a chief financial officer, "Have you committed fraud?" an examiner can say to the executive, "Suppose someone in the position of chief financial officer decided to increase the financials. How would he do it?" The latter question is far more likely to elicit specific information than the former. Later in the interview, the executive should be asked specifically if he has committed the fraud. The examiner can say something along the lines of "My professional responsibilities require me to ask you one particularly sensitive direct question. Have you committed fraud or other illegal acts against the company?" The vast majority of respondents will answer "No" to such a question without hesitation, whether they have or not; however, simply asking the question places the examiner in a much more favorable position if attacked professionally for not detecting a fraud.

The Interview

Fraud examiners and auditors should ask questions designed to elicit the most specific information possible in a professional manner.

THE CHIEF EXECUTIVE OFFICER

Generally, the CEO should be interviewed first in any proactive or reactive fraud situation. There are several good reasons for this approach. First of all, the auditor or fraud examiner must have a thorough understanding with management as to what his responsibilities in this area are. Second, it is unwise to conduct sensitive inquiries within any organization without first advising the CEO. If he learns from some other source that you are making discreet fraud-related inquiries without telling him, he is more likely to misunderstand your objectives and take the inquiry as a personal affront. Third, if there is any significant cooking of the books, the CEO is almost always involved. The fraud-related questions you should ask in connection with a regular audit should include the following, at a minimum. Note how the questions are for "set up" purposes.

1. *Mr. CEO, as you know, we are required to assess the risk that material fraud exists in every company, not just yours. This is sort of a sensitive area for everyone, but our professional responsibilities dictate that we address this area. Do you understand? (Wait for an affirmative response before proceeding.)*

2. *Do you have any reason to believe that material fraud is being committed at any level within the organization?*

3. *Mr. CEO, one trend in fraud is that small frauds are committed by employees with little authority, which means that the largest ones are usually committed with upper management's knowledge. Do you understand that? (Wait for an affirmative response before proceeding.)*

4. *Because of that, we are required to at least look at the possibility that all CEOs, including you, might commit significant fraud against customers, investors, or shareholders. Do you understand our situation? (Wait for an affirmative response.)*

5. *So during this audit (examination) we need to ask direct questions about this subject to you and your staff. As a matter of fact, we will at least discuss the possibility of fraud with every employee we talk with in connection with this audit (examination). Do you have any problem with that? (Wait for a negative response. If the CEO protests, satisfy his objections. If he cannot be satisfied, assess the risk of whether the CEO is attempting to obstruct the audit or examination.)*

6. *First, let's look at your CFO. Can you think of a reason he might have to get back at you or the company by committing fraud?*

7. *Has the CFO ever asked you to approve any financial transaction you thought might be improper or illegal?*

8. *Do you know whether the CFO has any outside business interests that might conflict with his duties here?*

9. *Does the CFO employ any friends or relatives in the company? (Look for possible conflicts or sweetheart deals.)*

10. *What information do you have about the CFO's lifestyle? (Look for expensive homes, cars, toys, and habits.)*

11. *What is your general impression of how the CFO gets along with his staff? (Look for abuses of authority, etc., that would motivate employees directly below the CFO to participate in fraud.)*

12. *How do you think fraud in your company compares with others in the same industry?*

13. *Of course, Mr. CEO, I must ask you many of the same questions about yourself. Is there any reason that anyone below you might claim you are committing fraud against the company?*

14. *I must also ask you some personal financial questions. Do you have any problem with this? (Wait for a negative response.)*

15. *Please give me a current estimate of your personal assets, liabilities, income, and expenses. (List.) What percentage of your net worth is tied directly to this company? (Look for highly leveraged individuals whose company holdings are a significant portion of their net worth.)*

16. *Are you currently experiencing any personal financial problems? (Look for lawsuits, liens, judgments, or other indicators.)*

17. *Do you have friends or relatives working for this company? (Look for conflicts of interest.)*

18. *Do you have friends or relatives working for major suppliers or vendors to this company? (Look for conflicts of interest.)*

19. *Do you own any portion of a company that does business with this organization? (Look for conflicts of interest.)*

20. *Hypothetically, if you wanted to pump up your company's profits, what would be the easiest way to do it?*

21. *As I said, we will be required to ask many questions of your staff. Is there any reason why someone who works for you would say you are at risk to commit significant fraud against the company or its shareholders?*

22. *Mr. CEO, this is the last question, and it should be obvious why I have to ask it. Have you committed fraud or other illegal acts against the company? (Do not apologize for asking the question; it's your job.)*

THE CEO'S TOP STAFF

CEOs of corporations, large and small, are busy individuals. Because they tend to be "big picture" people by nature, they rely heavily on their staffs—principally their personal assistants—to take care of details. But personal assistants do not usually become closely tied to the boss without a demonstrated history of loyalty and discretion. In short, if you make the boss's assistant mad, your fraud-related questions are going to be interpreted in the worst possible light, thereby making your job much more difficult.

So the key to interviewing the CEO's top staff is to approach the interviewing process correctly from the outset. This means laying a great deal of groundwork before asking sensitive questions. Start with procedural matters or some other non-sensitive topic, and ask the fraud-related questions toward the end of your conversation.

1. *Mr. Assistant, part of my job as an auditor (fraud examiner) is to assess the risk that the company's books are not materially correct as a result of fraud by employees or management. I have already talked about these issues with your boss. He understands their importance and is aware that, as part of the audit, I will be talking to everyone about the subject to some extent. Do you have any problem with this? (Wait for a negative response.)*

2. *Do you think fraud is a problem for business in general? (Icebreaker.)*

3. *How do you think this company stacks up to others in terms of its employees' and managers' honesty?*

4. *Have you ever heard rumors in the company that someone is committing fraud, especially someone high up in the organization?*

5. *Is the company in any kind of financial trouble that would motivate management to misstate the company's profits?*

6. *Do you think your coworkers are essentially honest?*

7. *Has anyone you work with ever asked you to do something you felt was not legal or ethical?*

8. *How would you handle such a situation? (Solicit information on the company's fraud reporting program.)*

9. *If someone in a position of authority in the company wanted to commit fraud, what would be the easiest way to do it?*

10. *As your auditor, may I ask you to report any instances in the future of anyone asking you to do anything to the books and records that you feel is not right? (Solicit future cooperation.)*

THE CHIEF FINANCIAL OFFICER

In the vast majority of cases, the CFO is an integral part of any financial statement fraud, as was illustrated previously. As a result, the interview with the CFO should concentrate not only on possible motivations to commit fraud, but also on the opportunity to do so. Since most CFOs are accountants, they should more readily understand your fraud-related mission. This can be good or bad; good if the CFO is honest, and bad if he isn't. Among all financial personnel, the CFO is in the best position to know how to cook the books and keep it from being uncovered. As if that weren't enough, many CFOs are hired directly from the firms that audit the company. Is there any other person more likely to be at the center of the fraud?

The following are recommended fraud-related questions for a company's CFO.

1. *Mr. CFO, you now know that audit standards require us to actively assess the risk that material fraud could be affecting the financial statements. We have talked with the CEO, and he is fully aware that we will be asking most everyone we speak with about the possibility of fraud or irregularities. You understand this, don't you? (Wait for an affirmative response.)*

2. *Of the accounts on the company's books, which do you suspect might be the most vulnerable to manipulation, and why?*

3. *What kind of history does the company have with fraud in general, including defalcations and employee thefts? (Look for signs of a weak corporate culture.)*

4. *We know that fraud usually exists to some extent—even if it is small—in most companies. How do you think your company compares to others?*

5. *What is your overall impression of the company's ethics and corporate culture?*

6. *During our assessment of fraud risk in your company, are there any specific areas you'd like to discuss with us?*

7. *Is there any reason that anyone in the company might say that management had a motive to misstate the financials?*

8. *Has anyone you work with ever asked you to do anything with the books that you thought was questionable, unethical, or illegal?*

9. *Are you involved in the personal finances of the CEO? If so, is there anything about them that might make you think he is under personal financial pressure?*

10. *Do either the CEO's lifestyle or habits give you any reason to think he might be living beyond his means?*

11. *Has anyone in a position of authority ever asked that you withhold information from the auditors, alter documents, or make fictitious entries in the books and records?*

12. *Is there anything about your own background or finances that would cause someone to suspect that you had a motive for committing fraud?*

13. *Because of your importance as CFO, I must ask you one final question: Have you, yourself, committed fraud or illegal acts against this company? (Remember—don't apologize.)*

THE ACCOUNTING STAFF

If a financial statement fraud has been ordered by the CFO, he will either do the actual dirty work himself or get his staff to do it. In some cases, the staff will understand the big picture, but in most situations, the employee is told only what he needs to know. It is uncommon for a CFO to share with a lower staff person the fact that he is cooking the books.

As a result, the fraud examiner generally must complete his audit work before beginning the interviews of the accounting staff. This will allow specific transactions to be discussed with the people who actually entered them into the company's records. For example, all thorough audits will examine the major journal entries. Frequently, these journal entries will be ordered by the CFO, but actually entered by a staff member. There would generally be no record of the CFO requesting the entry, so this fact must be established through interviews.

Interviews of the accounting staff will allow for sufficient examination of procedures and controls over assets. After these questions are answered, you can generally pursue the line of inquiry suggested previously for the CEO's assistant.

It should be noted that there are similarities and differences in the questions asked of the CEO, the CFO, and their staffs. In the case of the CEO and the CFO, both were specifically asked if they had committed fraud against the company, although in a nice way. The staffers were not asked that specific question.

The reasoning is this: significant financial statement fraud, as previously stated, generally originates with one or both of these two executives. Staffers have less motivation to engage in financial statement fraud and are, therefore, at less risk to do so. They are also less likely to have the financial authority to enter transactions into the books without higher approval.

So absent any specific information to the contrary, asking the employees point blank if they have committed fraud is less likely to produce information and more likely to offend them. But with the CFO and the CEO, asking the direct question will add measurably to the prevention of fraud. There are few defenses to not asking the question, other than the possibility of embarrassing the executives you are auditing. That will, of course, sound rather weak in a court of law where you are fighting for your professional life.

Prevention of Financial Statement Fraud

Prevention and deterrence of financial statement fraud consists of those actions taken to discourage the perpetration of fraud and limit the exposure if fraud does occur. Since financial statements are the responsibility of management, preventing financial statement fraud requires minimizing the pressures, incentives, and opportunities unique to management for manipulating the company's financial position.

Management and the Board of Directors

Financial statements are management's presentation of the financial position of the entity. Setting the ethical tone of the organization is the responsibility of management and the board of directors. As with other types of occupational fraud and abuse, reducing the three factors that contribute to fraud (the fraud triangle) as they specifically relate to management and the board can mitigate the risk of financial statement fraud. Reducing existing pressures to commit fraud, removing potential opportunities to commit fraud, and

relieving possible rationalizations for committing fraud will greatly aid in the prevention of financial statement fraud.

Reduce the Situational Pressures that Encourage Financial Statement Fraud

- Avoid setting unachievable financial goals.
- Eliminate external pressures that might tempt accounting personnel to prepare fraudulent financial statements.
- Remove operational obstacles that block effective financial performance, such as working capital restraints, excess production volume, or inventory restraints.
- Establish clear and uniform accounting procedures that do not contain exception clauses.

Reduce the Opportunity to Commit Fraud

- Maintain accurate and complete internal accounting records.
- Carefully monitor the business transactions and interpersonal relationships of suppliers, buyers, purchasing agents, sales representatives, and others who interface in the transactions between financial units.
- Establish a physical security system to secure company assets, including finished goods, cash, capital equipment, tools, and other valuable items.
- Segregate duties between employees, ensuring that no single individual has total control of one area.
- Maintain accurate personnel records, including background checks (where permitted by law) on new employees.
- Encourage strong supervisory and leadership relationships within groups to ensure enforcement of accounting procedures.

Reduce the Rationalization of Fraud—Strengthen Employee Personal Integrity

- Managers should set an example by promoting honesty in the accounting area. It is important that management practice what it preaches. Dishonest acts by management, even if they are directed at someone outside of the organization, create a dishonest environment that can spread to other business activities and other employees, both internal and external.
- Honest and dishonest behavior should be defined in company policies. Organizational accounting policies should clear up any ambiguity in accounting procedures.
- The consequences of violating the rules, including the punishment of violators, should be clear.

Internal Auditors

Internal auditors are responsible for helping to deter fraud by examining and evaluating the adequacy and effectiveness of controls, along with the extent of the potential exposure in the various segments of an entity's operations. The internal auditing standards state that the principal mechanism for deterring fraud is internal control. Primary responsibility for establishing and maintaining internal control rests with management. The Treadway Commission addresses this issue by recommending that internal audit departments or staffs have not only the support of top management, but also the necessary resources available to carry out their mission. The internal auditors' responsibility is to aid management in the deterrence of fraud by evaluating the adequacy and effectiveness of the company's internal control system, as well as the company's potential exposure to fraud, with particular consideration given to the five elements of internal control laid out by the Committee of Sponsoring Organizations (COSO). The five elements of internal control are discussed in more detail in the Fraud Prevention and Deterrence section of the *Fraud Examiners Manual*.

External Auditors

External auditors inspect clients' accounting records and independently express an opinion as to whether financial statements are presented fairly in accordance with the applicable accounting standards of the entity, such as GAAP or IFRS. They must assert whether financial statements are free of material misstatement, whether due to error or fraud.

Independence is the cornerstone of the auditing function. The only way external auditors can uncover and rectify instances of fraud is if they view the financial statements objectively. However, external auditors are not required to uncover all instances of fraud that might be occurring, as this would be a difficult and nearly impossible task.

The responsibilities of the external auditor as they relate to fraud detection are clearly outlined in International Standard on Auditing (ISA) 240, *The Auditor's Responsibility Relating to Fraud in an Audit of Financial Statements*. According to this guidance:

> *the auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this [standard] are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement.*

Audited financial statements are examined by a variety of external users, including investors, creditors, and government bodies. These users depend on the integrity of the statements for a variety of decision-making purposes. Therefore, external auditors have a professional obligation to evaluate the financial statements as thoroughly and objectively as possible. Furthermore, if management and the accountants know that external auditors conduct sensible audits, they might be deterred from committing financial statement fraud.

ASSET MISAPPROPRIATION: CASH RECEIPTS

Asset misappropriations are by far the most common of all occupational frauds. There are three major categories of asset misappropriation schemes. Cash receipts schemes are discussed in this section, fraudulent disbursements of cash are addressed in the next section, and the following section covers schemes involving the theft of inventory and other noncash assets.

Cash is the focal point of most accounting entries. Cash, both on deposit in banks and on hand as petty cash, can be misappropriated through many different schemes. These schemes can be either on-book or off-book, depending on where they occur.

Cash receipts schemes fall into two categories: *skimming* and *larceny*. The difference in the two types of fraud depends completely on when the cash is stolen. Cash larceny is the theft of money that has *already appeared* on a victim organization's books, while skimming is the theft of cash that has *not yet been recorded* in the accounting system. The way in which an employee extracts the cash might be exactly the same for a cash larceny or skimming scheme.

Skimming

Skimming is the removal of cash from a victim entity prior to its entry in an accounting system. Employees who skim from their companies steal sales or receivables before they are recorded in the company books. Skimming schemes are known as *off-book frauds*, meaning cash is stolen before it is recorded in the victim organization's accounts. This aspect of skimming schemes means they leave no direct audit trail. Because the stolen funds are never recorded, the victim organization might not be aware that the cash was ever received. Consequently, it can be difficult to detect that the cash has been stolen. This is the primary advantage of a skimming scheme to the fraudster.

Skimming is one of the most common forms of occupational fraud. It can occur at any point where cash enters a business, so almost anyone who deals with the process of receiving cash might be in a position to skim money. This includes salespeople, tellers, waitpersons, and others who receive cash directly from customers.

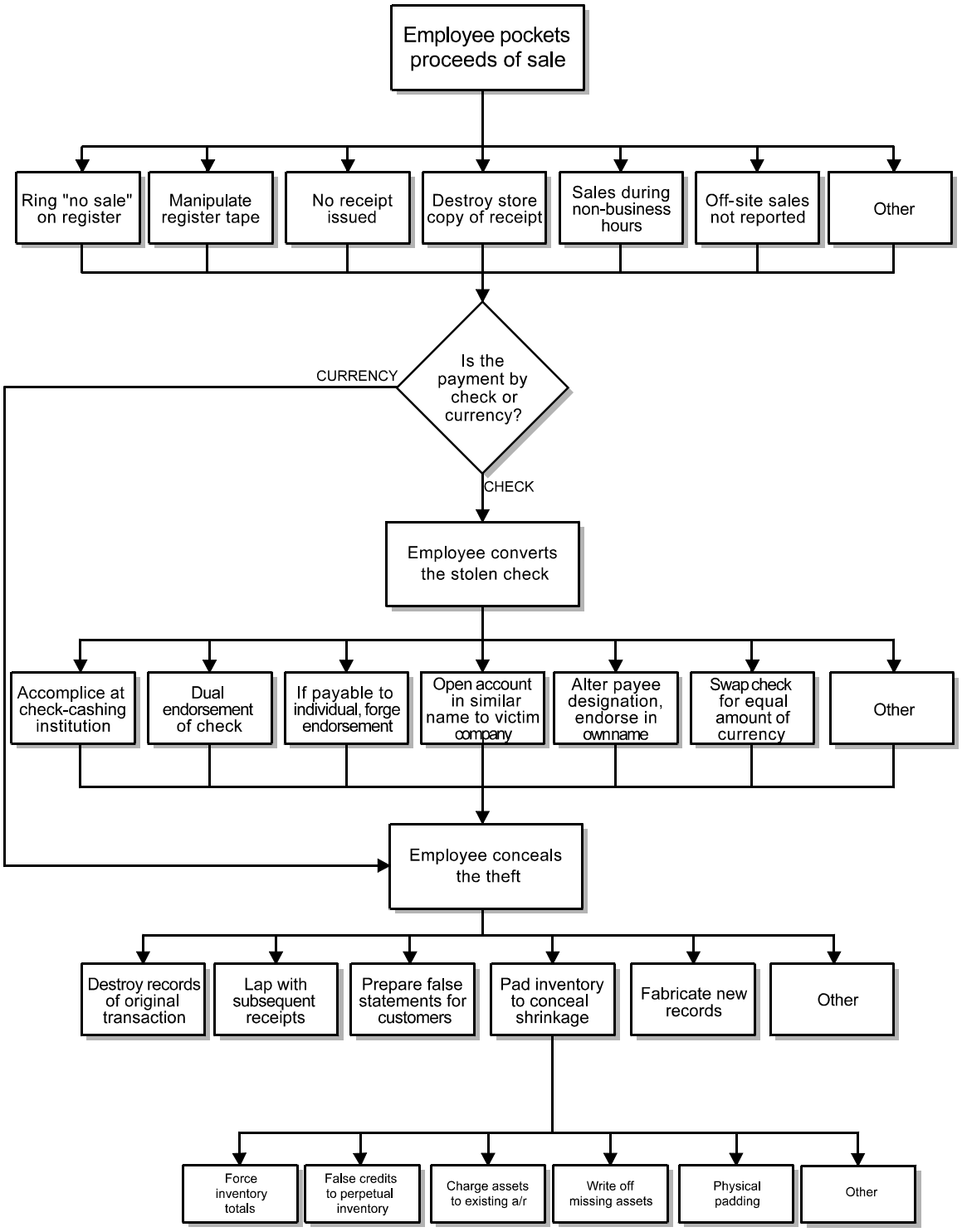
In addition, many skimming schemes are perpetrated by employees whose duties include receiving and logging payments made by customers through the mail. These employees slip customer payments out of the incoming mail instead of posting the payments to the proper revenue or receivables accounts. Those who deal directly with customers or who handle customer payments are obviously the most likely candidates to skim funds.

Sales Skimming

The most basic skimming scheme occurs when an employee sells goods or services to a customer and collects the customer's payment, but makes no record of the sale. The employee simply pockets the money received from the customer instead of turning it over to his employer. (See the "Unrecorded Sales" flowchart.)

Consider one of the simplest and most common sales transactions: a sale of goods at the cash register. In a normal transaction, a customer purchases an item and an employee enters the sale on the register. The register log reflects that the sale has been made and shows that a certain amount of cash (the purchase price of the item) should have been placed in the register. By comparing the register log to the amount of money on hand, it might be possible to detect thefts. For instance, if there were $500 worth of sales recorded on a particular register on a given day, but only $400 cash in the register, it would be obvious that someone had stolen $100 (assuming no beginning cash balance).

If the employee is skimming money, however, it will be impossible to detect theft simply by comparing the register log to the cash drawer. Returning to the example in the previous paragraph, assume that an employee wants to steal $100. Throughout the course of the day, there is $500 worth of sales at his register; one sale is for $100. When the $100 sale is made, the employee does not record the transaction on his register. The customer pays $100 and takes the merchandise home, but instead of placing the money in the cash drawer, the employee pockets it. To create the appearance that the sale is being entered in the register, the employee might ring a "no sale" or some other noncash transaction. Since the employee did not record the sale, at the end of the day, the register log will only reflect $400 in sales. There will be $400 on hand in the register ($500 in total sales minus the $100 that the employee stole), so the register will balance. Thus, by not recording the sale, the employee is able to steal money without the missing funds appearing on the books. Of course, the theft will show up indirectly in the company's records as inventory shrinkage. But the books will provide no direct evidence of the theft.



Unrecorded Sales

The most difficult part in skimming at the register is that the employee must commit the overt act of taking money. If the employee takes the customer's money and shoves it into his pocket without entering the transaction on the register, the customer will probably suspect that something is wrong and might report the conduct to another employee or a manager. It is also possible that a manager, a fellow employee, or a surveillance camera will spot the illegal conduct. Therefore, it is often desirable for a perpetrator to act as though he is properly recording a transaction while he skims sales.

Register Manipulation

Some employees might ring a "no sale" or other noncash transaction to mask the theft of sales. The false transaction is entered on the register so that it appears that a sale is being made. The perpetrator opens the register drawer and pretends to place the cash he has just received in the drawer, but in reality he pockets it. To the casual observer, it looks as though the sale is being properly recorded.

Some employees might also rig their registers so that a sale can be entered on the register keys, but will not appear on the register logs. The employee can then safely skim the sale. Anyone observing the employee will see the sale entered, the register drawer open, etc., yet the register log will not reflect the transaction.

EXAMPLE

A service station employee hid stolen gasoline sales by simply lifting the ribbon from the printer on his register. He collected and pocketed the sales, which were not recorded on the register log. The fraudster would then roll back the tape to the point where the next transaction should appear and replace the ribbon. The next transaction would be printed without leaving any blank space on the tape, apparently leaving no trace of the fraud.

When the ribbon is removed from the register, the result is a blank space on the register log where the skimmed sale should have been printed. Unusual gaps between transactions on a register log might mean that someone is skimming sales.

Fraudsters will often manually roll back the tape when they replace the ribbon on their registers so that there is no gap between transactions. Most register transactions, however, are sequentially numbered. If a transaction has been omitted from the register log, the result is a break in the sequence. For instance, if an employee skimmed sale #155, then the register

log would only show transactions #153, #154, #156, #157, and so on. The missing transaction numbers, omitted because the ribbon was lifted when the transactions took place, would indicate fraud.

Skimming During Nonbusiness Hours

Another way to skim unrecorded sales is to conduct sales during nonbusiness hours. For instance, some employees will open stores on weekends or after hours without the owners' knowledge. They can pocket the proceeds of all sales made during these times because the owners have no idea that their stores are even open for business.

EXAMPLE

A manager of a retail facility went to work two hours early every day, opening his store at 8:00 a.m. instead of 10:00 a.m., and pocketed all the sales made during those two hours. He rang up sales on the register as if it was business as usual, but then removed the register log and all the cash he had accumulated. The manager then started from scratch at 10:00 as if the store was just opening. The tape was destroyed so there was no record of the before-hours revenue.

To this point, skimming has been discussed in the context of cash register transactions, but skimming does not have to occur at a register. Some of the most costly skimming schemes are perpetrated by employees who work at remote locations or without close supervision. This can include on-site sales persons who do not deal with registers, independent salesmen who operate off-site, and employees who work at branches or satellite offices. These employees have a high level of autonomy in their jobs, which often translates into poor supervision and, in turn, fraud.

Skimming of Off-Site Sales

Several industries rely on remote salespersons to generate revenue. The fact that these employees are largely unsupervised puts them in a good position to skim revenues. For example, consider the apartment rental industry, where apartment managers handle the day-to-day operations without much oversight. A common scheme is for an on-site employee to identify the tenants who pay in currency and remove them from the books. This causes a particular apartment to appear as vacant on the records when, in fact, it is occupied. The manager can skim the rental payments from the "vacant" unit, and the revenue will never be missed. As long as no one physically checks the apartment, the perpetrator can continue skimming indefinitely.

Another rental-skimming scheme occurs when apartments are rented out but no lease is signed. On the books, the apartment will still appear to be vacant, even though there are tenants on the premises. The perpetrator can skim the rental payments from these tenants without fear that they will show up as past due in the company records. Sometimes the employees in these schemes work in conjunction with the renters and give them a "special rate." In return, the renters' payments are made directly to the employee and any complaints or maintenance requests are directed only to that employee so the tenant's presence in the apartment remains hidden.

Instead of skimming rent, some property managers focus on less predictable forms of revenue like application fees and late fees. Ownership might know when rent is due and how many apartments are occupied, but often there is no control in place to track the number of people who fill out rental applications or how many tenants pay their rent a day or two late. Property managers can make thousands of dollars by skimming these small payments.

Off-site skimming is by no means limited to the apartment rental industry. The schemes described previously can easily translate into any arena where those who generate or collect revenues operate in an independent fashion. A prime example is the insurance agent who sells policies to customers, and then neglects to file the policies with the carrier. Most customers do not want to file claims on a policy, especially early in the term, for fear that their premiums will rise. Knowing this, the agent keeps all documentation on the policies instead of turning it over to the carrier. The agent is able to skim the customer's payments because the carrier does not know the policy exists. The customer continues to make his payments, thinking that he is insured when in fact the policy is a ruse.

Poor Collection Procedures

Poor collection and recording procedures can make it easy for an employee to skim sales or receivables.

EXAMPLE

A government authority that dealt with public housing was victimized because it failed to itemize daily receipts. This agency received payments from several public housing tenants, but at the end of the day, "monies" received from tenants was listed as a whole. Receipt numbers were not used to itemize the payments made by tenants, so there was no way to pinpoint which tenant had paid how much. Consequently, the employee in charge of

collecting money from tenants was able to skim a portion of their payments. The employee simply did not record the receipt of over $10,000. This action caused certain accounts receivable to be overstated where tenant payments were not properly recorded.

Understated Sales

The previous discussion focused on purely off-book sales—those which are never recorded. Understated sales work differently because the transaction in question is posted to the books, but for a lower amount than what the perpetrator actually collected. (See the "Understated Sales" flowchart that follows.) One way employees commit understated sales schemes is by altering receipts or preparing false receipts that misstate sales amounts.

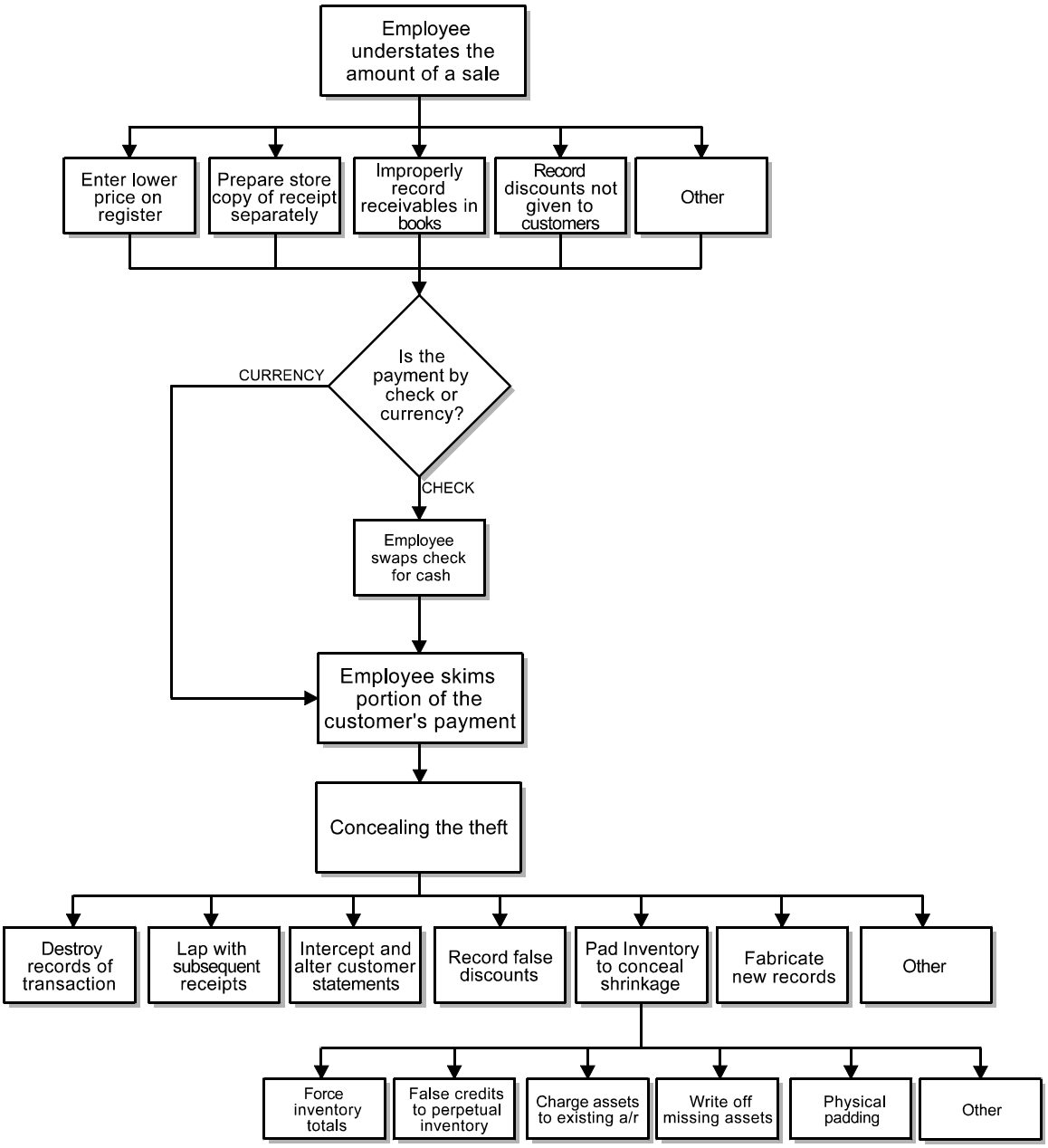
EXAMPLE

An employee wrote receipts to customers for their purchases, but removed the carbon paper backing on the receipts so that they did not produce a company copy. The employee then used a pencil to prepare company copies that showed lower purchase prices. For example, if the customer had paid $100, the company copy might reflect a payment of $80. The employee skimmed the difference between the actual amount of revenue and the amount reflected on the fraudulent receipt.

Understated sales schemes are commonly undertaken by employees who work at the cash register. In a typical scheme, an employee enters a sales total that is lower than the amount actually paid by the customer. The employee skims the difference between the actual purchase price of the item and the sales figure recorded on the register. For instance, if an item is sold for $100, the employee could ring up the sale of an $80 item and skim the excess $20.

Rather than reduce the price of an item, an employee might record the sale of fewer items. If 100 units are sold, for instance, an employee might only record the sale of 50 units and skim the excess receipts.

A similar method is used when sales are made on account. The bill to the customer reflects the true amount of the sale, but the receivable is understated in the company books. For instance, a company might be owed $1,000, but the receivable is recorded as $800. (Sales are correspondingly understated by $200.) When the customer makes payment on the account, the employee can skim $200 and post the $800 to the account. The account will appear to have been paid in full.



Understated Sales

FALSE DISCOUNTS

Those employees with the authority to grant discounts might use this authority to skim sales and receivables. In a false discount skimming scheme, an employee accepts full payment for an item, but records the transaction as if the customer had been given a discount. The employee skims the amount of the discount. For example, on a $100 purchase, if an employee granted a false discount of 20 percent, he could skim $20 and leave the company's books in balance.

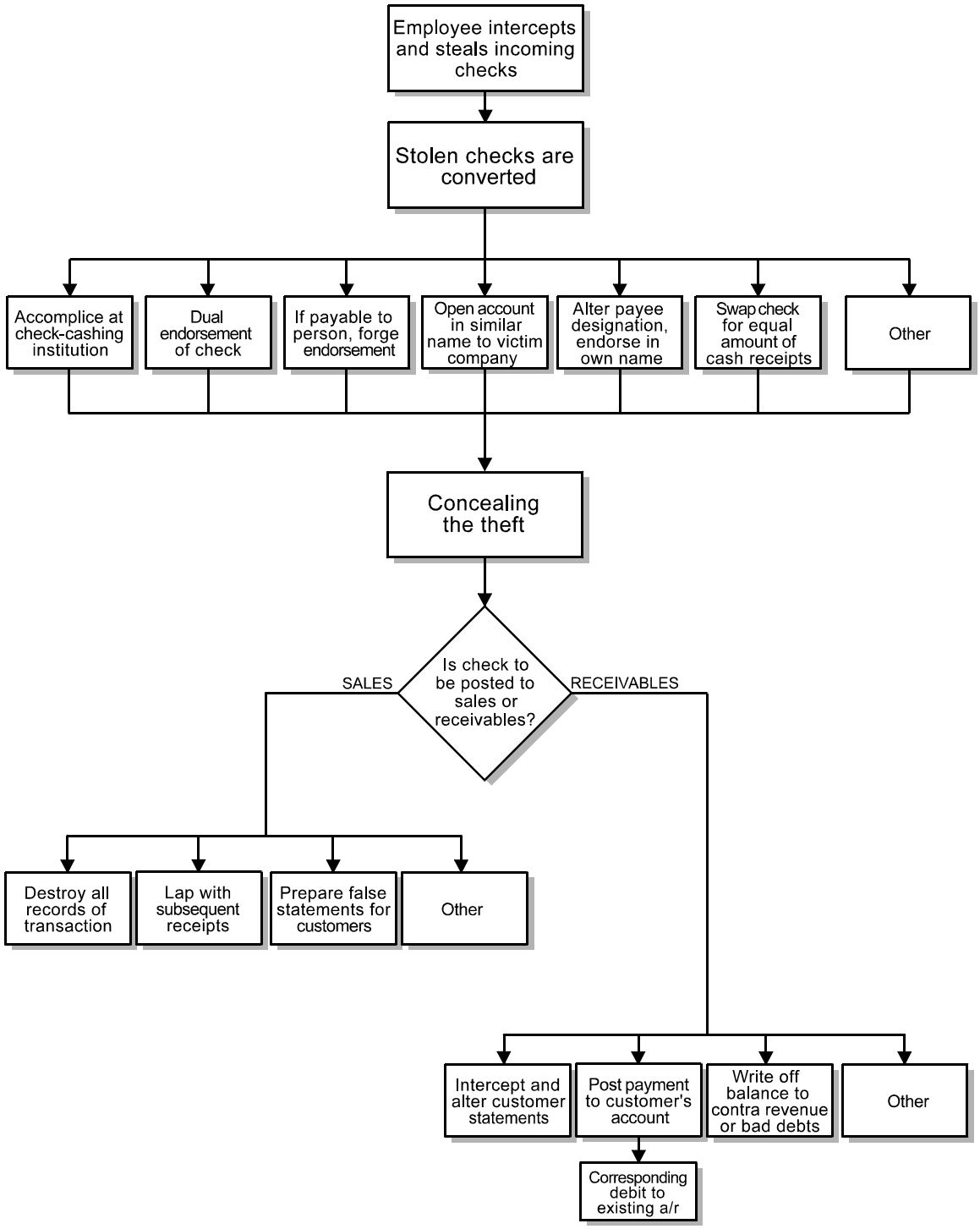
Theft of Checks Received Through the Mail

Checks received through the mail are a frequent target of employees seeking illicit gains. Theft of incoming checks usually occurs when a single employee is in charge of opening the mail and recording the receipt of payments. This employee simply steals one or more incoming checks instead of posting them to customer accounts. (See the "Theft of Incoming Checks" flowchart that follows.) When the task of receiving and recording incoming payments is left to a single person, it is all too easy for that employee to make off with an occasional check.

EXAMPLE

A mailroom employee stole over $2 million in government checks arriving through the mail. This employee simply identified and removed envelopes delivered from a government agency known to send checks to the company. Using a group of accomplices acting under the names of fictitious persons and companies, this individual was able to launder the checks and divide the proceeds with his accomplices.

The theft of checks is not usually complicated, but it is sometimes more difficult to conceal a check theft scheme than other forms of skimming. If the stolen checks were payments on the victim company's receivables, then these payments were *expected*. As receivables become past due, the victim company will send notices of nonpayment to its customers. A customer is likely to complain when he receives a second bill for a payment he has already made. In addition, the cashed check will serve as evidence that the customer made his payment. The methods used to conceal check theft schemes will be discussed later in this section.



Theft of Incoming Checks

Check for Currency Substitutions

A criminal generally prefers to steal currency rather than checks if given the opportunity. The reasons why are obvious. First, currency is harder to trace than a check. A cashed check eventually returns to the person who wrote it and might provide evidence of who cashed it or where it was spent. Endorsements, bank stamps, and so forth might indicate the thief's identity. Currency, on the other hand, disappears into the economy once it is stolen.

The second reason that currency is preferable to a check is the difficulty in converting the check. When currency is stolen, it can be spent immediately. A check, however, must be endorsed and cashed or deposited before the thief can put his hands on the money it represents. To avoid this problem, employees who steal unrecorded checks will frequently substitute them for receipted currency. If, for example, an employee skims an incoming check worth $500, he can add the check to the day's receipts and remove $500 in currency. The total receipts will match the amount of cash on hand, but payments in currency are replaced by the check.

EXAMPLE

An employee responsible for receipting ticket and fine payments on behalf of a municipality abused her position and stole incoming revenues for nearly two years. When payments in currency were received by this individual, she issued receipts, but when checks were received, she did not. The check payments were therefore unrecorded revenues—ripe for skimming. These unrecorded checks were placed in the days' receipts and an equal amount of cash was removed. The receipts matched the amount of money on hand except that payments in currency had been replaced with checks.

The check for currency substitution is very common. While these substitutions make it easier for a crook to convert stolen payments, the problem of concealing the theft still remains. The fact that the stolen checks are not posted means that some customers' accounts are in danger of becoming past due. If this happens, the perpetrator's scheme is in danger because these customers will almost surely complain about the misapplication of their payments. However, the misapplied payments can be concealed on the books by forcing account totals, stealing customers' account statements, lapping, and making other fraudulent accounting entries. These concealment techniques will be discussed in more detail in the "Skimming Receivables" section.

Checks for currency substitutions are especially common when an employee has access to some unexpected source of funds, such as a manufacturer's refund that arrives outside the regular stream of sales and receivables payments. In these cases, the check can be swapped for cash and there is usually no additional step required to conceal the crime. The refund check, an unexpected source of funds, will not be missed by the victim organization, and the party who issued the check expects no goods or services in return.

Skimming Receivables

It is generally more difficult to conceal the skimming of receivables than the skimming of sales because receivables payments are *expected*. The victim organization knows the customer owes money and it is waiting for the payment to arrive. When unrecorded sales are skimmed, it is as though the sale never existed. But when receivables are skimmed, the absence of the payment appears on the books as a delinquent account. To conceal a skimmed receivable, a perpetrator must somehow account for the payment that was due to the company but never received. There are a number of common techniques fraudsters use to conceal the skimming of receivables.

Forcing Account Balances or Destroying Transaction Records

Among the most dangerous receivables skimming schemes are those in which the perpetrator is in charge of collecting and posting payments. If a fraudster has a hand in both ends of the receipting process, he can falsify records to conceal the theft of receivables payments. For example, the fraudster might post the customer's payments to its receivables accounts, even though the payments will never be deposited. This keeps the receivable from aging, but it creates an imbalance in the cash account. The perpetrator hides the imbalance by forcing the total on the cash account, overstating it to match the total postings to accounts receivable.

EXAMPLE

The chief financial officer of a small corporation stole approximately $100,000 from his company by diverting customer checks. This individual controlled all the books and records for the victim company. He stole checks from customers and deposited them in his personal bank account. The customers' payments were still posted to keep the receivables from aging.

The perpetrator stole checks in an amount equal to the victim company's tax liability. To keep the books in balance, he would prepare checks payable to the national tax authority, but he never mailed them. The checks were recorded in the victim's records and the false

disbursements offset the amount of false postings to accounts receivable. The scheme was uncovered when the government notified the victim company that its taxes were delinquent.

Some fraudsters simply destroy all records that might prove that they have been stealing. Destroying records does not prevent the victim organization from realizing that it is being robbed, but it might help conceal the thief's identity.

Lapping

Lapping customer payments is one of the most common methods of concealing receivables skimming. Lapping is the crediting of one account through the abstraction of money from another account. It is the fraudster's version of "robbing Peter to pay Paul."

Suppose a company has three customers, A, B, and C. When A's payment is received, the fraudster steals it instead of posting it to A's account. Customer A expects that his account will be credited with the payment he has made. If the payment has not been posted by the time A's next statement is mailed, he will see that the payment was not applied to his account and will almost certainly complain. To avoid this, the thief must take some action to make it appear that the payment was posted.

When B's check arrives, the thief posts this money to A's account. Payments now appear to be up to date on A's account, but B's account is behind. When C's payment is received, the perpetrator applies it to B's account. This process continues indefinitely until one of three things happens: (1) someone discovers the scheme, (2) restitution is made to the accounts, or (3) some concealing entry is made to adjust the accounts receivable balances.

EXAMPLE

A clerk working for a government agency committed a lapping scheme that involved the theft of more than 150 customer payments, causing a total misappropriation of more than $30,000 in government funds. This individual stole taxes, fees, and other incoming payments from customers to cover personal expenses. When a customer's payment was stolen, the documentation on that payment would be hidden until a later payment was received. The later payment would be applied to the earlier customer's records.

As the rotating schedule of applying and misapplying payments became more and more complicated, the perpetrator insisted on exerting more and more control over the receipting process. The fraudster insisted on handling all incoming mail, preparing the deposit, and

> *delivering the deposit to the bank so that he could continue to delay the posting of payments. The fraud was detected in large part because several consumers complained that they had not received confirmation of their payments, even though their checks had cleared months earlier.*

Because lapping schemes can become very intricate, fraudsters sometimes keep a second set of books on hand detailing the true nature of the payments received. In many skimming cases, a search of the fraudster's work area will reveal a set of records tracking the actual payments and how they have been misapplied to conceal the theft. It might seem odd that people would keep records of their illegal activity on hand, but many lapping schemes become extremely complicated as more and more payments are misapplied. The second set of records helps the perpetrator keep track of the funds that were stolen and which accounts need to be credited to conceal the fraud. Uncovering these records, if they exist, will greatly facilitate the investigation of a lapping scheme.

While lapping is more commonly used to conceal receivables skimming, it can also be used to disguise the skimming of sales. Employees sometimes steal all or part of one day's receipts and replace them with the receipts from the following day. This type of concealment requires the employee to delay making the company deposit until enough money can be collected to recoup the stolen funds. If an organization rigidly adheres to a deposit schedule, it is unlikely that lapping will be effective in concealing this type of fraud.

Stolen Statements

When employees skim receivables, they might let the targeted accounts age instead of attempting to force the balances. In other words, they steal an incoming check intended as payment on a receivable, and they simply act as if the check never arrived. This method keeps the victim organization's cash account in balance because the stolen payment is never posted.

Of course, if the customer's payment is not posted, the receivable will eventually become past due. The customer will have proof in the form of a canceled check that a payment was made on the account. The question will arise: where did the payment go? The answer, of course, is that it went into the fraudster's pocket. So the fraudster's goal must be to keep the customer from realizing that his account was not credited with the payment. If this can be accomplished, the customer will not complain about the missing payment, and the victim organization will not realize that skimming has occurred.

One way fraudsters attempt to conceal the fact that they have skimmed a payment from a customer is to intercept the customer's account statement and/or late notices. In some cases, the perpetrator intercepts the account statement by changing the customer's address in the billing system so that statements are sent directly to the perpetrator's home or to an address where he can retrieve them. In other instances, the perpetrator physically intercepts the statements before they are mailed.

Once the real statement indicating that the payment was not received has been intercepted, the fraudster usually alters the statement or produces a counterfeit. The false statements indicate that the customer's payment was properly posted. This leads the customer to believe that his account is up to date and keeps the customer from complaining about stolen payments.

False Account Entries

Intercepting the customer's statements will keep him unaware of his account's status, but as long as the customer's payments are being skimmed, his account is slipping further and further past due. The perpetrator must bring the account back up to date to conceal his crime. Lapping is one way to keep accounts current as the employee skims from them. Another way is to make false entries in the victim organization's accounting system.

DEBITS TO EXPENSE ACCOUNTS

An employee might conceal the skimming of funds by making unsupported entries in the victim company's books. If a payment is made on a receivable, for instance, the proper entry is a debit to cash and a credit to the receivable. Instead of debiting cash, the employee might choose to debit an expense account. This transaction still keeps the company's books in balance, but the incoming cash is never recorded. In addition, the customer's receivable account is credited, so it will not become delinquent.

DEBITS TO AGING OR FICTITIOUS RECEIVABLES

The same method discussed previously is used when employees debit existing or fictitious accounts receivable to conceal skimmed cash. For example, an employee who has skimmed one customer's payments might add the stolen amounts to aging accounts that will soon be written off as uncollectible or to very large accounts where a small debit might go unnoticed.

Some perpetrators also set up completely fictitious accounts and debit them for the cost of skimmed receivables. The employees then simply wait for the fictitious receivables to age

and be written off as uncollectable. In the meantime, the fictitious receivables carry the cost of a skimming scheme where it will not be detected.

WRITING OFF ACCOUNT BALANCES

Some employees cover their skimming by posting entries to contra revenue accounts such as "discounts and allowances." If, for instance, an employee intercepts a $1,000 payment, he would create a $1,000 "discount" on the account to compensate for the missing money. Another account that might be used in this type of concealment is the bad debts expense account.

EXAMPLE

A billing manager was authorized to write off certain patient balances as hardship allowances. This employee accepted payments from patients, and then instructed billing personnel to write off the balance in question. The payments were never posted; they were intercepted by the billing manager. She stole approximately $30,000 by using her authority to write off patients' balances.

Inventory Padding

A problem for fraudsters in some skimming schemes is the victim organization's inventory. Off-book sales of goods (skimming schemes) will always leave an inventory shortage and a corresponding rise in the cost of goods sold.

When a sale of goods is made, the physical inventory is reduced by the amount of merchandise sold. For instance, when a retailer sells a pair of shoes, there is one less pair of shoes in the stock room. If this sale is not recorded, however, the shoes are not removed from the perpetual inventory records. Thus, there is one less pair of shoes on hand than in the perpetual inventory. A reduction in the physical inventory without a corresponding reduction in the perpetual inventory is known as "shrinkage."

There is no shrinkage when an employee skims sales of services (because there is no inventory for services), but when sales of goods are skimmed, shrinkage always occurs. Some shrinkage is expected due to customer theft, faulty products, and spoilage, but high levels of shrinkage serve as a warning that a company could be a victim of occupational fraud. The general methods used to conceal inventory shrinkage are discussed in detail in the "Asset Misappropriation: Inventory and Other Assets" chapter in this section of the *Fraud Examiners Manual.*

Short-Term Skimming

Short-term skimming is not a distinct method for stealing sales and receivables, but rather a distinct way of using skimmed money. The peculiar aspect to short-term skimming is that the fraudster keeps the stolen money only for a short while before eventually passing the payment on to his employer. The employee merely delays the posting. In a short-term skimming scheme, an employee steals an incoming payment and then places the skimmed funds in an interest-bearing account or in a short-term security. The employee earns interest on the skimmed payments while they remain under his control. Eventually, he withdraws the principal and applies it to the customer's account, but retains the interest for himself.

Detection of Skimming Schemes

The following are some detection methods that might be effective in detecting skimming schemes.

Receipt- or Sales-Level Detection

Key analytical procedures, such as vertical and horizontal analysis of sales accounts, can be used for skimming detection on a grand scale. These procedures analyze changes in the accounts and can possibly point to skimming problems, including understated sales.

Ratio analysis can also provide keys to the detection of skimming schemes. These procedures are discussed in detail in the "Financial Statement Fraud" chapter.

Detailed inventory control procedures can also be used to detect inventory shrinkage due to unrecorded sales. Inventory detection methods include statistical sampling, trend analysis, reviews of receiving reports and inventory records, and verification of material requisition and shipping documentation, as well as actual physical inventory counts. These procedures are reviewed in the "Asset Misappropriation: Inventory and Other Assets" chapter.

Journal Entry Review

Skimming can sometimes be detected by reviewing and analyzing all journal entries made to the cash and inventory accounts. Journal entries involving the following topics should be examined:

- False credits to inventory to conceal unrecorded or understated sales
- Write-offs of lost, stolen, or obsolete inventory

- Write-offs of accounts receivable accounts
- Irregular entries to cash accounts

Detecting Lapping of Sales or Receivables

A skimming scheme that involves lapping can be detected by comparing the dates of customers' payments with the dates that those payments are posted to the books. This requires an examination of the source documents, such as canceled check copies, bank statements, and deposit slips. Any significant discrepancies between these two dates might indicate that a customer's payment was skimmed, and the fraudster had to wait until another customer paid to post payment to the victim's account. Any significant discrepancies between deposit date and posting date should be investigated. Confirmation of customers' accounts is another method that might detect lapping.

Confirmations are especially effective on large accounts where the time value of money is an issue. However, customers who pay on invoice rather than on balance might not know the exact balance of their account. If this is the case, it might be more effective to confirm by invoice and reconstruct the account balance using the source documents in the files and the results of the confirmation. If fraud is suspected, ask the customer or the bank to return a copy of both the front and the back of the check(s) used to pay specific invoices. Match the data on the check copies with the posting dates in the customer's account.

Prevention of Skimming Schemes

Receipt- or Sales-Level Control

As with most fraud schemes, internal control procedures are a key to the prevention of skimming schemes. An essential part of developing control procedures is management's communication to employees. Controlling whether an employee will not record a sale, understate a sale, or steal incoming payments is extremely difficult.

General Controls

Sales entries and general ledger access controls should include documented policies and procedures, which are communicated directly from management. The control procedures will generally cover the following subjects:

- Appropriate separation of duties and access control procedures regarding who makes ledger transactions will be followed.
- Transactions must be properly recorded as to amount, date of occurrence, and ledger account.

- Proper safeguard measures will be adopted to ensure physical access to the accounting systems. Additional measures should ensure the security of company assets.
- All areas where employees handle cash should be monitored with visible video cameras.
- Independent reconciliations, as well as internal verification of accounts, will be performed on ledger accounts.[1]

It is important to note that since skimming is an off-book fraud, routine account reconciliation is not likely to prevent or detect a skimming scheme. If such a scheme is taking place, reconciling the register records to the cash in the drawer will not indicate there is anything amiss. Reconciling the physical inventory count with the perpetual inventory records, however, might reveal that there is shrinkage, and therefore a skimming scheme.

Skimming Controls

The discovery of thefts of checks and cash involves proper controls on the receipt process. Deficiencies in the answers to these typical audit-program questions might be red flags.

- Is mail opened by someone independent of the cashier, accounts receivable bookkeeper, or other accounting employees who may initiate or post journal entries?
- Is the delivery of unopened business mail prohibited to employees having access to the accounting records?
- Does the employee who opens the mail:
  - Place restrictive endorsements ("For Deposit Only") on all checks received?
  - Prepare a list of the money, checks, and other receipts?
  - Forward all remittances to the person responsible for preparing and making the daily bank deposit?
  - Forward the total of all remittances to the person responsible for comparing it to the authenticated deposit ticket and amount recorded?
- Is a lock box used?
- Do cash sales occur? If yes:
  - Are cash receipts prenumbered?
  - Is an independent check of prenumbered receipts done daily and reconciled to cash collections?
- Do cash refunds require approval?
- Are cash receipts deposited intact daily?
- Are employees who handle receipts bonded?

[1] George Georgiades, *Audit Procedures* (New York: Harcourt Brace Professional Publishing, 1995).

- Is the accounts receivable bookkeeper restricted from:
  - Preparing the bank deposit?
  - Obtaining access to the cash receipts journal?
  - Having access to collections from customers?
  - Are banks instructed not to cash checks drawn to the order of the company?
- Is the cashier restricted from gaining access to the accounts receivable records and bank and customer statements?
- Are areas where physical handling of cash takes place reasonably safeguarded?
- Is the person who makes postings to the general ledger independent of the cash receipts and accounts receivable functions?
- Does a person independent of the cashier or accounts receivable functions handle customer complaints?

Cash Larceny

The second type of cash receipts scheme is cash larceny. In the occupational fraud setting, *cash larceny* is the intentional taking of an employer's cash (the term *cash* includes both currency and checks) without the consent and against the will of the employer. However, recall that skimming also involves the intentional taking of an employer's cash. The difference between skimming and cash larceny is that skimming is the theft of cash *before* it appears on the books. Cash larceny involves the theft of money that has already appeared on the victim company's books. Accordingly, these schemes are much harder to get away with—they leave an audit trail.

A cash larceny scheme can take place in any circumstance in which an employee has access to cash. Every company must deal with the receipt, deposit, and distribution of cash, so every company is potentially vulnerable to a cash larceny scheme. While the circumstances in which an employee might steal cash are nearly limitless, most larceny schemes involve the theft of incoming cash, currency on hand (in a cash register, cash box, etc.), or theft of cash from the victim organization's bank deposits.

Incoming Cash

Theft of Cash from the Register

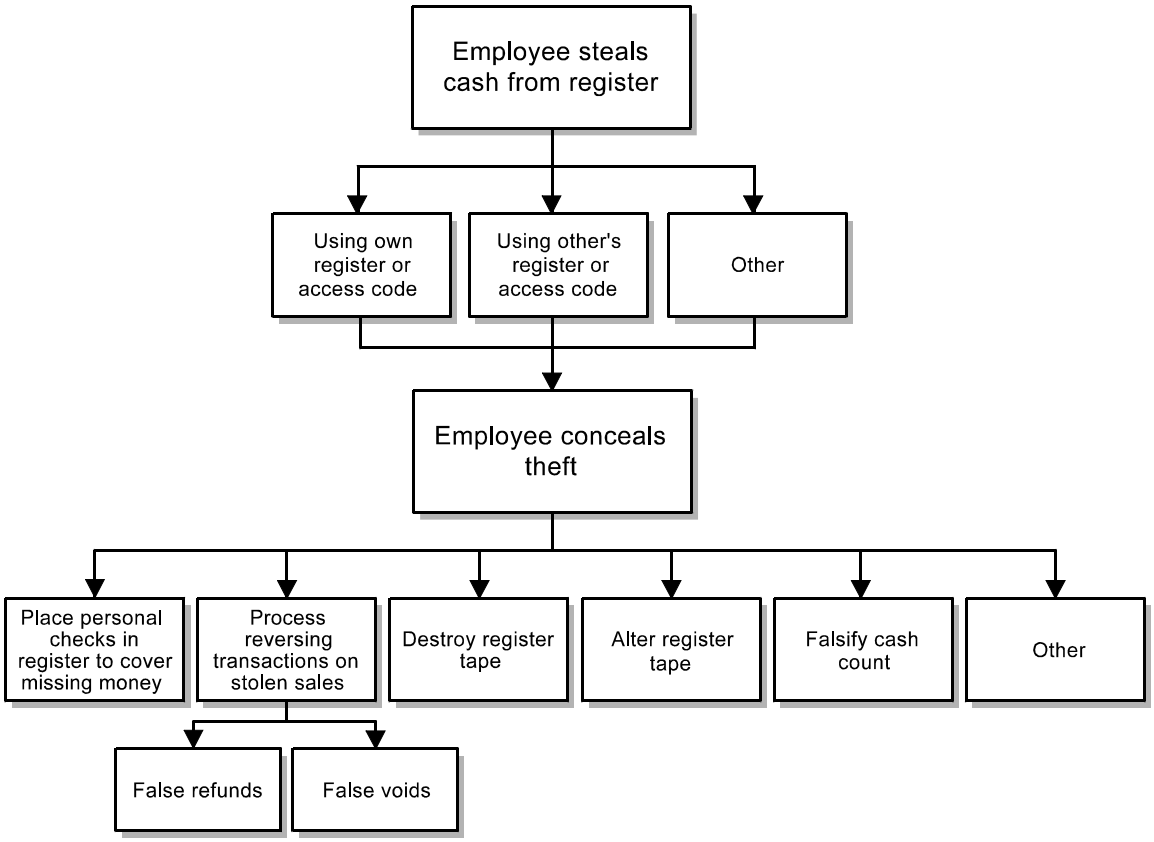
A large percentage of cash larceny schemes occur at the cash register, and for good reason—the register is usually where the cash is. The register (or similar cash collection points like cash drawers or cash boxes) is usually the most common point of access to cash for

employees, so it is understandable that this is where larceny schemes frequently occur. Furthermore, there is often a great deal of activity at the register—numerous transactions that require employees to handle cash. This can serve as a cover for cash theft. In a flurry of activity, with money being passed back and forth between customer and employee, an employee can often slip cash out of the register and into his pocket undetected.

The most straightforward cash larceny scheme is to simply open the register and remove currency or checks. (See the "Cash Larceny from the Register" flowchart that follows.) The theft is often committed as a sale is being conducted so that it appears to be part of the transaction. In other circumstances, the perpetrator waits for a slow moment when no one is around to notice him digging into the cash drawer.

Recall that the difficulty in detecting skimming schemes comes from the fact that the stolen funds are never entered on the victim organization's accounts. In a larceny scheme, on the other hand, the funds that the perpetrator steals have already been reflected on the register log. As a result, an imbalance will result between the register log and the cash drawer.

A register is balanced by comparing the transactions on the register log to the amount of cash on hand. Sales, returns, and other register transactions that are recorded on the register log are added to or subtracted from a known balance to arrive at a total for the period in question. The actual cash is then counted and the two totals are compared. If the register log shows that there should be more cash in the register than what is present, the discrepancy might be due to larceny.



Cash Larceny from the Register

The actual method for taking money at the register—opening the register and removing currency—rarely varies. It is the methods used by perpetrators to avoid getting caught that distinguish larceny schemes. Oddly, in many instances the perpetrator has no plan for avoiding detection. A large part of fraud is rationalizing; the employee convinces himself that he is somehow entitled to what he is taking, or that what he is doing is not actually a crime. Register larceny schemes frequently begin when the perpetrator convinces himself that he is only "borrowing" the funds to cover a temporary monetary need. These people might carry the missing currency in their registers for several days, deluding themselves in the belief that they will one day repay the funds they have stolen.

The employee who does nothing to camouflage his crimes is easily caught. More dangerous is the person taking active steps to hide his crimes. One basic way for an employee to disguise the fact that he is stealing currency is to take money from someone else's register.

In some retail organizations, employees are assigned to certain registers. Alternatively, one register is used and each employee has an access code. When cash is missing from a certain cashier's register, that cashier is obviously the most likely suspect for the theft. Therefore, by stealing from a coworker's register, or by using someone else's access code to enter the register, the perpetrator makes sure that another employee will be the prime suspect in the theft.

EXAMPLE

A teller for a retail sales company simply signed onto a register, rang a "no sale," and took currency from the drawer. Over a period of time, the teller took approximately $6,000 through this simple method. To get away with the theft, the teller waited until a coworker was on break and then logged onto that person's register, rang a "no sale," and took the cash. The resulting cash shortage therefore appeared in an honest employee's register, deflecting attention from the true thief.

A very unsophisticated way to avoid detection is to steal currency in very small amounts over an extended period of time. Because the missing amounts are small, the shortages might be dismissed as accounting errors rather than theft. Typically, the employee becomes dependent on the extra money he is pilfering and his thefts increase in scale or become more frequent, which causes the scheme to be uncovered. Most retail organizations track overages or shortages by employee, making this method largely ineffective.

REVERSING TRANSACTIONS

Some employees conceal cash larceny by processing reversing transactions, which cause the register log to reconcile to the amount of cash on hand after the theft. By processing false voids or refunds, an employee can reduce the cash balance reflected on the register log.

EXAMPLE

A cashier received payments from a customer and recorded the transactions on her system. The cashier stole the payments from the customers and then destroyed the company's receipts that reflected the transactions. To complete the cover-up, the cashier went back and voided the transactions that she had entered at the time the payments were received. The reversing entries brought the receipt totals into balance with the cash on hand.

REGISTER MANIPULATION

Instead of using reversing entries, an employee might manually alter the register log. Again, the purpose of this activity is to force a balance between the cash on hand and the actual cash received. An employee might use correction fluid to cover up a sale where the proceeds were stolen or might simply cross out or alter the numbers on the tape so that the register total and the cash drawer balance. This type of concealment is not common because the alterations will generally be noticeable.

ALTERING CASH COUNTS

Another method for concealing cash larceny is to alter the cash counts on registers. When cash from a register is totaled and prepared for deposit, an employee simply records the wrong amount so that the cash on hand appears to balance with the total on the register log. Obviously, employees who deal with the receipt of cash should not be charged with verifying the amount of cash on hand in their own register, but this control is often overlooked.

DESTROYING REGISTER LOGS

If the fraudster cannot make the cash and the tape balance, the next best thing is to prevent others from computing the totals and discovering the imbalance. Employees who are stealing from the register sometimes destroy detail tapes that would implicate them in a crime. When detail tapes are missing or defaced, it might be because someone is trying to conceal a fraud.

Other Larceny of Sales and Receivables

Not all receipts arrive via the cash register. Employees can just as easily steal money received at other points. One of the more common methods is to take checks received through the mail and post the payments to the accounting system, but steal the checks. (See the "Other Cash Larceny" flowchart that follows.) Obviously, this type of scheme leaves the cash account out of balance. From a perpetrator's perspective, it would make much more sense to take checks that have not yet been posted to customer accounts. Often, this type of cash larceny scheme is committed by an employee who claims to only be "borrowing" the funds for a short while—one of the classic rationalizations in occupational fraud schemes.

Those employees who have total control of a company's accounting system can overcome the problem of out-of-balance accounts. It is common, especially in small businesses, for a single person to control all of a company's deposits and ledgers. These employees can steal

incoming cash that has already been posted and then conceal the crime by making unsupported entries in the victim organization's books. Poor separation of duties is often the weakness that allows cash larceny schemes to go undetected.

EXAMPLE

An employee posted customer payments to the accounts receivable journal but stole the cash received. This resulted in an imbalance in the victim company's cash account. But the perpetrator had control over the company's deposits and all its ledgers. This allowed the employee to conceal the crime by making unsupported entries in the company's books that produced a fictitious balance between receipts and ledgers.

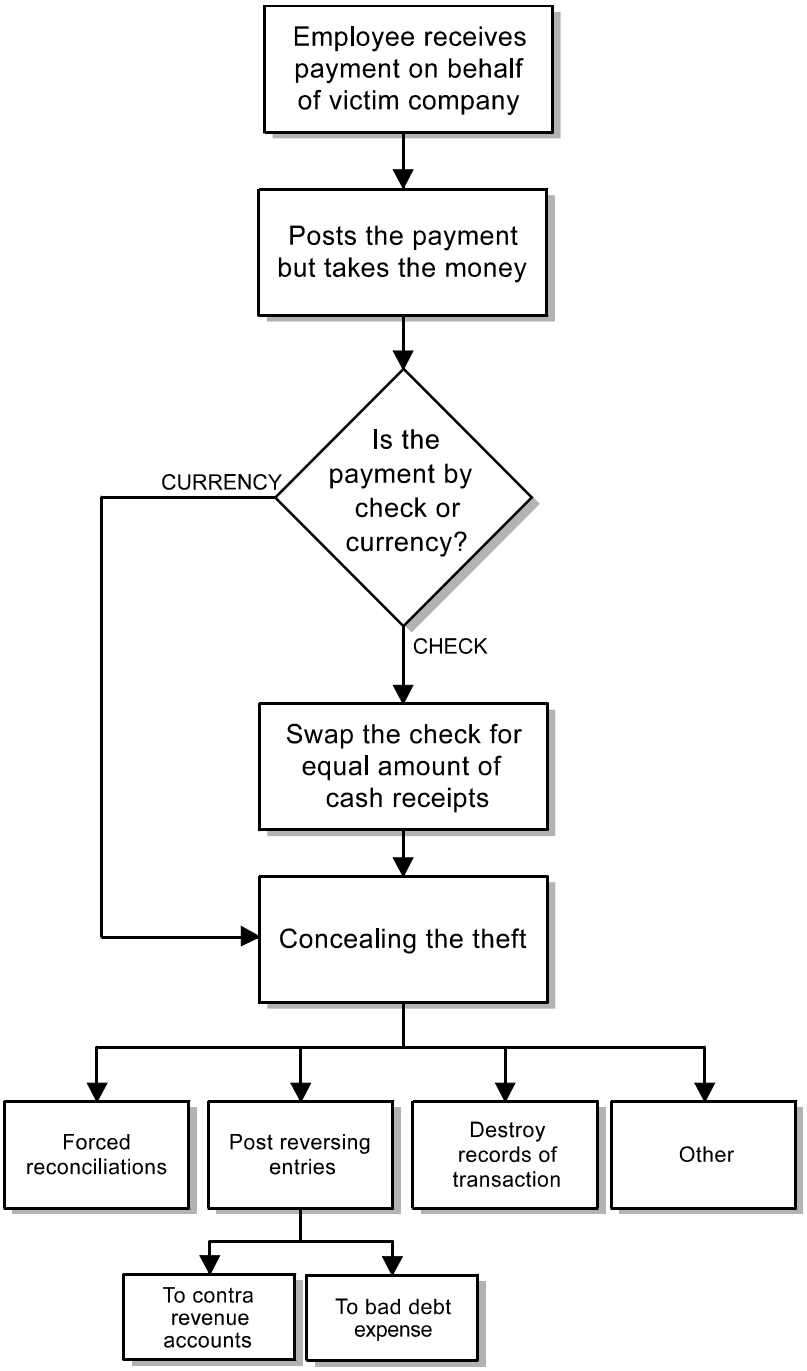
In circumstances in which payments are stolen but nonetheless posted to the cash receipts journal, reversing entries are sometimes used to balance the victim company's accounts. The incoming payment is initially credited to the customer's account, but the entry is later reversed with an unauthorized adjustment such as a "courtesy discount."

A less elegant way to hide a crime is to simply destroy all records that might prove that the perpetrator has been stealing. This "slash and burn" concealment technique does not prevent the victim company from realizing that it has been robbed, but it might help conceal the thief's identity.

Cash Larceny from the Deposit

At some point in every revenue-generating business, someone must physically take the company's currency and checks to the bank. This person or persons, left alone literally holding the bag, will have an opportunity to take a portion of the money prior to depositing it into the company's accounts.

Typically, when a company receives cash, someone is assigned to tabulate the receipts, list the form of payment (currency or check), and prepare a deposit slip for the bank. Then another employee takes the cash and deposits it in the bank. The person who made out the deposit generally retains one copy of the slip. This copy is matched to a receipted copy of the slip, which the bank stamps when the deposit is made.



Other Cash Larceny

This procedure is designed to prevent the theft of funds from the deposit, but thefts still occur, often because companies do not adhere to the process. (See the "Cash Larceny from the Deposit" flowchart that follows.) For example, when one person is in charge of preparing the deposit slips, making the deposit, and reconciling the bank statement, that person can pilfer money from the day's receipts and conceal it by falsifying the deposit slips. If the day's receipts are $1,000, the perpetrator might fill out a deposit slip for $500 and steal the other $500. The employee then makes correspondingly false entries in the books, understating the day's receipts. This process creates a false balance in the victim organization's records.

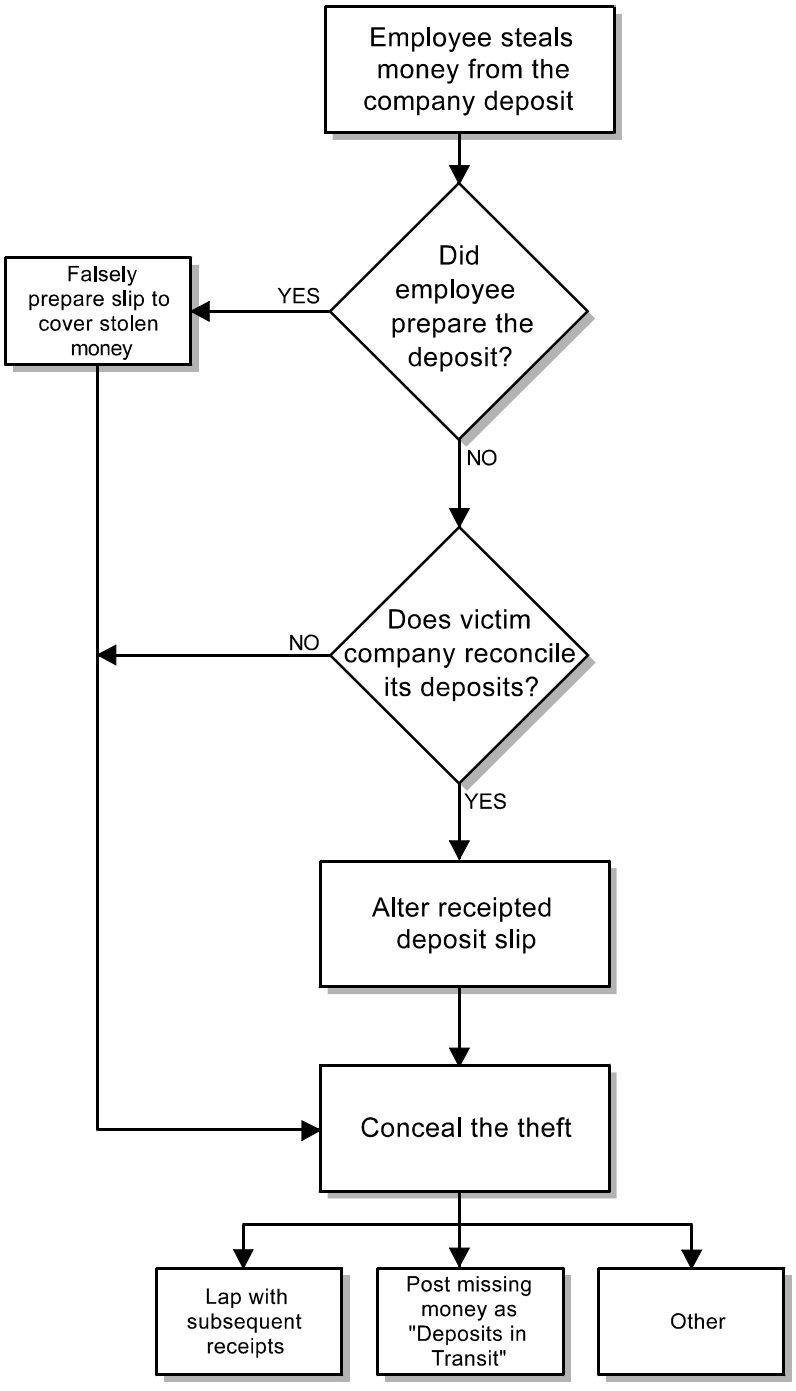
A failure to reconcile the bank copy of the deposit slip with the office copy can result in fraud. When the person making the deposit knows his company does not reconcile the two copies, he can steal cash from the deposit on the way to the bank and alter the deposit slip so that it reflects a lesser amount. In some cases, sales records are also altered to match the diminished deposit.

When cash is stolen from the deposit, the receipted deposit slip will of course be out of balance with the company's copy of the deposit slip (unless the perpetrator also prepared the deposit). To correct this problem, some perpetrators alter the bank copy of the deposit slip after it has been validated. This brings the two copies back into balance.

EXAMPLE

An employee altered 24 deposit slips and validated bank receipts in the course of a year to conceal the theft of over $15,000. These documents were altered with correction fluid and ink to match the company's cash reports.

One common-sense issue that organizations sometimes overlook is the handling of the deposit on the way to the bank. Once prepared, the deposit should immediately be put in a safe place until it is taken to the bank. Unfortunately, some organizations leave their deposits carelessly unattended. For example, some companies prepare the daily deposit, and then leave it in the office overnight to be taken to the bank the next morning. Employees familiar with this routine have little trouble pilfering checks and currency from the deposit after hours.



Cash Larceny from the Deposit

As with all cash larceny schemes, stealing from the company deposit can be rather difficult to conceal. In most cases, these schemes are only successful in the long term when the person who counts the cash also makes the deposit. In any other circumstance, the scheme's success depends primarily on the inattentiveness of those charged with preparing and reconciling the deposit.

Deposit Lapping

One method that fraudsters sometimes use to conceal cash larceny from the deposit is *lapping*. Lapping occurs when an employee steals the deposit from day one and then replaces it with day two's deposit. Day two's deposit is then replaced with money received on day three, and so on. The perpetrator is always one day behind, but as long as no one demands an up-to-the minute reconciliation of the deposits to the bank statement—and if daily receipts do not drop precipitously—he might be able to avoid detection for a period of time. Lapping is discussed in more detail in the "Skimming" section.

Deposits in Transit

A final concealment strategy used for stolen deposits is to carry the missing money as *deposits in transit* on the bank reconciliation, which is money that has been recorded in the company's cash account in its general ledger, but hasn't yet cleared the bank. This is one of the ways to account for discrepancies between the company's records and the bank statement. Although usually reasonable, deposits in transit can be used to conceal a cash larceny from the deposit. The deposit in transit amount should be traced to subsequent bank statements to ensure its legitimacy.

EXAMPLE

An employee was responsible for receiving collections, issuing receipts, posting transactions, reconciling accounts, and making deposits. This employee took over $20,000 in collections from her employer over a five-month period. To hide the theft, the perpetrator carried the missing money as deposits in transit, meaning that the missing money would appear on the next month's bank statement. Of course, it never did. The balance was carried for several months as "d.i.t." until an auditor recognized the discrepancy and put a halt to the fraud.

Detection of Cash Larceny

Cash larceny schemes are easier to detect than skimming schemes. Cash larceny involves the theft of cash that appears on a company's books or records, whether it's theft of cash in a

cash register or theft of cash from a deposit. Cash larceny schemes are more difficult to get away with because they leave an audit trail.

Receipt Recording

In-depth analysis of the cash receipts and recording process is the key to detecting a cash larceny scheme. Areas of analysis might include:

- Mail and register receipt points
- Journalizing and recording of the receipts
- Security of the cash from receipt to deposit

Control Objectives

In analyzing the cash receipt process, it is important to meet the following control objectives:

- Cash receipts must be complete. Each day's receipts must be promptly collected and deposited in full.
- Each receivable transaction recorded must be legitimate and have supporting documentation.
- All information included in the transaction must be correctly verified as to amount, date, account coding, and descriptions.
- The cash must be safeguarded while in the company's physical possession.
- There must be appropriate personnel responsible for overseeing cash control processes.
- Cash register log totals should be reconciled to the amount of cash in the drawer.
- An independent listing of cash receipts should be prepared before the receipts are submitted to the cashier or accounts receivable bookkeeper.
- An independent person should verify the listing against the deposit slips.
- Authenticated deposit slips should be retained and reconciled to the corresponding amounts in the cash receipts records.
- The bank deposit should be made by someone other than the cashier or the accounts receivable clerk. A person independent of the cash receipts and accounts receivable functions should compare entries to the cash receipts journal with:
  - Authenticated bank deposit slips
  - Deposit per the bank statements
- Areas where physical handling of cash takes place should be reasonably safeguarded.

Analytical Review

Analyzing the relationship among sales, cost of sales, and the returns and allowances can detect inappropriate refunds and discounts.

- If a large cash fraud is suspected, a thorough review of these accounts might enlighten the fraud examiner as to the magnitude of the suspected fraud.
- An analysis of refunds and returns and allowances with the actual flow of inventory might reveal some fraud schemes. The refund should cause an entry to inventory, even if it is damaged inventory. Likewise, a return will cause a corresponding entry to an inventory account.
- There should be a linear relationship between sales and returns and allowances over a relevant range. Any change in this relationship might point to a fraud scheme unless there is another valid explanation, such as a change in the manufacturing process, change in product line, or change in price.

Detection at the Register

As cash is received, whether at a register or through the mail, it is important to ensure that the employees responsible for completing these important tasks are informed of their responsibility and properly supervised.

- Access to the register must be closely monitored and access codes must be kept secure.
- All employees should have unique access codes to the cash registers. The time periods that each access code is used should be checked against employee work schedules to ensure an employee's access code was not used in his absence.
- An employee other than the register worker should be responsible for preparing register count sheets and reconciling them with register totals.
- Popular concealment methods must be watched for. These methods, discussed earlier, include checks for cash, reversing transactions, register log destruction or alteration, and sales cash counts.
- Complete register documentation and cash must be delivered to the appropriate personnel in a timely manner.
- Cash thefts are sometimes revealed by customers who have either paid money on an account and have not received credit or, in some cases, have noticed that the credit they have been given does not agree with the payment they have made. Complaints and inquiries are also received frequently from banks.

Cash Account Analysis

Cash larceny can be detected by reviewing and analyzing all journal entries made to the cash accounts. This review and analysis should be performed on a regular basis. If an employee is unable to conceal the fraud through altering the source documents, such as the cash register log, then he might resort to making a journal entry directly to cash. In general (except in financial institutions), there are very few instances in everyday business activity where an independent journal entry is necessary for cash. One of these exceptions is the recording of the bank service charge. However, this is an easy journal entry to trace to its source documentation, namely the bank statement. Therefore, all other entries directly to cash are suspect and should be traced to their source documentation or explanation. Suspect entries will generally credit the cash account and correspondingly debit various other accounts such as a sales contra account or bad debt expenses.

Prevention of Cash Larceny

Separation of Duties

The primary means of preventing cash larceny is separation of duties. Whenever one individual has control over the entire accounting transaction (e.g., authorization, recording, and custody), the opportunity is present for cash fraud. Ideally, each of the following duties and responsibilities should be separated:

- Cash receipts
- Cash counts
- Bank deposits
- Deposit receipt reconciliation
- Bank reconciliations
- Posting of deposits
- Cash disbursements

If any one person has the authority to collect the cash, deposit the receipts, record that collection, and disburse company funds, the risk of fraud is high.

Assignment Rotation and Mandatory Vacations

Many internal fraud schemes are continuous in nature and require ongoing efforts by the employee to conceal the fraud. Mandatory vacations are an excellent method of detecting cash fraud. If mandatory vacations are within the company's policies, it is important that during the employee's absence, that employee's normal workload be performed by another

individual. The purpose of mandatory vacations is lost if the work is allowed to remain undone during the employee's time off.

Surprise Cash Counts and Procedure Supervision

Surprise cash counts and supervisory observations are a useful fraud prevention method if properly used. It is important that employees know that cash will be counted on a periodic and unscheduled basis. These surprise counts must be made at all steps of the process, from receiving the check to deposit.

Physical Security of Cash

- Ensure proper separation of duties of key personnel.
- Review the check and cash composition of the daily bank deposit during unannounced cash counts and during substantive audit tests of cash receipts.
- Review the entity's records of the numerical series of printed prenumbered receipts, and verify that these receipts are used sequentially (including voided documents).
- Review the timeliness of deposits from locations to the central treasurer function.
- Observe locations' cash receipting operations.
- Prepare and review a schedule of all cash receipting functions from a review of revenue reports, from cash receipt forms at the central treasurer function, and from discussion with knowledgeable employees.
- Prepare and analyze an inventory of all imprest and change funds by purpose, amount, custodian, date, and location.
- Audit all revenue sources on a cycle.
- Periodically use comparative analytical reviews to determine which functions have unfavorable trends.
- Determine reason(s) why revenue has changed from previous reporting periods.
- Confirm responses obtained from managers by using alternative records or through substantive audit tests.
- Adhere to a communicated policy of unannounced cash counts.

ASSET MISAPPROPRIATION: FRAUDULENT DISBURSEMENTS

In fraudulent disbursement schemes, an employee makes a distribution of company funds for a dishonest purpose. Examples of fraudulent disbursements include forging company checks, the submission of false invoices, altering timecards, and so forth. On their face, the fraudulent disbursements do not appear any different from valid disbursements of cash. In many cases, the fraudster "tricks" the victim company into remitting payment. For instance, when an employee runs a fake invoice through the accounts payable system, the victim organization cuts a check for the bad invoice right along with all the legitimate payments it makes. The perpetrator has taken money from his employer in such a way that it appears to be a normal disbursement of cash. Someone might notice the fraud based on the amount, recipient, or destination of the payment, but the *method* of payment is legitimate.

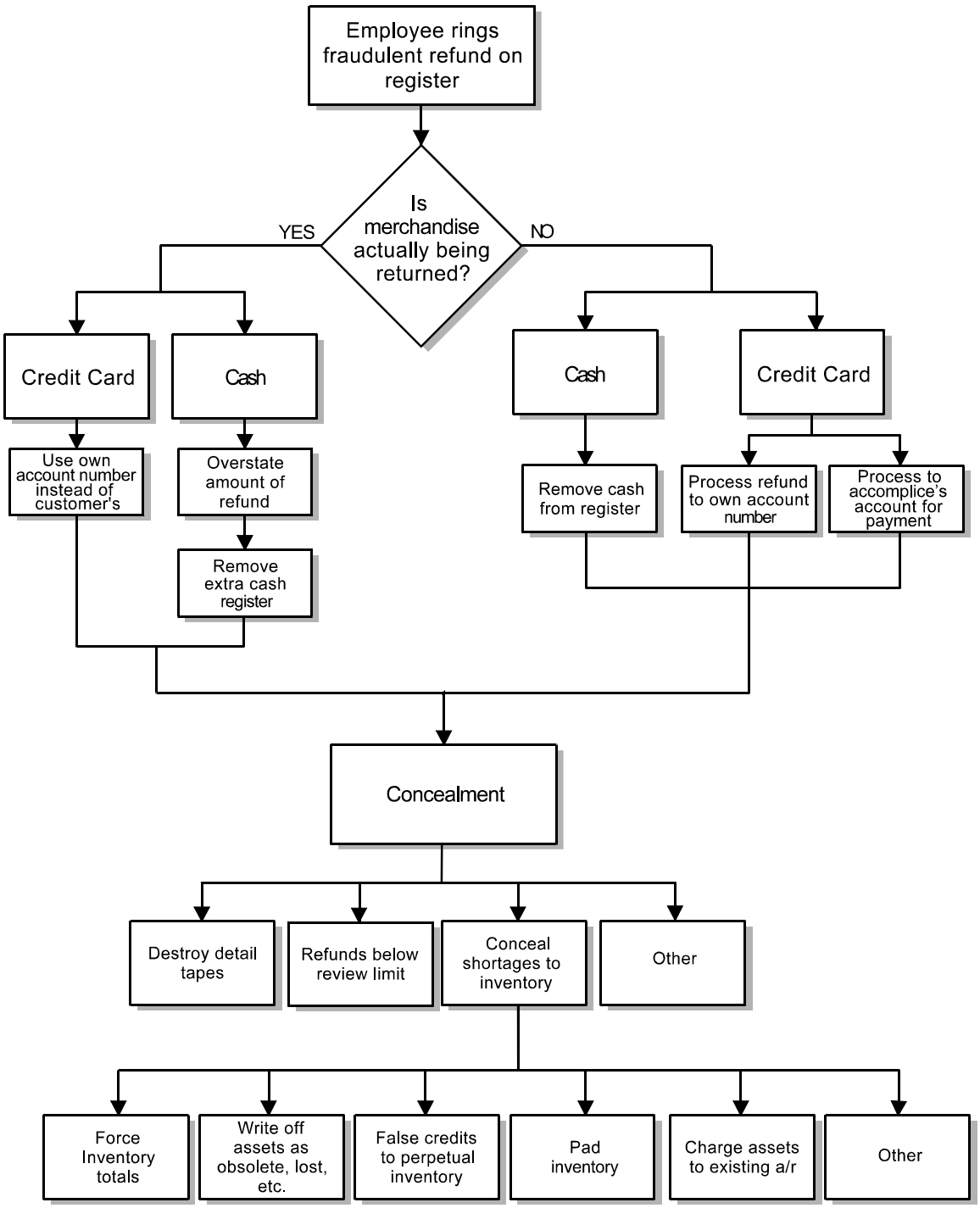
Register Disbursement Schemes

Fraudulent disbursements at the cash register are different from the other schemes that often take place at the register, such as skimming and cash larceny. When cash is stolen as part of a register disbursement scheme, the removal of the cash is recorded.

There are two basic register disbursements schemes: *false refunds* and *false voids*. While the schemes are largely similar, there are a few differences between the two that merit discussing them separately.

False Refunds

A refund is processed at the register when a customer returns an item of merchandise that was purchased from the store. The transaction that is entered on the register indicates that the merchandise is being replaced in the store's inventory and the purchase price is being returned to the customer. In other words, a refund shows cash being disbursed from the register to the customer. (See the "False Refunds" flowchart that follows.)



False Refunds

Fictitious Refunds

In a fictitious refund scheme, an employee processes a transaction as if a customer were returning merchandise, even though there is no actual return. Then the employee takes cash from the register in the amount of the false return. The customer might or might not be aware of the scheme taking place.

For instance, if an employee processes a fictitious return for a $100 pair of shoes, he removes $100 from the register. Two things result from this fraudulent transaction. First, the register log indicates that the shoes were returned, so the disbursement appears to be legitimate. The register log balances with the amount of cash in the register, because the money that was taken by the fraudster is supposed to have been removed and given to a customer as a refund.

The second repercussion is that a debit is made to the inventory system showing that the merchandise has been returned to the inventory. Since the transaction is fictitious, no merchandise is actually returned. The result is that the company's inventory balance on the books is overstated by the amount of the excess refund.

EXAMPLE

A manager created $5,500 worth of false returns, resulting in a large shortage in the company's inventory. He was able to carry on his scheme for several months, however, because (1) inventory was not counted regularly and (2) the perpetrator, the manager, was one of the people who performed inventory counts.

Overstated Refunds

Rather than create an entirely fictitious refund, some employees merely overstate the amount of a legitimate refund and steal the excess money. For example, if a customer returns $100 worth of merchandise, the employee might ring up a $200 return. The employee gives the customer $100 in return for the merchandise and then pockets the remaining $100. This will result in shrinkage of $100 worth of inventory.

Credit Card Refunds

When purchases are made with a credit card rather than cash, refunds appear as credits to the customer's credit card rather than as cash disbursements. Some dishonest employees process false refunds on credit card sales in lieu of processing a normal cash transaction. One benefit of the credit card method is that the perpetrator does not have to physically take

cash from the register and carry it out of the store. By processing the refunds to a credit card account, a perpetrator reaps a financial gain and avoids the potential embarrassment of being caught red-handed taking cash.

In a typical credit card refund scheme, the perpetrator rings up a refund on a credit card sale even though the merchandise is not actually being returned. The employee credits his own credit card number rather than the customer's. The result is that the item's cost is credited to the perpetrator's credit card account.

A more creative and wide-ranging application of the credit card refund scheme occurs when employees process refunds to other people's accounts and receive a portion of the refund as a kickback in return. Suppose a person is $100 short on the rent. That person goes to the retail store where his friend is a teller and has the teller process a credit of $150 to his account. The "customer" then goes to an ATM and withdraws $150 in cash. He pays $50 to the teller and keeps $100 for himself.

Refund schemes are more difficult to perpetrate in many high-tech retail stores where the cash registers have anti-fraud controls that require the refund to be made to the original credit card used for the purchase or that only allow for refunds in the form of a store credit for the current value of the item purchased.

False Voids

Fictitious voids are similar to refund schemes in that they make fraudulent disbursements from the register appear to be legitimate. When a sale is voided on a register, a copy of the customer's receipt is usually attached to a void slip, along with the signature or initials of a manager indicating that the transaction has been approved. (See the "False Voids" flowchart that follows.) To process a false void, the first thing the perpetrator needs is the customer's copy of the sales receipt. Typically, when an employee sets about processing a fictitious void, he simply withholds the customer's receipt at the time of the sale. In many cases, customers do not notice that they are not given a receipt.

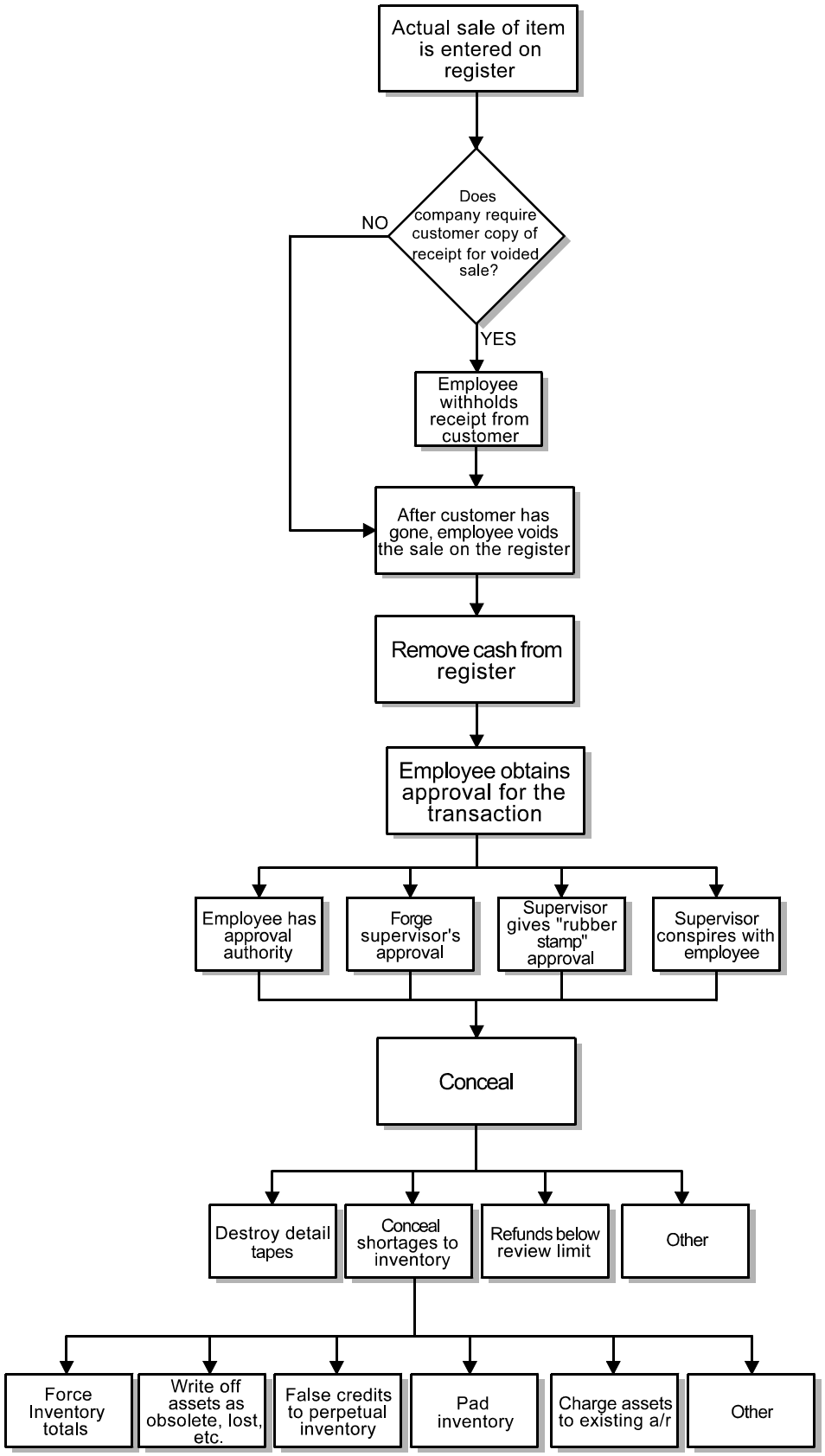
With the customer's copy of the receipt in hand, the culprit rings a voided sale. Whatever money the customer paid for the item is removed from the register as though it is being returned to a customer. The copy of the customer's receipt is attached to the void slip to verify the transaction's authenticity.

Before the voided sale will be perceived as valid, a manager generally must approve the transaction. In many instances, the manager in question simply neglects to verify the voided sale's authenticity. A number of managers will sign almost anything presented to them and thus leave themselves vulnerable to voided sales schemes. It is not a coincidence that the perpetrators of these crimes present their void slips to managers who are lackadaisical about authorizing them. These kinds of managers are generally targeted by the fraudsters and are essential to the schemes' success.

EXAMPLE

An employee processed fraudulent voids, kept customer receipts, and presented them to her supervisors for review at the end of her shift, long after the alleged transactions had taken place. Her supervisors approved the voided sales and the accounts receivable department failed to notice the excessive number of voided sales processed by this employee.

Obviously, not all managers give rubber-stamp approval to voided sales. Some employees must therefore take other routes to get their voided sales "approved." In most of these cases, the perpetrator simply forges his supervisor's authorization on the fraudulent void slips. It is also possible that managers will conspire with register employees and approve false voids in return for a share of the proceeds from the scheme.


Actual sale of item is entered on register
Does company require customer copy of receipt for voided sale?
NO
YES
Employee withholds receipt from customer
After customer has gone, employee voids the sale on the register
Remove cash from register
Employee obtains approval for the transaction
Employee has approval authority
Forge supervisor's approval
Supervisor gives "rubber stamp" approval
Supervisor conspires with employee
Conceal
Destroy detail tapes
Conceal shortages to inventory
Refunds below review limit
Other
Force Inventory totals
Write off assets as obsolete, lost, etc.
False credits to perpetual inventory
Pad inventory
Charge assets to existing a/r
Other

False Voids

Concealing Register Disbursement Schemes

As has already been discussed, two things happen when a false refund or void is entered into the register. The first is that the employee committing the fraud removes cash from the register, and the second is that the item allegedly being returned is debited back into the perpetual inventory. Of course, there really is no merchandise being returned. This leads to inventory shrinkage, a situation in which there is less inventory actually on hand than the perpetual inventory records reflect. A certain amount of shrinkage is expected in any retail industry, but too much of it raises concerns of fraud. It is therefore in the perpetrator's best interest to conceal the appearance of shrinkage on the books.

Inventory is essentially accounted for by a two-step process. The first part of the process is the perpetual inventory, which is a running tabulation of how much inventory *should be on hand*. When a sale of merchandise is made, the perpetual inventory is credited to remove this merchandise from the records. The amount of merchandise that should be on hand is reduced. (Conversely, when merchandise is returned, the perpetual inventory is debited.) Periodically, someone from the company takes a physical count of the inventory, going through the stockroom or warehouse and counting the amount of inventory that *is actually on hand*. The two figures are then compared to see if there is a discrepancy between the perpetual inventory (what should be on hand) and the physical inventory (what is on hand).

In register disbursement schemes, shrinkage is often concealed by overstating inventory during the physical count, especially if taking inventory is one of the perpetrator's duties. The perpetrator simply overstates the amount of inventory on hand so it matches the perpetual inventory. For a more detailed analysis of methods used to conceal inventory shrinkage, please see the "Asset Misappropriation: Inventory and Other Assets" chapter.

Small Disbursements

Another way for employees to avoid detection in a refund scheme is to keep the sizes of the disbursements low. Many companies set limits below which management review of a refund is not required. Where this is the case, employees simply process numerous refunds that are small enough that they do not have to be reviewed.

EXAMPLE

An employee created over 1,000 false refunds, all under the review limit of $15. He was eventually caught because he began processing refunds before store hours and another employee noticed that refunds were appearing on the system before the store opened.

Nevertheless, the man made off with over $11,000 of his employer's money before his scheme was detected.

Destroying Records

One final means of concealing a register scheme is to destroy all records of the transaction. Most concealment methods are concerned with keeping management from realizing that fraud has occurred. When an employee resorts to destroying records, however, he typically has conceded that management will discover his theft. The purpose of destroying records is usually to prevent management from determining *who* the thief is.

Detection of Register Disbursement Schemes

Fictitious Refunds or Voided Sales

Fictitious refunds or voided sales can often be detected when closely examining the documentation submitted with the cash receipts.

- One detection method is to evaluate the refunds or discounts given by each cashier or salesperson. This analysis might point out that a single employee or group of employees has a higher incidence of refunds or discounts than others. Further examination is then necessary to determine if the refunds are appropriate and properly documented.
- Signs in the register area asking customers to ask for and examine their receipts employ the customer as part of the internal control system. This helps ensure that the cashier or salesperson is properly accounting for the sale and prevents employees from using customer receipts as support for false void or refunds.
- Random service calls to customers who have returned merchandise or voided sales can be used to verify the legitimacy of transactions.

Review and Analysis of Decreases in Gross Sales and/or Increases in Returns and Allowances

Analyzing the relationship between sales, cost of sales, and the returns and allowances can detect inappropriate refunds and discounts. If a large cash fraud is suspected, a thorough review of these accounts might enlighten the examiner as to the suspected fraud's magnitude. An analysis of refunds and returns and allowances with the actual flow of inventory might reveal some fraud schemes. The refund should cause an entry to inventory, even if it is damaged inventory. Likewise, a return will cause a corresponding entry to an inventory account. There should be a linear relationship between sales and returns and allowances over a relevant range. Any change in this relationship might point to a fraud

scheme unless there is another valid explanation, such as a change in the manufacturing process, change in product line, or change in price.

Register Disbursement Scheme Red Flags

- There is inappropriate employee separation of duties. For example, register counting and reconciling should not be done by the cashier.
- Cashiers, rather than supervisors, have access to the control keys necessary for refunds and voids.
- The register employee has authority to void his own transactions.
- Register refunds are not carefully reviewed.
- Multiple cashiers operate from a single cash drawer without separate access codes.
- Personal checks from the cashier are found in his register.
- Voided transactions are not properly documented or approved by a supervisor.
- Voided cash receipt forms (manual systems) or supporting documents for voided transactions (cash register systems) are not retained on file.
- There are missing or obviously altered register logs.
- There are gaps in the sequence of transactions on the register logs.
- An excessive number of refunds, voids, or no-sales appear on the register records.
- Inventory totals appear forced.
- There are multiple refunds or voids for amounts just under the review limit.

Prevention of Register Disbursement Schemes

- Review the segregation of duties of key employees who staff the register, as well as the duties of their supervisors.
- As cash is received, ensure that the employees responsible for completing these important tasks are informed of their responsibilities and properly supervised.
- Ensure that an employee other than the register worker is responsible for preparing register count sheets and reconciling them with register totals.
- Make sure that complete register documentation and cash are delivered to the appropriate personnel in a timely manner.
- Be aware that cash thefts are sometimes revealed by customers who have paid money on an account and have not received credit or have been credited for an amount that does not agree with the payment they have made. Complaints and inquiries are also received frequently from banks.
- Closely monitor access to the register and keep access codes secure.
- Analyze the quantity of refunds to detect multiple small refunds.

- Communicate and adhere to the company policy of performing unannounced cash counts.
- Maintain the presence of a manager or supervisor near the area of the cash register as a deterrent to theft.
- Review supporting documents for voided and refunded transactions for propriety (i.e., legitimacy and approvals).
- Review the numerical sequence and completeness of cash register logs.

Check Tampering Schemes

Check tampering is unique among the fraudulent disbursement schemes because it is the one group in which the perpetrator physically prepares the fraudulent check. In most fraudulent disbursement schemes, the culprit generates a payment to himself by submitting some false document to the victim organization, such as an invoice or a timecard. The false document represents a claim for payment and causes the victim organization to issue a check that the perpetrator can convert.

Check tampering schemes are fundamentally different. In these schemes, the perpetrator takes physical control of a check and makes it payable to himself through one of several methods. Check tampering frauds depend upon factors such as access to the company checkbook, access to bank statements, and the ability to forge signatures or alter other information on the face of the check. Most check tampering crimes fall into one of four categories: forged maker schemes, forged endorsement schemes, altered payee schemes, and authorized maker schemes.

Because many business payments are currently still made by check, the bulk of this section will focus on how traditional check-based payments can be manipulated by dishonest employees. However, businesses are increasingly using electronic forms of payment—such as wire transfers, ACH debits, and online bill-pay services—to pay vendors and other third parties. Consequently, the specific implications and considerations of these types of payments will be discussed in a separate section at the end of this chapter.

Forged Maker Schemes

Forgery can include not only the *signing of another person's name* to a document (such as a check) with a fraudulent intent, but also the fraudulent *alteration* of a genuine instrument. This definition is so broad that it would encompass all check tampering schemes. For the

purposes of this text, the definition of forgery has been narrowed to fit the fraud examiner's needs. To properly distinguish the various methods used by individuals to tamper with checks, the concept of "forgeries" will be limited to those cases in which an individual signs another person's name on a check.

The person who signs a check is known as the "maker" of the check. A forged maker scheme can thus be defined as a check tampering scheme in which an employee misappropriates a check and fraudulently affixes the signature of an authorized maker thereon. (See the "Forged Maker Schemes" flowchart that follows.) Frauds that involve other types of check tampering, such as the alteration of the payee or the changing of the amount, are classified separately.

To forge a check, an employee must have access to a blank check, be able to produce a convincing forgery of an authorized signature, and be able to conceal his crime. Concealment is a universal problem in check tampering schemes; the methods used are basically the same whether one is dealing with a forged maker scheme, an intercepted check scheme, or an authorized maker scheme. Therefore, concealment issues will be discussed as a group later in this section.

Obtaining the Check

EMPLOYEES WITH ACCESS TO COMPANY CHECKS

One cannot forge a company check unless one first possesses a company check. Most forgery schemes are committed by accounts payable clerks, office managers, bookkeepers, or other employees whose duties typically include the preparation of company checks. These are people who have access to the company checkbook on a regular basis and are therefore in the best position to steal blank checks.

EMPLOYEES LACKING ACCESS TO COMPANY CHECKS

If perpetrators do not have access to the company checkbook through their work duties, they will have to find other means of misappropriating a check. The method by which a person steals a check depends largely on how the checkbook is handled within a particular company. In some circumstances, the checkbook is poorly guarded and left in unattended areas where anyone can get to it. In other companies, the check stock might be kept in a restricted area, but the perpetrator might have obtained a key or combination to this area, or might know where an employee with access to the checks keeps his own copy of the key or combination. An accomplice might provide blank checks for the fraudster in return for a

portion of the stolen funds. Perhaps a secretary sees a blank check left on a manager's desk or a custodian comes across the check stock in an unlocked desk drawer.

In some companies, checks are computer-generated. When this is the case, an employee who knows the password for preparing and issuing checks can usually obtain as many unsigned checks as he desires. There are an unlimited number of ways to steal a check, each dependent on the way in which a particular company guards its blank checks. In some instances, employees go as far as to produce counterfeit checks.

EXAMPLE

An employee had an accomplice who worked for a check-printing company. The accomplice was able to print blank checks with the account number of the perpetrator's company. The perpetrator then wrote over $100,000 worth of forgeries on these counterfeit checks.

To Whom Is the Check Made Payable?

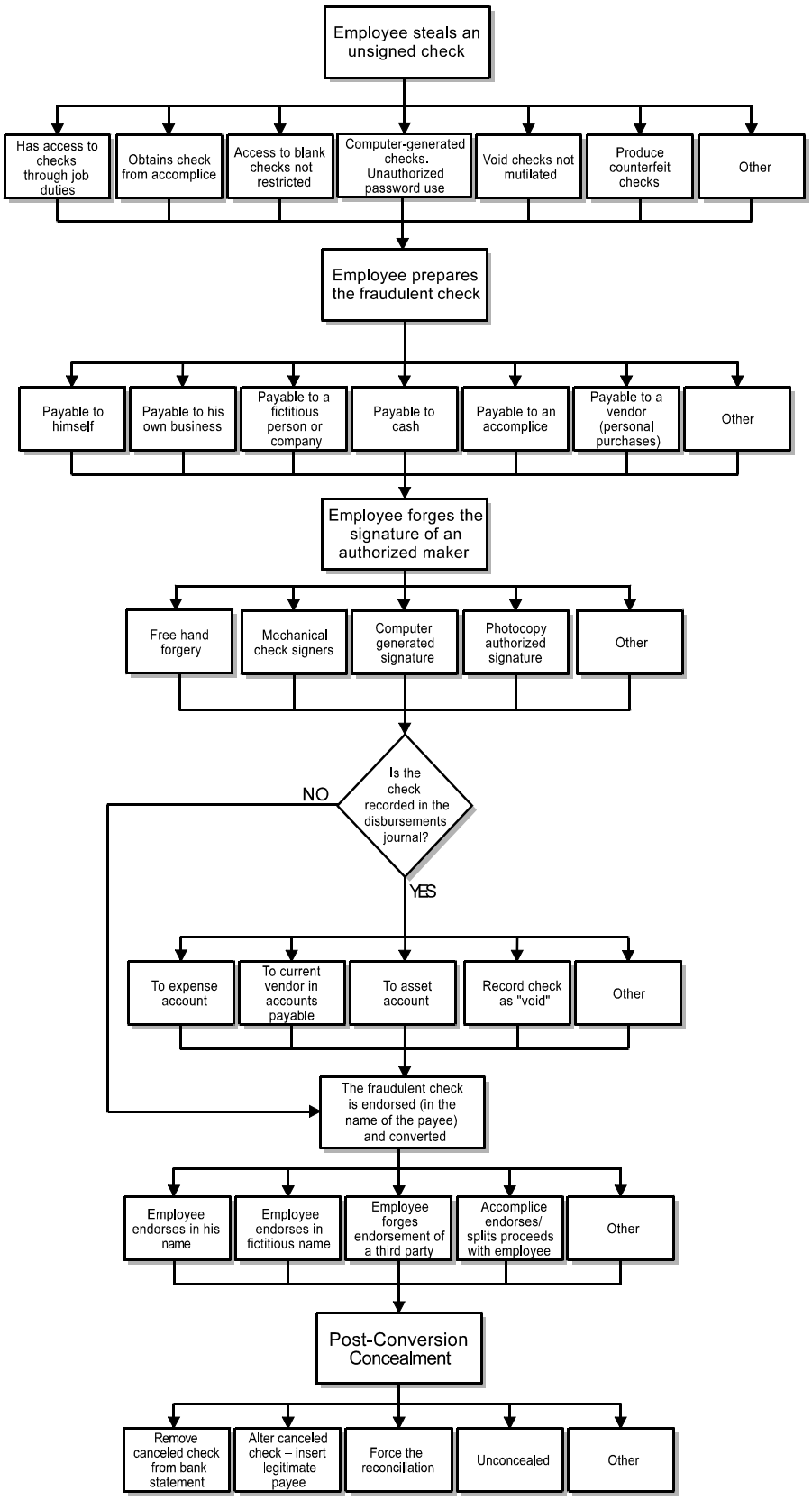
TO THE PERPETRATOR

Once a blank check has been obtained, the perpetrator must decide to whom it should be made payable. In most instances, forged checks are made payable to the perpetrator himself so that they can be easily converted. Canceled checks that are payable to an employee should be closely scrutinized for the possibility of fraud.

If the perpetrator owns his own business or has established a shell company, he will usually write fraudulent checks to these entities rather than himself. These checks are not as obviously fraudulent on their faces as checks made payable to an employee. At the same time, these checks are easy to convert because the perpetrator owns the entity to which the checks are payable.

TO AN ACCOMPLICE

If a fraudster is working with an accomplice, he can make the forged check payable to that person. The accomplice then cashes the check and splits the money with the employee-fraudster. Because the check is payable to the accomplice in his true identity, it is easily converted. An additional benefit to using an accomplice is that a canceled check payable to a third-party accomplice is not as likely to raise suspicion as a canceled check to an employee. The obvious disadvantage to using an accomplice in a scheme is that the employee-fraudster usually has to share the proceeds.



Forged Maker Schemes

TO "CASH"

The perpetrator might also write checks payable to "cash" to avoid listing himself as the payee. Checks made payable to cash, however, must still be endorsed. The perpetrator will have to sign his own name or forge the name of another to convert the check. Checks payable to "cash" are usually viewed more skeptically than checks payable to persons or businesses. Some institutions might refuse to cash checks made payable to "cash."

TO VENDORS

Not all fraudsters forge company checks to obtain cash. Some employees use forged maker schemes to purchase goods or services for their own benefit. These fraudulent checks are made payable to third-party vendors who are uninvolved in the fraud. For instance, an employee might forge a company check to buy a computer for his home. The computer vendor is not involved in the fraud at all. Furthermore, if the victim organization regularly does business with this vendor, the person who reconciles the company's accounts might assume that the check was used for a legitimate business expense.

Forging the Signature

After the employee has obtained and prepared a blank check, he must forge an authorized signature to convert the check. The most obvious method, and the one that comes to mind when one thinks of the word *forgery,* is to simply take pen in hand and sign the name of an authorized maker.

FREE-HAND FORGERY

The difficulty a fraudster encounters when physically signing the authorized maker's name is in creating a reasonable approximation of the true signature. If the forgery appears authentic, the perpetrator will probably have no problem cashing the check. In truth, the forged signature might not have to be particularly accurate. Many fraudsters cash forged checks at liquor stores, grocery stores, or other institutions that are known to be less than diligent in verifying signatures and identification. Nevertheless, a poorly forged signature is a clear red flag of fraud. The maker's signature on canceled checks should be reviewed for forgeries during the reconciliation process.

PHOTOCOPIED FORGERIES

To guarantee an accurate forgery, some employees make photocopies of legitimate signatures. The signature of an authorized signer is copied from some document (such as a business letter) onto a transparency, and then the transparency is laid over a blank check so

that the signature copies onto the maker line of the check. The result is a check with a perfect signature of an authorized maker.

AUTOMATIC CHECK-SIGNING MECHANISMS

Companies that issue a large number of checks sometimes use automatic check-signing mechanisms in lieu of signing each check by hand. Automated signatures are produced with manual instruments, such as signature stamps, or they are printed by computer. Obviously, a fraudster who gains access to an automatic check-signing mechanism will have no trouble forging the signatures of authorized makers. Even the most rudimentary control procedures should severely limit access to these mechanisms.

EXAMPLE

A fiscal officer maintained a set of manual checks that were unknown to other persons in the company. The company used an automated check signer and the custodian of the signer let the officer have uncontrolled access to it. Using the manual checks and the company's check signer, the fiscal officer was able to write over $90,000 worth of fraudulent checks to himself over a period of approximately four years.

The same principle applies to computerized signatures. Access to the password or program that prints signed checks should be restricted, specifically excluding those who prepare checks and those who reconcile the bank statement.

Converting the Check

To convert the forged check, the perpetrator must endorse it. The endorsement is typically made in the name of the payee on the check. Since identification is typically required when one seeks to convert a check, the perpetrator usually needs fake identification if he forges checks to real or fictitious third persons. As discussed earlier, checks payable to "cash" require the endorsement of the person converting them. Without a fake ID, the perpetrator will likely have to endorse these checks in his own name. An employee's endorsement on a canceled check is obviously a red flag.

Forged Endorsement Schemes

Forged endorsements are those check tampering schemes in which an employee intercepts a company check intended to pay a third party and converts the check by endorsing it in the third party's name. In some cases, the employee also signs his own name as a second endorser. (See the "Forged Endorsement Schemes" flowchart that follows.)

A fraudster's main dilemma in a forged endorsement scheme (and in all intercepted check schemes, for that matter) is gaining access to a check after it has been signed. The fraudster must either steal the check between the point where it is signed and the point where it is delivered, or he must re-route the check, causing it to be delivered to a location where he can retrieve it. The manner used to steal a check depends largely upon the way the company handles outgoing disbursements. Anyone who is allowed to handle signed checks might be in a good position to intercept them.

Intercepting Checks Before Delivery

EMPLOYEES INVOLVED IN DELIVERY OF CHECKS

Obviously, the employees in the best position to intercept signed checks are those whose duties include the handling and delivery of signed checks. The most obvious example is a mailroom employee who opens outgoing mail containing signed checks and steals the checks. Other personnel who have access to outgoing checks might include accounts payable employees, payroll clerks, and secretaries.

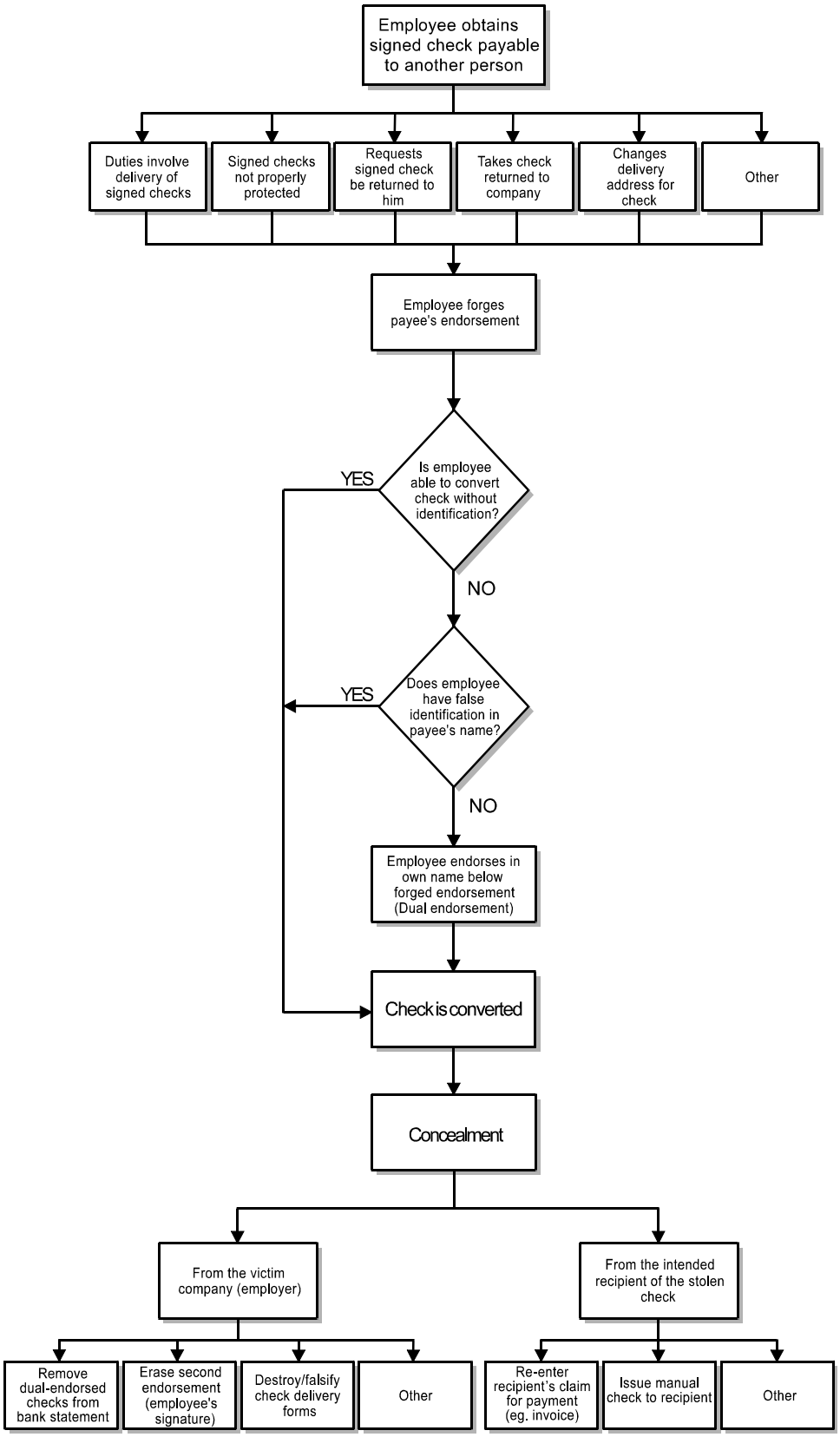
POOR CONTROL OF SIGNED CHECKS

Unfortunately, employees are often able to intercept signed checks because of poor internal controls. For instance, many employees simply find signed checks left unattended in the work areas of the individuals who signed them or the people charged with their delivery. In these cases, it is easy for the perpetrator to steal the check. Another common breakdown occurs when the person who prepares a check is also involved in the delivery of that check once it has been signed.

EXAMPLE

A high-level manager with authority to disburse employee benefits instructed accounts payable personnel to return signed benefits checks to him instead of immediately delivering them to their intended recipients. These instructions were not questioned due to the manager's level of authority within the company. The perpetrator simply took the checks that were returned to him and deposited them into his personal bank account, forging the endorsements of the intended payees.

In addition to the preceding example, secretaries or clerks who prepare checks for their bosses to sign are often responsible for mailing those checks. It is very simple for those employees to make out a fraudulent check and obtain a signature, knowing that the boss will give the signed check right back to them. This scheme is indicative of the key problem with



Forged Endorsement Schemes

occupational fraud: trust. For an office to run efficiently, high-level employees must be able to rely on their subordinates. Yet this reliance is precisely what puts subordinates in a position to defraud their employer.

Theft of Returned Checks

Checks that have been mailed and are later returned to the victim for some reason, such as an incorrect address, are often targeted for theft by fraudsters. Employees with access to incoming mail are able to intercept these returned checks and convert them by forging the intended payee's endorsement.

EXAMPLE

A manager took and converted approximately $130,000 worth of checks that were returned due to noncurrent addresses (he also stole outgoing checks, cashed them, and then declared them lost). The fraudster was well known at his bank and was able to convert the checks by claiming that he was doing it as a favor for the real payees, who were "too busy to come to the bank." The fraudster was able to continue with his scheme because the nature of his company's business was such that the recipients of the misdelivered checks were often not aware that the victim company owed them money. Therefore, they did not complain when their checks failed to arrive. In addition, the perpetrator had complete control over the bank reconciliation, so he could issue new checks to those payees who did complain and then "force" the reconciliation, making it appear that the bank balance and book balance matched when they actually did not.

Re-Routing the Delivery of Checks

Employees might also misappropriate signed checks by altering the addresses to which those checks are mailed. These perpetrators usually replace the payee's legitimate address with an address where the employee can retrieve the check, such as the employee's home or a PO Box the employee controls. In other instances, the perpetrator might purposely misaddress a check so that it will be returned as undeliverable. The employee steals the check after it is returned to the victim organization.

Obviously, proper separation of duties should preclude anyone who prepares disbursements from being involved in their delivery. Nevertheless, the person who prepares a check is often allowed to address and mail it as well. In some instances where proper controls are in place, employees are still able to cause the misdelivery of checks.

EXAMPLE

A clerk in the customer service department of a mortgage company was in charge of changing the mailing addresses of property owners. She was assigned a password that gave her access to make these changes. The clerk was transferred to a new department where one of her duties was the issuance of checks to property owners. Unfortunately, her supervisor forgot to cancel her old password. When the clerk realized this oversight, she would request a check for a certain property owner and then sign onto the system with her old password and change the address of that property owner. The check would be sent to her. The next day, the employee would use her old password to re-enter the system and replace the proper address so that there would be no record of where the check had been sent. This fraudster's scheme resulted in a loss of over $250,000 to the victim company.

Converting the Stolen Check

Once a check has been intercepted, the perpetrator can cash it by forging the payee's signature, hence the term *forged endorsement scheme*. Depending on where he tries to cash the check, the perpetrator may or may not need fake identification at this stage. If a perpetrator is required to produce identification to cash his stolen check, and if he does not have a fake ID in the payee's name, he might use a dual endorsement to cash or deposit the check. In other words, the perpetrator forges the payee's signature as though the payee had transferred the check to him, and then the perpetrator endorses the check in his own name and converts it. When the bank statement is reconciled, dual endorsements on checks should always raise suspicions, particularly when the second signer is a company employee.

Altered Payee Schemes

The second type of intercepted check scheme is the altered payee scheme. This is a form of check tampering in which an employee intercepts a company check intended for a third party and alters the payee designation so that the employee or an accomplice can convert the check. (See the "Altered Payee Schemes" flowchart that follows.) The employee inserts his own name, the accomplice's name, or a fictitious entity's name on the check's payee line. The alteration essentially makes the check payable to the employee (or an accomplice), so there is no need to forge an endorsement and no need to obtain false identification.

Altering Checks Prepared by Others: Inserting a New Payee

The method used to alter the payee designation on a check depends largely on how that check is prepared and intercepted. (Incidentally, the *amount* of the check might also be altered at the same time and by the same method as the payee designation.) Checks prepared

by others can be intercepted by any of the methods discussed in the forged endorsements section. When the perpetrator intercepts a check that has been prepared by someone else, there are basically two methods that can be employed to change the payee. The first is to insert the false payee's name in place of the true payee's. The true name might be scratched out with a pen or covered up with correction fluid. Another name is then entered on the payee designation line. These kinds of alterations are usually simple to detect.

A more sophisticated method occurs when the fraud perpetrator enters the accounts payable system and changes the payees' names before checks are generated. Anyone with a password that permits access to the accounts payable address file can accomplish this.

EXAMPLE

An accounts payable employee was so trusted that her manager allowed her to use his computer password in his absence. The password permitted access to the accounts payable address file. This employee waited until the manager was absent and then selected a legitimate vendor with whom her company did a lot of business. She held up the vendor's invoices for the day and used the manager's log-in code to change the vendor name and address to that of a fictitious company after work. The new name and address were run through the accounts payable cycle with an old invoice number, causing a fraudulent check to be issued. The victim company had an automated duplicate invoice test, but the perpetrator circumvented it, substituting "1" for "I" and "0" (zero) for capital "O." The next day, the employee would replace the true vendor's name and address and manipulate the check register so that the check payable to the fictitious vendor was concealed. Approximately $300,000 in false checks was issued using this method.

Altering Checks Prepared by Others: "Tacking On"

The other method that can be used by perpetrators to alter checks prepared by others is "tacking on" additional letters or words to the end of the real payee designation. For instance, checks payable to "ABC" company might be altered to read "A.B. Collins." The employee then cashes the checks in the name of A.B. Collins. In these cases, the simple inclusion of a filler line after the payee designation would prevent the loss.

In addition to altering the payee designation, the amount of the check can be altered by tacking on extra numbers if the person preparing the check is careless and leaves space for extra numbers in the "amount" portion of the check.

Altering Checks Prepared by the Fraudster: Erasable Ink

When the perpetrator prepares the check that is to be altered, the schemes tend to be a bit more sophisticated. The reason for this is obvious: If the perpetrator is able to prepare the check himself, he can prepare it with the thought of how the payee designation will be changed. One of the most common ways to prepare a check for alteration is to write or type the payee's name (and possibly the amount) in erasable ink. After an authorized maker signs the check, the perpetrator retrieves the check, erases the payee's name, and inserts his own name.

EXAMPLE

A bookkeeper printed small checks to a local supplier and had the company's owner sign them. The bookkeeper then put the checks back in the printer so she could alter the payee and check amount. For instance, the owner might sign a $10 check that later became a $10,000 check. These checks were entered in the disbursements journal as payments for aggregate inventory to the company's largest supplier, who received several large checks each month. The bookkeeper stole over $300,000 from her employer in this scheme.

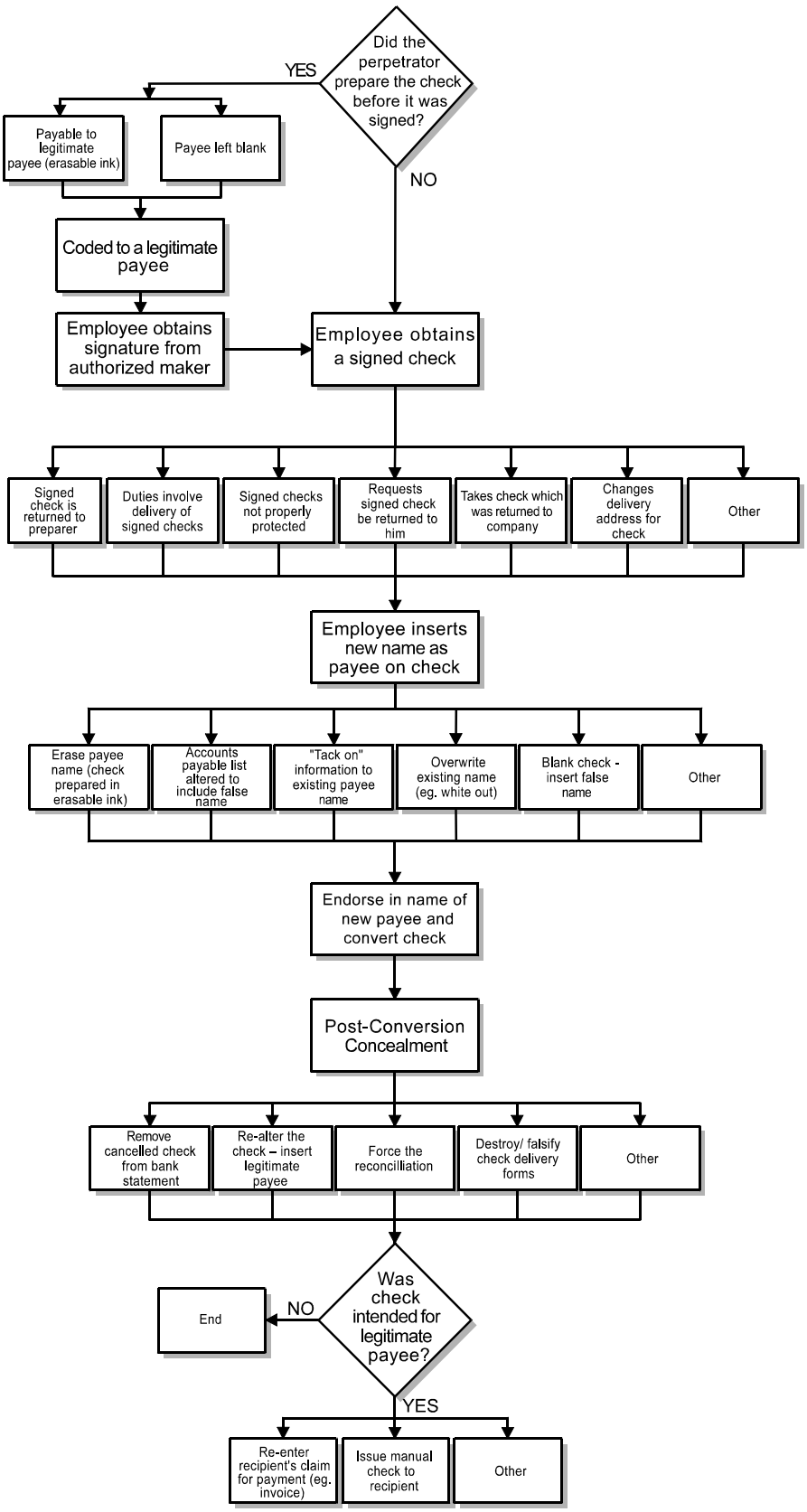
Where a proper separation of duties is in place, a person who prepares a check should not be permitted to handle the check after it has been signed. Nevertheless, this is exactly what happens in most altered payee schemes. The person who prepares the check knows that the maker of the check will return it to him after it has been signed.

Altering Checks Prepared by the Fraudster: Blank Checks

The most egregious example of poor controls in the handling of signed checks is one in which the perpetrator prepares a check, *leaves the payee designation blank*, and submits it to an authorized maker who signs the check and returns it to the employee. Obviously, this makes it quite easy for the perpetrator to designate himself or an accomplice as the payee. Common sense should prevent anyone from giving a signed, blank check to another person. Nevertheless, this is a fairly common occurrence, especially when the perpetrator is a trusted long-time employee.

Converting Altered Checks

As with all other types of fraudulent checks, conversion is accomplished by endorsing the checks in the payee's name. Conversion of fraudulent checks has already been discussed in previous sections and will not be re-examined here.



Altered Payee Schemes

Authorized Maker Schemes

The final check tampering scheme, the authorized maker scheme, might be the most difficult to defend against. An authorized maker scheme occurs when an employee with signature authority on a company account writes fraudulent checks for his own benefit and signs his own name as the maker. (See the "Authorized Maker Schemes" flowchart that follows.) The perpetrator in these schemes can write and sign fraudulent checks himself. He does not have to alter a pre-prepared document or forge the maker's signature.

Overriding Controls Through Intimidation

When a person is authorized to sign company checks, preparing the checks is easy. The employee simply writes and signs the documents the same way he would with any legitimate check. In most situations, check signers are owners, officers, or otherwise high-ranking employees and thus have or can obtain access to all the blank checks they need. Even if company policy prohibits check signers from handling blank checks, the perpetrator can normally use his influence to overcome this impediment. What employee is going to tell the CEO that he can't have a blank check?

The most basic way an employee accomplishes an authorized maker scheme is to override controls designed to prevent fraud. Most authorized signatories have high levels of influence within their companies. The perpetrators use this influence to deflect questions about fraudulent transactions.

A common authorized maker scheme is one in which a majority owner or sole shareholder uses his company to pay personal expenses directly out of company accounts. Instead of paying personal expenses, the perpetrator might cut checks directly to himself, his friends, or his family. Using fear of job security as a weapon, the owner can maintain a work environment in which employees are afraid to question these transactions.

High-level managers or officers might also use their authority to override controls in companies with absent or inattentive owners. Intimidation can play a large part in the commission and concealment of occupational fraud schemes involving powerful individuals.

EXAMPLE

The manager of a sales office stole approximately $150,000 from his employers over a two-year period. This manager had primary check-signing authority and abused this power by writing company checks to pay his personal expenses. The manager's fraudulent activities

were well known by certain members of his staff, but these employees' careers were controlled by the perpetrator. Fear of losing their jobs combined with lack of a proper whistleblowing structure prevented the manager's employees from reporting his fraud.

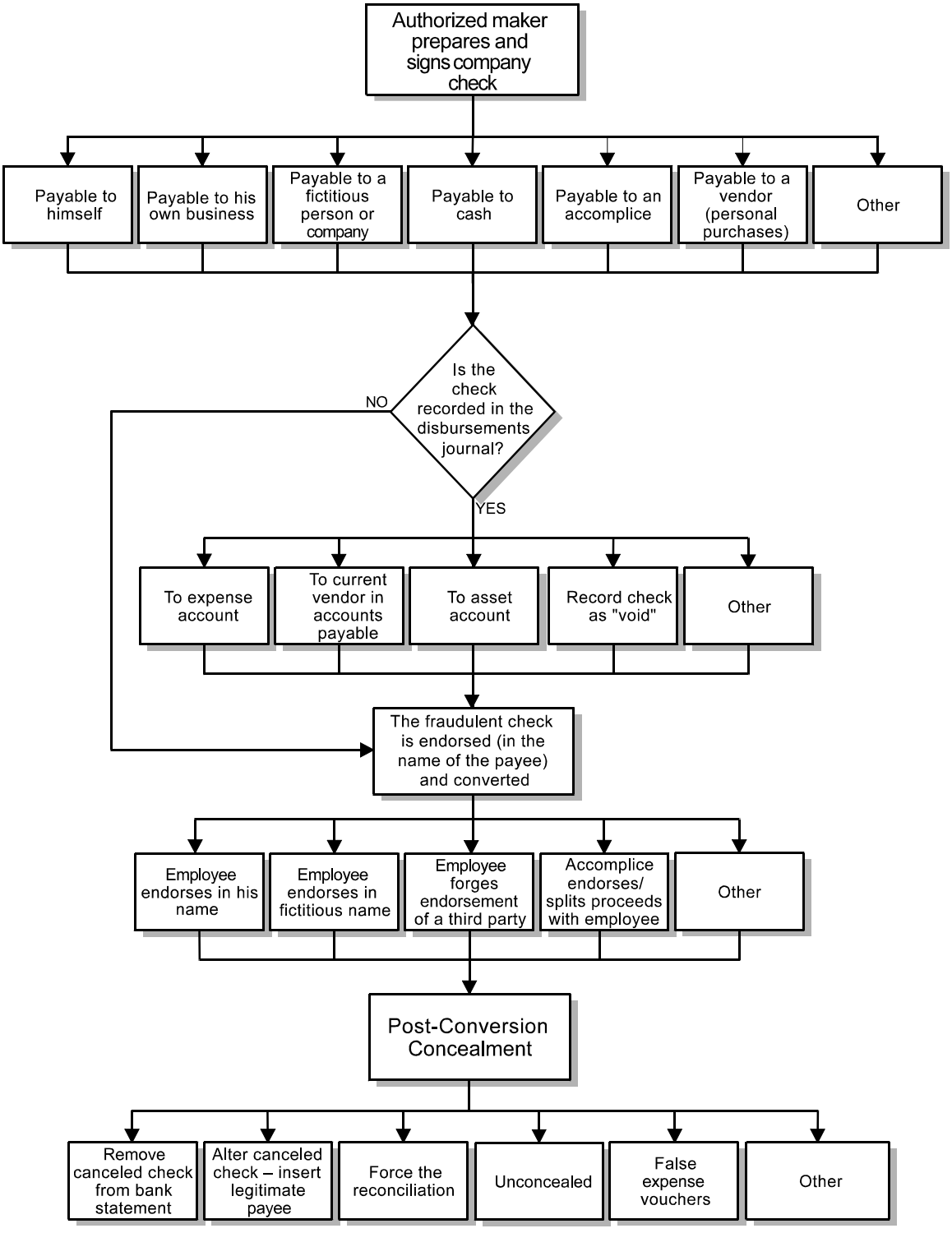
Poor Controls

Although overriding controls is the most obvious way to execute an authorized maker scheme, it is not the most common. Far more of these schemes occur because no one is paying attention to the accounts and few controls are present to prevent fraud. Some employees who write checks to themselves or to purchase items for themselves simply code the checks to expense accounts that they know are not likely to be reviewed.

The failure to closely monitor accounts is supplemented by lack of internal controls, specifically the absence of separation of duties in the cash disbursements process. Employees who commit authorized maker fraud are often in charge of reconciling the business's bank accounts. This is especially common in small businesses. Employees with total control over the disbursements process are in a perfect position to write fraudulent checks for their own benefit.

EXAMPLE

The bookkeeper of a medium-sized company was charged with paying all bills and preparing the company payroll. She had access to an automatic check signer and total control over company bank accounts. The bookkeeper wrote extra checks to herself, coded the expenditures to payroll, and destroyed the canceled checks when they were returned with the bank statement.



Authorized Maker Schemes

Concealing Check Tampering Schemes

Most check tampering schemes do not consist of a single occurrence, but instead continue over a period of time. Therefore, concealing the fraud is arguably the most important aspect of the scheme. If an employee intended to steal a large sum of money and escape to another country, hiding the fraud might not be so important. But the vast majority of occupational fraudsters remain employees of their companies as they continue to steal from them, which makes concealment the key to the crime.

Concealment of the fraud means not only hiding the criminal's identity, but also hiding the fact that a fraud has even occurred. The most successful frauds are those in which the victim organization is unaware that it is being robbed. Obviously, once a business learns that it is being victimized, it will take steps to find the source and put a stop to the scheme.

Check tampering schemes can present especially complex concealment problems for dishonest employees. In other types of fraudulent disbursements, such as invoice or payroll schemes, someone other than the perpetrator enters the fraudulent payment in the books as a legitimate transaction. The payments in those schemes are generated by the production of false documents that cause accounts payable personnel to think that money is owed to a particular person or vendor. When accounts payable issues a disbursement for a fake invoice, it does so because it believes the invoice to be genuine. The payment is then entered in the books as a legitimate payment. In other words, the perpetrator generally does not have to worry about concealing the payment in the books because someone else unwittingly does it for him. But in forgery and authorized maker schemes, the perpetrator is the one writing the check, and he is usually the one coding the check in the disbursements journal. He must "explain" the check on the books.

Forged endorsement schemes and altered payee schemes are different because they involve the alteration of checks that were already prepared and coded by someone else. Nevertheless, they create a problem for the perpetrator because the intercepted check was intended for a legitimate recipient. Someone is out there waiting for the check that the perpetrator has taken. The culprit in these schemes must worry not only about hiding the fraud from his employer, but also about appeasing the intended payee.

The Fraudster Reconciling the Bank Statement

A large percentage of those who perpetrate check tampering frauds are involved in reconciling the company's bank statement. The bank statement that a company receives

normally includes the canceled checks that have been cashed in the preceding period. A person who reconciles the accounts is therefore in a position to hide the existence of any fraudulent checks he has written to himself. He can remove the fraudulent checks, alter the bank statement, or both.

In forged maker and authorized maker schemes, the perpetrator usually has to code the check in the disbursements journal. The most basic way to hide the check is to code it as "void" or to include no listing at all in the journal. Then, when the bank statement arrives, perpetrators remove the fraudulent check from the returned checks and destroy it or alter the bank statement. Now there is no record of the payment in the journal and no physical evidence of the check on hand. Of course, the bank will have a copy of the check, but unless someone questions the missing check, it is unlikely that the company will discover the problem. And since the perpetrator is the one who reconciles the account, it is unlikely that anyone will even notice that the check is missing.

The problem with simply omitting the fraudulent check from the disbursements journal is that the bank balance will not reconcile to the book balance. For instance, if the perpetrator wrote a $25,000 check to himself and did not record it, then the book balance will be $25,000 higher than the bank balance ($25,000 was taken out of the bank account by the perpetrator, but was not credited out of the company's cash account). Perpetrators usually omit their illegal checks from the disbursements journal only in situations in which they personally reconcile the bank statement and no one reviews their work, thus allowing fraudsters to "force" the reconciliation. In other words, fraudsters report that the bank balance and book balance match when in fact they do not.

Some victim organizations simply do not regularly reconcile their accounts. This makes it easy for employees to write checks without recording them. In a system in which controls are so lax, almost any concealment method will be effective to disguise fraud. In fact, it might not be necessary to make any effort at all to conceal the crime.

Some fraudsters physically alter the bank statement to cause it to match the company's book balance. For instance, a person engaging in a forged maker scheme might decide to steal blank checks from the bottom of the check stock. These checks are out of sequence and therefore will be listed last on the bank statement. This employee can delete the clump of fraudulent checks at the end of the statement and alter the balance to match the victim company's books.

Re-Alteration of Checks

In altered payee schemes, remember that it is common for the perpetrator to take a check intended for a legitimate recipient and then alter the check so that the perpetrator becomes the designated payee. But a canceled check payable to an employee will obviously raise suspicions of fraud. Therefore, some employees re-alter their fraudulent checks when the bank statement arrives. It has already been discussed how employees can alter checks by writing the payee's name in erasable ink when the check is prepared. These employees obtain a signature for the check and then erase the true payee's name and insert their own. When the fraudulent checks return with the bank statement, the employee erases his own name and re-enters the proper payee's name. Thus, there will be no appearance of mischief.

Miscoding Fraudulent Checks

Rather than omit a fraudulent check from the disbursements journal or list it as void, the perpetrator might write a check payable to himself but list a different person as the payee on the books. Usually, the fake payee is a regular vendor—a person or business that receives numerous checks from the victim company. Employees tend to pick known vendors for these schemes because one extra disbursement to a regular payee is less likely to be noticed than a check to an unknown person.

The fraudster can also conceal a fraudulent check by overstating the amounts of *legitimate* disbursements in the journal to absorb a fraudulent check's cost. For instance, assume that a company owes $10,000 to a particular vendor. The fraudster would write a check to the vendor for $10,000, but enter the check in the disbursements journal as a $15,000 payment. The company's disbursements are now overstated by $5,000. The fraudster can write a $5,000 check to himself and list that check as void in the disbursements journal. The bank balance and the book balance will still match because the cost of the fraudulent check was absorbed when the amount of the legitimate check was overstated. Of course, the fact that the canceled checks do not match the entries in the journal should indicate potential fraud. This type of concealment is really only effective when the bank accounts are not closely monitored or where the employee is in charge of reconciling the accounts.

If possible, fraudsters will try to code their fraudulent checks to existing accounts that are rarely reviewed or to accounts that are very active. Most of these checks are coded to expense accounts or liability accounts. This particular method can be very effective in concealing fraud, particularly when the victim company is not diligent in reconciling its bank accounts. For instance, some organizations reconcile their accounts by cross-referencing

check numbers with the amounts of the checks, but they do not verify that the payee on the actual check matches the payee listed in the disbursements journal. These organizations will be unable to detect checks that have been coded to the wrong payee in the disbursements journal.

Re-Issuing Intercepted Checks

In intercepted check schemes, the fraudster faces detection not only through his employer's normal control procedures, but also by the intended recipients of the stolen checks. When the real payees do not receive their checks, they are likely to complain. These complaints, in turn, could trigger a fraud investigation. One way for a fraudster to avoid this problem is to issue new checks to the intended payees.

EXAMPLE

An accounts payable troubleshooter was in charge of auditing payments to all suppliers, reviewing supporting documents, and mailing checks. Every once in a while, she would purposely fail to mail a check to a vendor. The vendor, of course, called accounts payable about the late payment and was told that the invoice had been paid on a certain date. Since accounts payable did not have a copy of the canceled check (because the fraudster was still holding it), it would call the troubleshooter to research the problem. Unfortunately for the company, the troubleshooter was the one who had stolen the check; she told accounts payable to issue another check to the vendor while she stopped payment on the first check. Thus, the vendor received his payment, and instead of stopping payment on the first check, the troubleshooter deposited it into her own account.

Fraudulent Supporting Documents

Whereas some perpetrators attempt to wipe out all traces of their fraudulent disbursements by destroying the checks, forcing the bank reconciliation, and so on, others opt to justify their checks by manufacturing fake support for them. These individuals prepare false payment vouchers, including false invoices, purchase orders, or receiving reports, to create an appearance of authenticity. This concealment strategy is only practical when the employee writes checks payable to someone other than himself (such as an accomplice or a shell company). A check made payable to an employee might raise suspicions regardless of any supporting documents that he manufactures.

Detection of Check Tampering Schemes

Account Analysis Through Cut-Off Statements

Bank cut-off statements should be requested for 10 to 15 days after the balance sheet's closing date. These statements may be used to detect cash fraud during periods between monthly bank statements. Auditors often use cut-off statements to ensure that income and expenses are reported in the proper period. If employees know that a cut-off statement might be ordered at any time during the month and reviewed independently, cash fraud will be less likely.

A cut-off statement is generally ordered from the bank, delivered unopened to the auditor (or outsider), and reconciled. It can be ordered at any time during the accounting cycle. If cut-off bank statements are not ordered or received, obtain the following period bank statement and perform account analysis and investigation.

Bank Reconciliations

Copies of the bank reconciliations and account analysis should be obtained along with the complete set of bank statements on all checking and savings accounts, as well as certificates of deposit and other interest-bearing and non-interest-bearing accounts. From the reconciliations, perform the following tests:

- Confirm the mathematical accuracy of the reconciliation.
- Examine the bank statement for possible alterations.
- Trace the balance on the statement back to the bank cut-off and bank confirmation statements.
- Foot the balance to the company's ledger.
- Trace the deposits in transit to the bank cut-off statement to ensure recording in the proper period.
- Examine canceled checks and compare them to the list of outstanding checks.
- Sample supporting documentation of checks written for a material amount.
- Verify supporting documentation on outstanding checks written for a material amount.
- Verify accuracy of nonoperational-cash or cash-equivalent accounts (CDs and other investment accounts). Analysis should include the verification of the institution holding the funds, interest rate, maturity date, beginning and ending balances, and current period activity. Book and bank balances should be compared and any accruals of interest analyzed.

Bank Confirmation

Another method related to the cut-off statement is the bank confirmation request. Unlike the cut-off statement, this detection method is merely a report of the balance in the account as of the date requested. This balance should be requested to confirm the statement balance, as well as any other necessary balance date. If fraud is occurring at the bank reconciliation stage, this independent confirmation might prove to be very helpful.

Check Tampering Red Flags

The following irregularities might indicate fraud:

- Voided checks might indicate that employees have embezzled cash and charged the embezzlement to expense accounts. When the expense is paid (from accounts payable), fraudulent checks are marked and entered as void and removed from distribution points. An account-balancing journal entry is then made. The list of voided checks should be verified against physical copies of the checks. Bank statements should be reviewed to ensure that voided checks have not been processed.
- Missing checks might indicate lax control over the physical safekeeping of checks. Stop payments should be issued for all missing checks.
- Checks payable to employees, with the exception of regular payroll checks, should be closely scrutinized. Such an examination might indicate other schemes, such as conflicts of interest, fictitious vendors, or duplicate expense reimbursements.
- Altered endorsements or dual endorsements of returned checks might indicate possible tampering.
- Returned checks with obviously forged or questionable signature endorsements should be verified with the original payee.
- Altered payees on returned checks should be verified with the intended payee.
- Duplicate or counterfeit checks more than likely indicate fraud. These checks might be traceable to the depositor through bank check coding.
- Questionable deposit dates should be matched to the corresponding customer accounts.
- An examination of all cash advances might reveal that not all advances were properly documented and, therefore, inappropriate payments have been made to employees.
- Customer complaints regarding payments not being applied to their accounts should be investigated.
- A questionable payee or payee address on a check should trigger review of the corresponding check and support documentation.

Prevention of Check Tampering Schemes

Check Disbursement Controls

The following list of activities will help tighten controls and possibly deter employees from giving in to the temptation to commit check fraud.

- Check "cutting" and preparation is not done by a signatory on the account.
- Checks are mailed immediately after signing.
- Theft control procedures are adhered to.
- Accounts payable records and addresses are secure from possible tampering. Changes in vendor information should be verified.
- Bank statements should be reviewed diligently to ensure that amounts and signatures have not been altered.
- Bank reconciliations should be completed immediately after monthly statements are received
- Bank reconciliations are not made by signatories on the account.
- Bank statements should be reconciled and reviewed by more than one person.
- Appropriate separation of duties should be documented and adhered to.
- Detailed comparisons are routinely made between check payees and the payees listed in the cash disbursements journal.
- Personnel responsible for handling and coding checks are periodically rotated, keeping total personnel involved to a minimum.

Bank-Assisted Controls

Companies should work in a cooperative effort with banks to prevent check fraud. Consider the following control measures that might be taken in regard to a firm's checking accounts.

- Establish maximum amounts above which the company's bank will not accept checks drawn against the account.
- Use positive pay banking controls. Positive pay allows a company and its bank to work together to detect fraudulent items presented for payment. The company provides the bank with a list of checks and amounts that are written each day. The bank verifies items presented for payment against the company's list. The bank rejects items that are not on the list. Investigations are conducted as to the origin of the "non-listed" items.

Physical Tampering Prevention

The following list details check tampering prevention techniques that are being used today by some institutions to secure businesses' check integrity. These methods can be used individually or in combination.

- Signature line void safety band—The word VOID appears on the check when photocopied.
- Rainbow foil bar—A horizontal colored bar placed on the check fades and is shaded from one bar to the next. Photocopied foil bars appear solid.
- Holographic safety border—Holographic images are created in a way that reflects light to reveal a three-dimensional graphic.
- Embossed pearlescent numbering—Checks are numbered using a technique that is revealed by a colored highlighter pen or by a bright light held behind the check.
- Other chemical voids—Checks reveal an image or the word VOID when treated with an eradicator chemical.
- Micro line printing—Extremely small print is too small to read with the naked eye and becomes distorted when photocopied.
- High-resolution microprinting—Images are produced on the check in high resolution. This technique is very difficult to reproduce.
- Security inks—Checks contain inks that react with eradication chemicals, reducing a forger's ability to modify the check.
- Watermark backers—Hidden images can only be seen when the check is held at an angle. This image is very difficult to reproduce.

Check Theft Control Procedures

It is very important to provide internal controls that will minimize the possibility of check tampering and theft. The following is a list of items that should be incorporated into companies' policies and procedures to help deter check tampering.

- New checks should be purchased from reputable, well-established check producers.
- Unused checks should be stored in a secure area, such as a safe, vault, or other locked area. Security to this area should be restricted to authorized personnel only. Routinely change keys and access codes to storage areas.
- Review all hiring procedures. One of the most important means of fighting fraud is to not hire people with questionable backgrounds. Develop a distinct separation of duties in the accounts payable department, including written policies and procedures for all personnel who have the opportunity to handle checks, from mailroom clerks to the CEO.
- Use electronic payment services to handle large vendor and financing payments, eliminating the use of paper checks.
- Report lost or stolen checks immediately.
- Properly and securely store canceled checks.

- Destroy unused checks for accounts that have been closed.
- Printed and signed checks should be mailed immediately after signing.

Electronic Payment Tampering

As businesses move to using electronic payments—such as automated clearing house (ACH) payments, online bill payments, and wire transfers—in addition to or instead of traditional checks, fraudsters are adapting their methods to manipulate these payments as well. Some of these fraudsters abuse their legitimate access to their employer's electronic payment system; these schemes are similar to traditional check tampering frauds carried out by authorized makers. Others gain access through social engineering or password theft, or by exploiting weaknesses in their employer's internal control or electronic payment system. Regardless of the means by which they log in to the system, the dishonest employees use this access to fraudulently initiate or divert electronic payments to themselves or their accomplices.

As with other schemes, once the fraudulent payment has been made, the employee must cover his tracks. However, the lack of physical evidence and forged signatures can make concealment of fraudulent electronic payments less challenging than other check tampering schemes. Some fraudsters attempt to conceal their schemes by altering the bank statement, miscoding transactions in the accounting records, or sending fraudulent payments to a shell company with a name similar to that of an existing vendor. Others merely rely on the company's failure to monitor or reconcile its accounts.

Prevention and Detection of Electronic Payment Tampering

Internal Controls

The most important practice for preventing and detecting electronic payment fraud is separation of duties. For example, in the case of online bill payments, such as those made through a bank's website or a third-party business-to-business payment service, separate individuals should be responsible for maintaining payment templates, entering payments, and approving payments. For wire transfers, duties for creating, approving, and releasing wires should be segregated. And to prevent attempts to conceal fraudulent electronic payment activity, no individual involved in the payment process should reconcile the bank statement or even have access to it. In addition to separating duties, companies should consider segregating their bank accounts to maintain better control over them—for example, separate accounts can be used for paper and electronic transactions.

Account monitoring and reconciliation should be performed daily so as to quickly spot and notify the bank of any unusual transactions. Depending on the accounting software in use at the company and the account reconciliation offerings of its bank, much of the reconciliation process can be automated. Additionally, many banks are able to provide daily itemized reports of outstanding payments in addition to a list of those payments that have already cleared.

In guarding against improper access to electronic payment systems, proper management and protection of user access and account information are essential. All log-in information, such as usernames and passwords, should be heavily guarded, with passwords changed frequently and user access immediately deactivated for any user who no longer has a need for it (e.g., a terminated employee or an employee who has changed roles). Although most electronic payment systems will eventually time out, users should log off immediately when they are finished using the system or if they need to leave their computer unattended, even if only for a short time. Unattended computers that are logged on to a payment system provide fraudsters with a free pass to the company's bank account. In one instance, an employee who was working in the company's electronic payment system left his computer unattended for less than ten minutes so that he could grab a cup of coffee. During that time, another employee who shared an office with him was able to wire $3,273 to an existing vendor with whom he was in collusion. Because the victim company performed daily account reconciliations, the fraud was caught the next day. The fraudster was fired immediately, and the individual who left his computer unattended while logged on to the system was reprimanded.

Bank Security Services

Most large banks offer a number of security services that can help business account holders mitigate fraud through early detection and prevention of fraudulent electronic payments. For example, ACH blocks allow account holders to notify their banks that ACH debits—whether authorized or not—should not be allowed on specific accounts. ACH filters enable account holders to provide their banks with a list of defined criteria (such as the sending company ID, account number, and transaction code) against which banks can filter ACH debits and reject any unauthorized transactions. Positive pay for ACH is another security feature offered by banks to their account holders. With positive pay, banks match the details of ACH payments with those on a list of legitimate and expected payments provided by the account holder. Only authorized electronic transactions are allowed to be withdrawn from the account; exceptions are reported to the customer for review.

Organizations can also set up their commercial banking software to restrict access to specific banking activities—such as viewing transactions, viewing bank statements, initiating electronic payments, or setting up ACH blocks or filters—to designated individuals. Companies should incorporate this feature into their internal control system to enhance separation of duties. For example, any individual authorized to make payments should not be permitted to set up ACH blocks or filters, or to submit positive pay information. In addition, businesses can customize their banking software to incorporate features such as dual authorization for certain transactions and daily or individual transaction limits.

Companies can further enhance their protection against unauthorized access to an electronic payment system through the use of their banks' multifactor authentication tools, mechanisms that combine two or more methods to validate the identity of the person attempting to access the system. These tools—such as tokens (physical devices that authorized users provide in addition to their passwords to prove their identities electronically), digital certificates, smart cards, and voiceprint recognition software—can help businesses overcome the problem of compromised credentials, such as usernames and passwords.

Billing Schemes

The asset misappropriation schemes discussed up to this point—skimming, larceny, register schemes, and check tampering—all require the scheme's perpetrator to physically take cash or checks from his employer. The next three sections will cover a different kind of asset misappropriation scheme, one which allows the perpetrator to misappropriate company funds without ever actually handling cash or checks while at work. These schemes succeed by making a false claim for payment upon the victim organization. This group consists of *billing schemes* (which attack the company's purchasing function), *payroll schemes*, and *expense reimbursement schemes*. The most common of these is the billing scheme.

Billing schemes are a popular form of employee fraud mainly because they offer the prospect of large rewards. Since most businesses' disbursements are made in the purchasing cycle, larger thefts can be hidden through false-billing schemes than through other kinds of fraudulent disbursements. There are three principal types of billing schemes: false invoicing via shell companies, false invoicing via non-accomplice vendors, and personal purchases made with company funds.

Invoicing Via Shell Companies

Forming a Shell Company

Shell companies are business entities that typically have no physical presence (other than a mailing address), no employees, and generate little, if any, independent economic value. Shell companies are not necessarily illegal or legitimate, but for the purposes of this text we will assume that shell companies are formed for committing and concealing fraud. They might be nothing more than a fabricated name and address that an employee uses to collect disbursements from false billings. However, since the checks received will be made out in the shell company's name, the perpetrator will normally also set up a bank account in his new company's name so he can deposit and cash the fraudulent checks. (See the "False Billings from Shell Companies" flowchart that follows.)

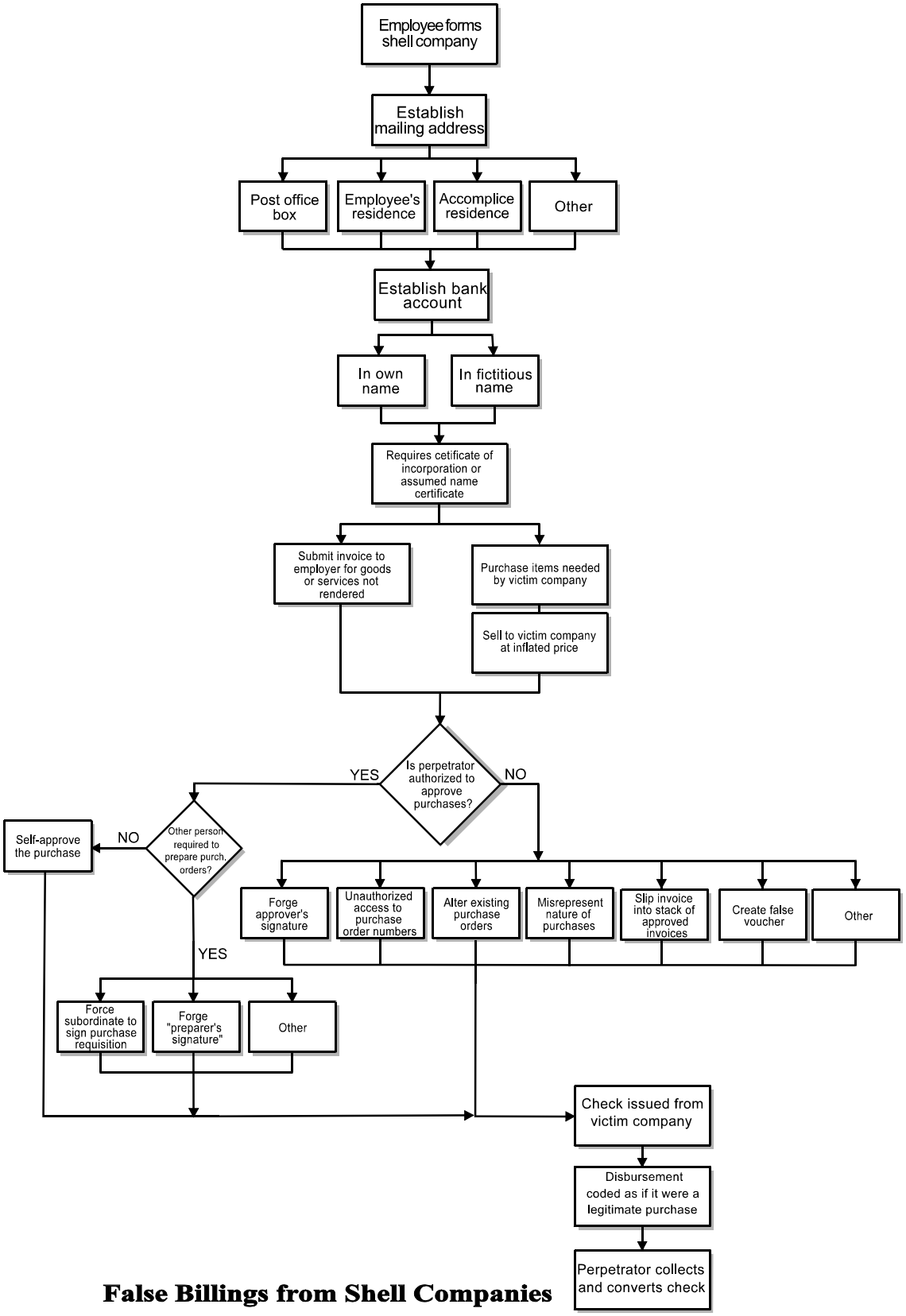
A person will probably have to present a bank with a certificate of incorporation or an assumed-name certificate in order to open a bank account for a shell company. These are documents that a company must obtain through the government. The documents can be forged, but it is more likely that the perpetrator will simply file the requisite paperwork and obtain legitimate documents from the relevant jurisdiction. This can usually be accomplished for a small fee, the cost of which will be more than offset by a successful fraud scheme.

If it is discovered that a vendor is falsely billing a company, investigators for the victim company might be able to identify the suspicious company's owner by reviewing its business registration filings, which are a matter of public record in many countries.

To avoid being detected through a records search, some perpetrators form their shell companies under another name. It is common, for instance, for employees to set up shell companies in the name of a spouse or other close relative. Male fraudsters often establish shell companies under their wives' maiden names. An employee might also form the company under a completely fictitious name.

EXAMPLE

An employee used a coworker's identification to form a shell vendor. The fraudster then proceeded to bill his employer for approximately $20,000 in false services. He deposited the resulting checks in the shell company's account and withdrew currency through an ATM.



False Billings from Shell Companies

Another issue involved in forming a shell company is the entity's address—the place where fraudulent checks will be collected. Often, an employee rents a PO Box and lists it as his shell company's mailing address. Some employees list their home address instead. A comparison of employee addresses to vendor addresses might reveal shell companies in an accounts payable system.

EXAMPLE

A department head set up a dummy company using his residence as the mailing address. Over a two-year period, this man submitted over $250,000 worth of false invoices. Eventually, a newly hired clerk detected the scheme. The clerk was processing an invoice when she noticed that the vendor's address was the same as her boss's address. (By a lucky coincidence, the clerk had typed a personal letter for her boss earlier that day and remembered his address.) Had the department head used a PO Box instead of his home address on the invoices, his scheme might have continued indefinitely.

Employees often use their home addresses to collect fraudulent disbursements because many businesses are wary of sending checks to vendors that have a PO Box for a mailing address. Other common collection sites for shell company schemes are the addresses of relatives, friends, or accomplices.

Submitting False Invoices

Once a shell company has been formed and a bank account has been opened, the corrupt employee begins billing his employer. Invoices can be easily generated on a personal computer. False invoices do not have to be of professional quality to generate fraudulent disbursements.

Self-Approval of Fraudulent Invoices

The difficulty in a shell company scheme is not usually in producing the invoices, but in getting the victim organization to pay them. Authorization for the fictitious purchase (and therefore payment of the bill) is the key. In a large percentage of shell company cases, the perpetrator is in a position to approve payment on the very invoices he is fraudulently submitting. The duties of preparing and approving vouchers should be separated to avoid this kind of scheme.

In companies where a proper separation of duties exists, the employee with approval authority sometimes creates fraudulent vouchers or purchase orders and forges the signature

of the person who is in charge of preparing these documents. Then the perpetrator approves payment on the fraudulent vouchers he has generated. This makes it appear that two employees have signed off on the voucher as mandated by the victim organization's controls.

Not all companies require the completion of payment vouchers before they will issue checks. In some enterprises, checks are written based on less formal procedures, such as the submission of "check requests." These requests simply list the payee's name, the amount to be paid, and a brief narrative stating the reason for the check. Obviously, this is not a very thorough procedure for preventing fraud. Dishonest employees have little trouble running shell company schemes in organizations that operate this way.

Negligent Supervisors

If an employee cannot authorize payments himself, the next best thing is if the person who has that authority is inattentive or overly trusting. Negligent supervisors are often targeted by unethical employees. In some cases, supervisors are attentive to the purchase orders they are asked to authorize, but they lack the technical knowledge to spot fraud as it is happening. For instance, a manager or administrator might not completely understand the costs associated with upgrading computer software to modernize a work area. This manager will have to rely on his subordinates who have the necessary technical expertise to determine that costs are being kept in line. The subordinates might be able to take advantage of this situation to cause the company to overpay for the equipment required to upgrade the system.

Reliance on False Documents

When an employee does not have approval authority for purchases and does not have the benefit of a negligent supervisor, he must run his vouchers through the normal accounts payable process. The success of this kind of scheme depends on the apparent authenticity of the false voucher he creates. If the perpetrator can generate purchase orders and receiving reports that corroborate the information on the fraudulent invoice from his shell company, he can fool accounts payable into issuing a check.

Collusion

Collusion is a type of fraud where two or more individuals agree to commit an act designed to deceive or gain an unfair advantage. Collusion among several employees is sometimes used to overcome well-designed internal controls. For example, in a company with proper

separation of duties, the functions of purchasing goods or services, authorizing the purchase, receiving the goods or services, and making the payment to the vendor should all be separated. If this process is strictly adhered to, it will be extremely difficult for any single employee to commit a false-billing scheme. But if several employees work together, they can overcome the internal controls of their employer.

EXAMPLE

A warehouse supervisor and a parts-ordering clerk conspired to purchase approximately $300,000 worth of nonexistent supplies. The clerk initiated the false transactions by obtaining approval to place orders for parts he claimed were needed. The orders were then sent to a vendor who, acting in conjunction with the two employee fraudsters, prepared false invoices that were sent to the victim company. Meanwhile, the warehouse supervisor verified receipt of the fictitious shipments of incoming supplies. The perpetrators were therefore able to compile complete vouchers for the fraudulent purchases without overstepping their normal duties.

Even if all internal controls are observed, at some point a company must rely on its employees to be honest. One of the purposes of separating duties is to prevent any one person from having too much control over a particular business function. It provides a built-in monitoring mechanism where every person's actions are in some way verified by another person. But if *everyone* is corrupt, even proper controls cannot prevent fraud.

Purchases of Services Rather than Goods

Most shell company schemes involve the purchase of services rather than goods. The primary reason for this is that services are not tangible. If an employee sets up a shell company to make fictitious sales of goods to his employer, these goods will obviously never arrive. By comparing its purchases to its inventory levels, the victim organization might detect the fraud. It is much more difficult for the victim organization to verify that the services were never rendered. For this reason, many employees involved in shell company schemes bill their employers for things like "consulting services."

Pass-Through Schemes

In most shell company schemes, victim organizations are billed for completely fictitious purchases of goods or services. However, there is a subcategory of shell company schemes in which actual goods or services are sold to the victim company. These are known as *pass-through schemes*.

Pass-through schemes are usually undertaken by employees in charge of purchasing on the victim company's behalf. Instead of buying merchandise directly from a vendor, the employee sets up a shell company and purchases the merchandise through that fictitious entity. He then resells the merchandise to his employer from the shell company at an inflated price.

EXAMPLE

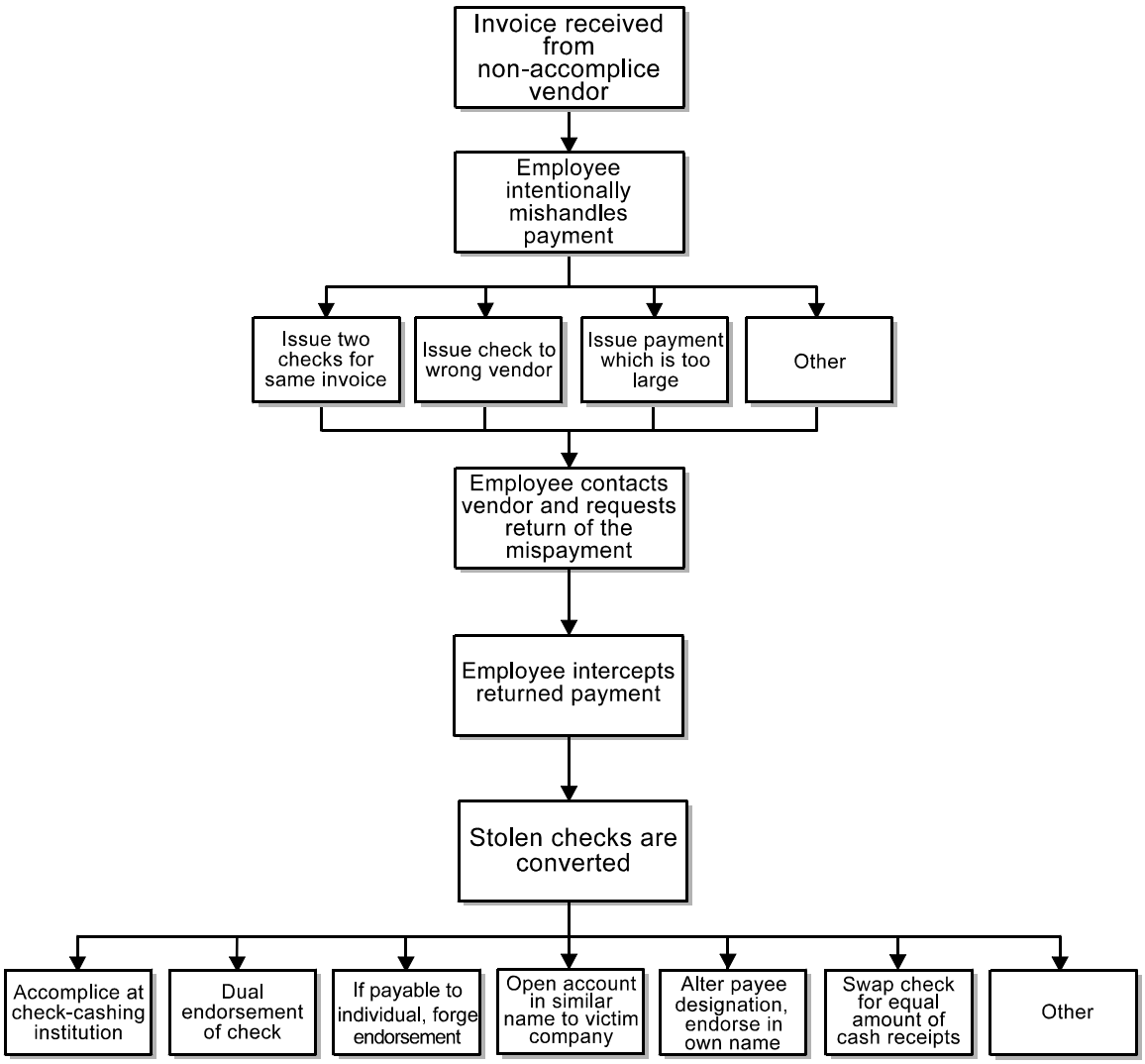
A department director was put in charge of purchasing computer equipment. Because of his expertise on the subject and his high standing within the company, he was unsupervised in this task. The director set up a shell company in another state/province and bought used computers through the shell company, and then turned around and sold them to his employer at a greatly exaggerated price. The money from the victim company's first installment on the computers was used to pay the shell company's debts to the real vendors. Subsequent payments were profits for the fake company. The scheme cost the victim company more than $1 million.

Invoicing Via Nonaccomplice Vendors

Pay-and-Return Schemes

Instead of using shell companies in their overbilling schemes, some employees generate fraudulent disbursements by using the invoices of legitimate third-party vendors who are not a part of the fraud scheme. In a *pay-and-return* scheme, an employee intentionally mishandles payments that are owed to legitimate vendors. (See the "Pay and Return Schemes" flowchart that follows.) One way to do this is to purposely double-pay an invoice. For instance, a clerk might intentionally pay an invoice twice and then call the vendor and request that one of the checks be returned. The clerk then intercepts the returned check.

Another way to accomplish a pay-and-return scheme is to intentionally pay the wrong vendor. In this type of scheme, an employee sends Vendor A's check to Vendor B. After the checks are mailed, the employee calls the vendors to explain the "mistake" and requests that they return the checks to his attention. When the checks arrive, the employee converts them and keeps the money. The employee usually runs the vouchers through the accounts payable system a second time so that the vendors eventually get their money.



Pay and Return Schemes

An employee might also pay the proper vendor but intentionally overpay him. Once again, the employee contacts the vendor, this time to request that the excess payment be returned. Finally, an employee might intentionally purchase excess merchandise, return the excess, and pocket the refund.

Overbilling with a Nonaccomplice Vendor's Invoices

In most instances where an employee creates fraudulent invoices to overbill his employer, he uses a shell company. It is not as common for an employee to submit an existing vendor's invoice. Nevertheless, in some instances an employee will undertake such a scheme by altering an existing vendor's invoice or by creating a counterfeit copy of a vendor's invoice form.

Personal Purchases with Company Funds

Instead of undertaking billing schemes to generate cash, many fraudsters simply purchase personal items with their company's money. Company accounts are used to buy items for employees, their businesses, their families, and so on. This type of scheme is classified as a fraudulent billing scheme rather than theft of inventory. The heart of the scheme is not the theft of the items but rather the purchase of them. The perpetrator causes the victim company to purchase something it did not actually need, so the damage to the company is the money lost in purchasing the item.

Personal Purchases Through False Invoicing

Employees who undertake purchases schemes might do so by running fraudulent invoices through the accounts payable system. The perpetrator in this type of scheme buys an item and submits the bill to his employer as if it represented a legitimate company expense. The victim company ends up unknowingly buying goods or services for a dishonest employee. (See the "Invoice Purchasing Schemes" flowchart that follows.)

THE FRAUDSTER AS AUTHORIZER OF INVOICES

The person who engages in a personal purchases scheme is often the very person in the company whose duties include *authorizing* purchases. Obviously, proper controls should stop anyone from approving his own purchases. Such poorly separated functions leave little other than his conscience to discourage an employee from fraud. Fraud arises in part because of a perceived opportunity. An employee who sees that no one is reviewing his actions is more likely to turn to fraud than one who knows his company works diligently to detect employee theft.

EXAMPLE

A manager of a remote location of a large, publicly traded company was authorized to order supplies and approve vendor invoices for payment. For over a year, the manager routinely added personal items and supplies for his own business to orders made on behalf of his employer. The orders often included a strange mix of items. For instance, technical supplies and home furnishings might be purchased in the same order. Because the manager was in a position to approve his own purchases, he could get away with such obvious frauds. In addition to ordering personal items, the perpetrator changed the delivery address for certain supplies so that they would be delivered directly to his home or side business. This scheme cost the victim company approximately $300,000 in unnecessary purchases.

In some situations, the perpetrator is authorized to approve purchases, but controls prevent him from also initiating purchase requests. This procedure is supposed to prevent an employee from purchasing personal items with company funds. Unfortunately, those with authority to approve purchases often have a good deal of control over their subordinates. These individuals can use their influence to force subordinates to assist in purchasing schemes. In other cases, the manager might simply initiate the purchase order himself by forging the subordinate's signature.

EXAMPLE

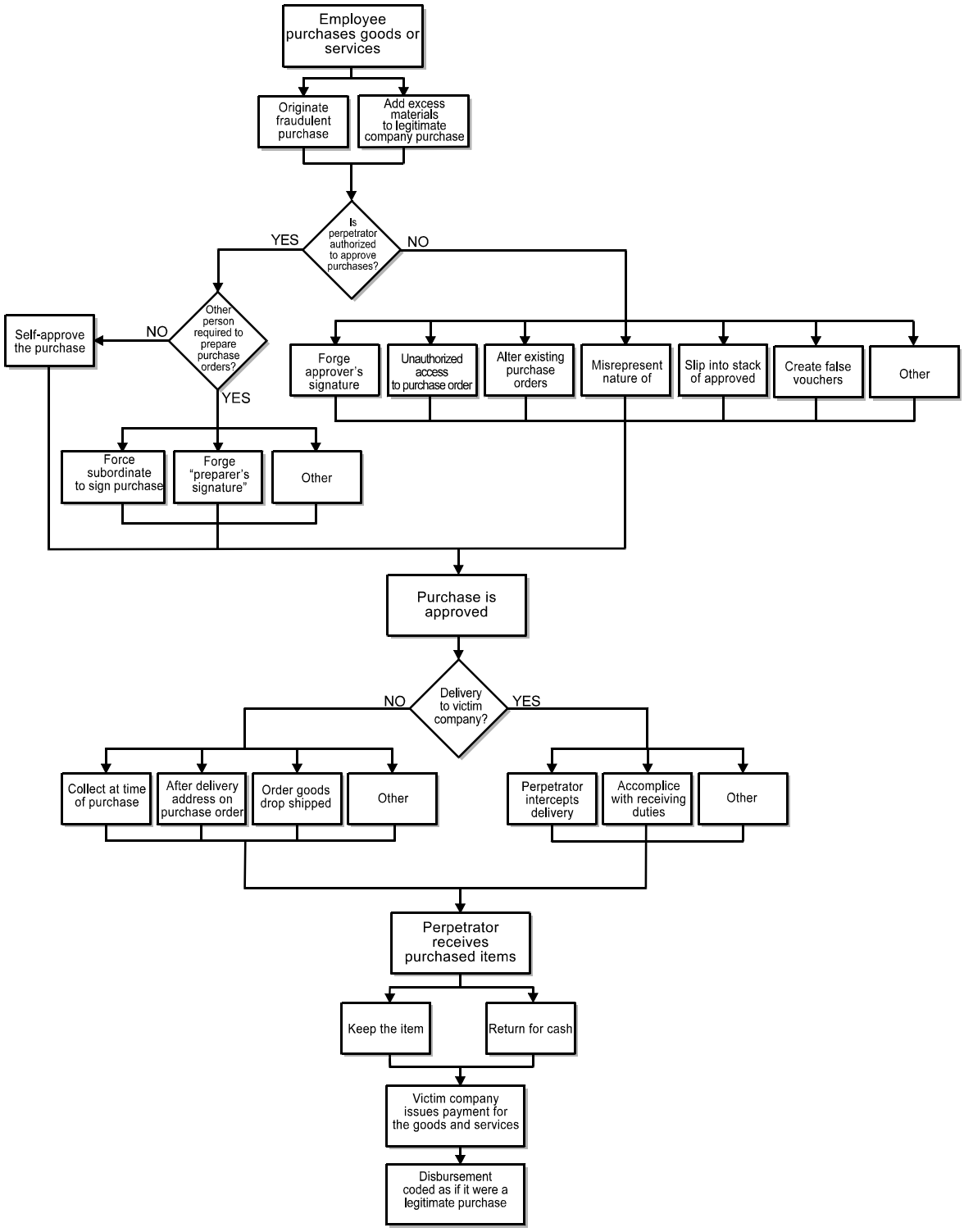
Purchases for under $1,000 at a certain utility company could be made with limited value purchase orders (LPOs), which required the signatures of two people: the originator of a purchase request and the approver of the request. An LPO attached to an invoice for less than $1,000 would be paid by the accounts payable department. In this case, a manager bought goods and services on company accounts and prepared LPOs for the purchases. (In some cases, the LPO would falsely describe the item to conceal the nature of the purchase.) Once the LPO was prepared, the manager forced a clerk in his department to sign the document as the originator of the transaction. The clerk, intimidated by her boss, did not question the authenticity of the LPOs. With two signatures affixed, the LPO appeared to be legitimate and the bills were paid. The scheme cost the victim company at least $25,000.

FALSE PURCHASE REQUISITIONS

If an employee does not have purchasing authority, he might get approval for a fraudulent purchase by misrepresenting the nature of the acquisition. In many companies, those with the power to authorize purchases are not always attentive to their duties. If a trusted subordinate says that the company needs to buy a certain item or items, busy supervisors often give rubber stamp approval to the purchase requisition. Additionally, employees sometimes misrepresent the nature of the items they are purchasing in order to pass a cursory review by their superiors.

EXAMPLE

An engineer bought over $30,000 worth of personal items. The engineer dealt directly with vendors and was also in charge of overseeing the receipt of the materials he purchased. He was therefore able to misrepresent the nature of the merchandise he bought, listing it as "maintenance items." Vendor invoices were altered to agree to this description.



Invoice Purchasing Schemes

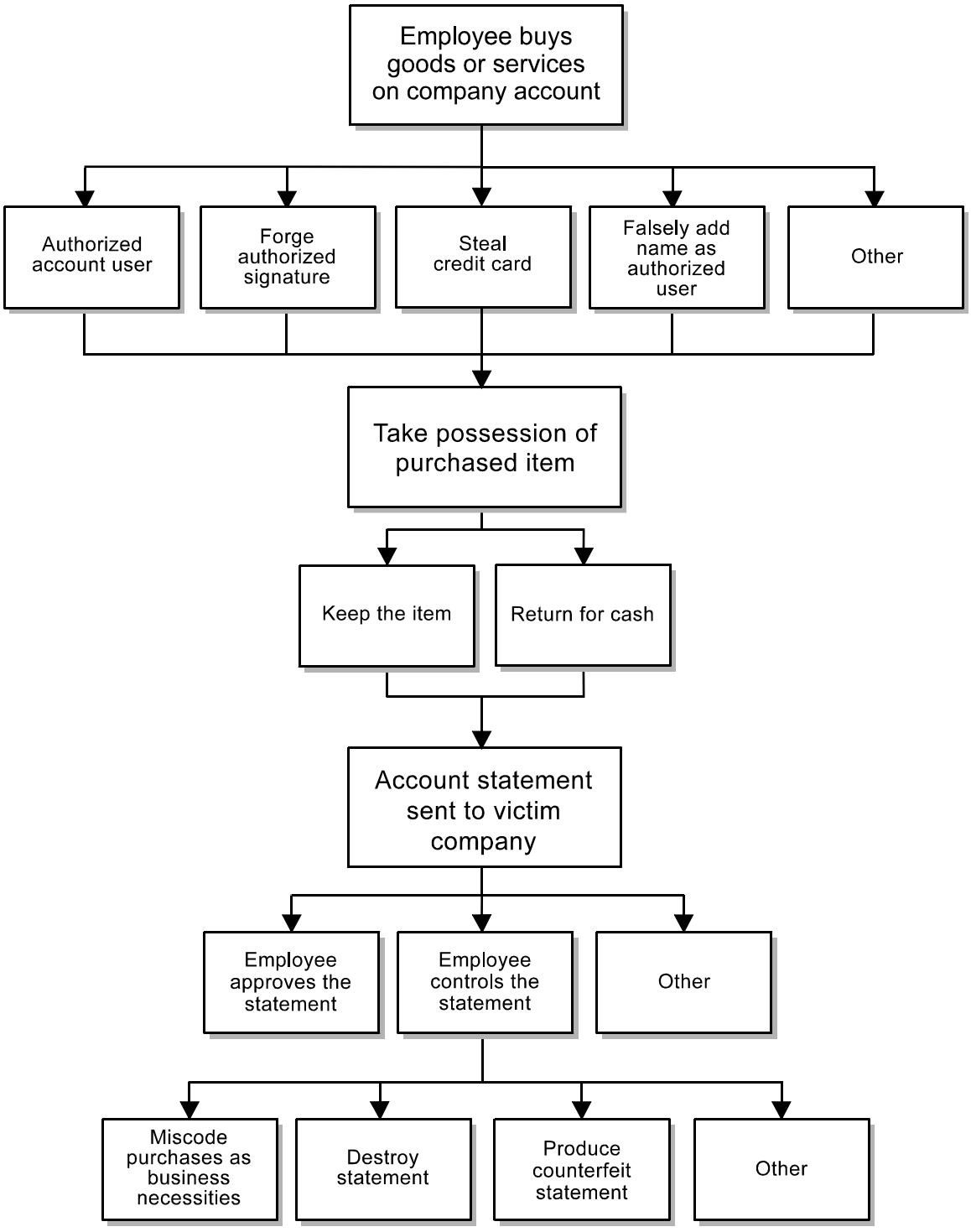
If the perpetrator falsifies his purchase requisition in this manner, the fraud should be detected when delivery occurs. For example, if the purchase requisition says "maintenance items," but the vendor delivers home furnishings, it will be obvious that the perpetrator has committed fraud. The problem of delivery can be avoided if the perpetrator is in charge of receiving incoming shipments. He can verify that delivery of "maintenance items" was received. This is a breach of separation of duties, but unfortunately, it is fairly common for purchasing agents to verify delivery of their own orders. Even if the victim organization enforces a centralized delivery point, the perpetrator might enlist the aid of an accomplice in the receiving department to falsify the organization's receiving reports.

Another way to avoid detection at the delivery stage is to change the delivery address for purchases. Instead of being shipped to the victim organization, the items that the employee buys are sent directly to his home or business. The perpetrator might also order the goods to be shipped to a remote location.

Personal Purchases on Credit Cards or Other Company Accounts

Instead of running false invoices through accounts payable, some employees make personal purchases on company credit cards or on running accounts with vendors. (See the "Purchases on Credit Card or Company Account" flowchart that follows.) Unlike invoicing schemes, prior approval for these purchases is not required. An employee with a company credit card can buy an item merely by signing his name (or forging someone else's) at the time of purchase. Later review of the credit card statement, however, might detect the fraudulent purchase. Unfortunately, many high-level employees approve their own credit card expenses, making it very easy to carry out a purchasing scheme.

Of course, only certain employees are authorized to use company credit cards. Employees without this privilege can only make fraudulent purchases with a company card if they first manage to get hold of one. To this end, company cards are sometimes stolen or "borrowed" from authorized users.



Purchases on Credit Card or Company Account

EXAMPLE

An accountant falsely added her name to a list of employees to whom cards were to be issued. She used her card to make fraudulent purchases, but forged the signatures of authorized cardholders to cover her tracks. Since no one knew she even had a company card, she would not be a prime suspect in the fraud even if someone questioned the purchases. This employee continued her scheme for over five years, racking up a six figure bill on her employer's account. In addition, she had control of the credit card statement and was able to code her purchases to various expense accounts, thereby further delaying detection of her crime.

Another way to conceal a credit card purchasing scheme is to alter the credit card statement so that fraudulent purchases do not show up. Some employees go so far as to destroy the real credit card statement and produce counterfeit copies on which their fraudulent purchases are omitted.

Returning Merchandise for Cash

The fraudulent purchase schemes discussed to this point have all involved false purchases of merchandise for the sake of obtaining the merchandise. In some cases, however, an employee buys items and then returns them for cash.

EXAMPLE

An employee made fraudulent gains from a business travel account. The employee's scheme began by purchasing tickets for herself and her family through her company's travel budget. Poor separation of duties allowed the fraudster to order the tickets, receive them, prepare claims for payments, and distribute checks. The only review of her activities was made by a busy and rather uninterested supervisor who approved the employee's claims without requiring support documentation. Eventually, the employee's scheme evolved. She began to purchase airline tickets and return them for their cash value. An employee of the travel agency assisted in the scheme by encoding the tickets as though the fraudster had paid for them herself. That caused the airlines to pay refunds directly to the fraudster rather than to her employer. In the course of two years, this employee embezzled over $100,000 through her purchase scheme.

Detection of Billing Schemes

Because there are many variations of billing schemes, there are also several detection methods. Detection methods are most effective when used in combinations. Each detection

method is likely to point out anomalies that can then be investigated further to determine if a fraud scheme has occurred or is currently underway. Additionally, the detection methods will point out the weaknesses in internal controls and alert the auditor to potential opportunities for future fraud schemes.

Analytical Review

A review of the various general ledger accounts might reveal unusual or unexpected events. These events could be undetected purchasing fraud. For example, a comparison of inventory purchases in relationship to net sales might indicate that purchases are too high or too low for that level of sales. This might be a red flag that indicates excess purchasing schemes or fictitious sales schemes.

Another analytical method uses a comparison of the inventory purchases of prior years with those of the current year. This comparison might indicate that an overbilling scheme or a duplicate-payment scheme is in progress.

Analyses such as those described previously can be performed for any acquisition of a company's goods or services. Analytical reviews are most effective in detecting fraud schemes that are large because the anomalies will be apparent. Other detection methods are more effective for fraud schemes that are smaller in relationship to the financial statements taken as a whole. Regardless of fraud size, examination of source documentation will be necessary. When an anomaly is detected, further investigation is required, which will demand an examination of source documentation.

Computer-Assisted Analytical Review

The computer can assist the auditor in determining the presence of unusual patterns in the acquisition or purchasing function. The computer can provide the auditor with a matrix of the purchasing activity to determine the presence of unusual patterns. An analysis of the following data might uncover billing schemes.

FRAUD SCHEME	DETECTION METHOD
Fictitious vendors	Vendors and employees with matching addresses More than one vendor with the same address Vendors with only PO Box addresses
Overbilling	Unusual or "one-time" extra charges
Conflict of interest	Vendors with employees who are employee family members An unusually high occurrence of complaints Complaints about specific vendors Higher prices or substandard quality

Statistical Sampling

As with inventory, the source documentation for purchases can be statistically sampled and examined for irregularities. Statistical samples can be drawn to test specific attributes. This detection method is particularly effective if a single attribute is suspected, such as fictitious vendors. A listing of all PO Box addresses might reveal fictitious vendors.

Vendor or Outsider Complaints

Fraudulent schemes will often unravel because a vendor or other outsider complains to the employer or company. Complaints from customers, vendors, and others are good detection tools that can lead the fraud examiner to further inquiry.

Site Visits—Observation

A site visit will often reveal much about the internal control, or lack thereof, for any location. The observation of how the accounting transactions are actually recorded will sometimes alert the fraud examiner to potential problem areas.

Sample Audit Program

The following audit program might be beneficial in detecting red flags of billing schemes:

- Does the company have a purchasing department? If yes, is it independent of (1) the accounting department, (2) the receiving department, or (3) the shipping department?
- Are purchases made only after the respective department heads sign purchase requisitions?
- Are purchases made by means of purchase orders sent to vendors for all purchases or only for purchases over a predetermined limit?
- Do purchase orders specify a description of items, quantity, price, terms, delivery requirements, and dates?
- Is a list of unfilled purchase orders maintained and reviewed periodically?

- Are purchase order forms prenumbered and is the sequence accounted for periodically?
- Does the client maintain an approved vendors list?
- Are items purchased only after competitive bids are obtained? If so, are competitive bids obtained for all purchases or only for purchases over a predetermined limit?
- Is a log maintained of all receipts?
- Does the receiving department prepare receiving reports for all items received? If yes, are receiving reports (1) prepared for all items, (2) prepared only for items that have purchase orders, or (3) renumbered?
- At the time the items are received, does someone independent of the purchasing department check the merchandise before acceptance as to description, quantity, and condition?
- Are copies of receiving reports (1) furnished to the accounting department, (2) furnished to the purchasing department, or (3) filed in the receiving department?
- Are receipts under blanket purchase orders monitored, and are quantities exceeding the authorized total returned to the vendor?
- Are procedures adequate for the proper accounting of partial deliveries of purchase orders?
- Are purchasing and receiving functions separate from invoice processing, accounts payable, and general ledger functions?
- Are vendors' invoices, receiving reports, and purchase orders matched before the related liability is recorded?
- Are invoices checked as to prices, extensions, footings, freight charges, allowances, and credit terms?
- Are controls adequate to ensure that all available discounts are taken?
- Are purchases recorded in a purchase register or voucher register before being processed through cash disbursements?
- Does a responsible employee assign the appropriate general ledger account distribution to which the invoices are to be posted?
- Are procedures adequate to ensure that invoices have been processed before payment and to prevent duplicate payment (e.g., a block stamp)?
- Does a responsible official approve invoices for payment?
- Are procedures adequate to ensure that merchandise purchased for direct delivery to customers is promptly billed to the customers and recorded as both a receivable and a payable?
- Are records of goods returned to vendors matched to vendor credit memos?

- Are unmatched receiving reports, purchase orders, and vendors' invoices periodically reviewed and investigated for proper recording?
- Is the accounts payable ledger or voucher register reconciled monthly to the general ledger control accounts?
- Are statements from vendors regularly reviewed and reconciled against recorded liabilities?
- Do adjustments to accounts payable (e.g., writing off of debit balances) require the approval of a designated official?
- Are budgets used? If yes, are budgets approved by responsible officials, and are actual expenditures compared with budgeted amounts and variances analyzed and explained?
- If excess inventory purchasing is suspicious, verify that all inventory purchased was received (receiving report) at the proper location. An examination of receiving reports or invoices might reveal alternate shipping sites.

Prevention of Billing Schemes

The prevention of billing schemes can be especially difficult. Purchasing personnel are often held to a different standard than other employees of a company. For example, sales people often are given incentives or certain privileges to persuade potential customers. These same incentives are offered to the purchasing personnel of the company from the company's vendors. And yet, the company expects the purchasing personnel to perform their function without partiality and to make decisions that are in the company's best interest, without regard to the incentives offered by suppliers. Additionally, the personnel involved in the purchasing and payment functions are generally not compensated on a basis commensurate with their performance, as are salespeople. Therefore, there is a reverse incentive to perform in the company's best interest.

Probably the most effective prevention measure for billing schemes is education and training of the purchasing and accounts payable personnel. The second most effective prevention measure is an objective compensation arrangement with people responsible for purchasing decisions.

Education (Training)

Purchasing personnel should be trained thoroughly in ethical situations. As an additional deterrent to fraud, companies might consider enrollment and certification in a program for purchasing managers and employees.

Compensation

People responsible for the purchasing decisions (buyers) should be paid well enough to reduce the motive and rationalization for fraud. Auditors can examine the compensation of purchasers and determine if any buyers were recently passed over for raises. This might be an indication of discontent that could lead to the formation of a fraudulent scheme against the employer.

Proper Documentation

Proper documentation for purchasing should include prenumbered and controlled purchase requisitions, purchase orders, receiving reports, and checks.

Proper Approvals

Before adding a vendor to the list, there should be an investigation of the "proposed" vendor, performed by someone other than the personnel in purchasing and accounts payable. If a vendor number is required before payment is made and the personnel responsible for the investigation assigns the vendor that identification number, then the buyer cannot place fictitious vendors on the list. Large or unusual purchases should be approved by someone independent of the purchasing department.

Separation of Duties

For the best results and accountability, each company sufficient in size should have a separate purchasing department. Regardless of the company size, the purchasing function should be separate from the payment function.

Hotlines

When possible, companies should implement a hotline function to provide a forum for complaints and fraud tips by employees and outsiders.

Competitive Bidding

Ensure that bid policies and procedures are thoroughly reviewed. Whenever possible, enforce competitive bidding. *Competitive bidding* is a transparent procurement method in which bids from competing contractors, suppliers, or vendors are invited by openly publicizing the scope, specifications, and terms and conditions of the proposed contract as well as the criteria by which the bids will be evaluated. Competitive bidding aims to obtain goods and services at the lowest prices by stimulating competition and preventing partiality and fraud.

After the bidding process has been completed, a questionnaire can be sent to successful and unsuccessful bidders. This questionnaire can reveal areas that will make the bidding process more effective and can provide a forum for bidders to express concerns over questionable or fraudulent activities.

Prevention Checklist

The following is a list of billing scheme prevention methods that might be helpful in the deterrence of billing fraud:

- Authorization procedures of purchase orders, invoicing, and payments should be documented and adhered to.
- The accounts payable list of vendors should be periodically reviewed for strange vendors and addresses.
- Payment codings should be reviewed for strange descriptions.
- Vendor purchases should be analyzed for odd levels on both a monthly and yearly basis.
- Purchases and inventory levels should be compared and analyzed. (See the "Asset Misappropriation: Inventory and Other Assets" chapter.)
- Control methods to check for duplicate invoices and purchase order numbers should be in place.
- A separation of duties between authorization, purchasing, receiving, shipping, and accounting should be in place.
- Payment of vouchers should be periodically reviewed to ensure integrity of proper documentation.
- Receiving and shipping reports should be reviewed for completeness and accuracy.
- Asset information should include purchasing trails and other information.
- Journal entries to inventory accounts should be strictly scrutinized.
- Appropriate bank reconciliation and review procedures should be performed periodically, checking for out-of-place vendors and endorsements.
- Credit card and purchasing card statements should be reviewed often for irregularities.
- The validity of invoices with a PO Box address should be verified.
- Proper controls for the receipt and handling of "return to sender" checks should be installed.

Payroll Fraud Schemes

Payroll schemes are similar to billing schemes. The perpetrators of these frauds produce false documents, which cause the victim company to unknowingly make a fraudulent

disbursement. In billing schemes, the false document is usually an invoice (coupled, perhaps, with false receiving reports, purchase orders, and purchase authorizations). In payroll schemes, the perpetrator typically falsifies a timecard or alters information in the payroll records. The major difference between payroll schemes and billing schemes is that payroll frauds involve disbursements to employees rather than to external parties. In general, payroll schemes fall into three categories: ghost employee schemes, falsified hours and salary schemes, and commission schemes.

Ghost Employees

The term *ghost employee* refers to someone on the payroll who does not actually work for the victim company. Through the falsification of personnel or payroll records, a fraudster causes paychecks to be generated to a non-employee, or *ghost*. The fraudster or an accomplice then converts these paychecks. (See the "Ghost Employees" flowchart that follows.) The ghost employee might be a fictitious person or a real individual who simply does not work for the victim employer. When the ghost is a real person, it is often the perpetrator's friend or relative.

For a ghost employee scheme to work, four things must happen: (1) the ghost must be added to the payroll, (2) timekeeping and wage rate information must be collected, (3) a paycheck must be issued to the ghost, and (4) the check must be delivered to the perpetrator or an accomplice.

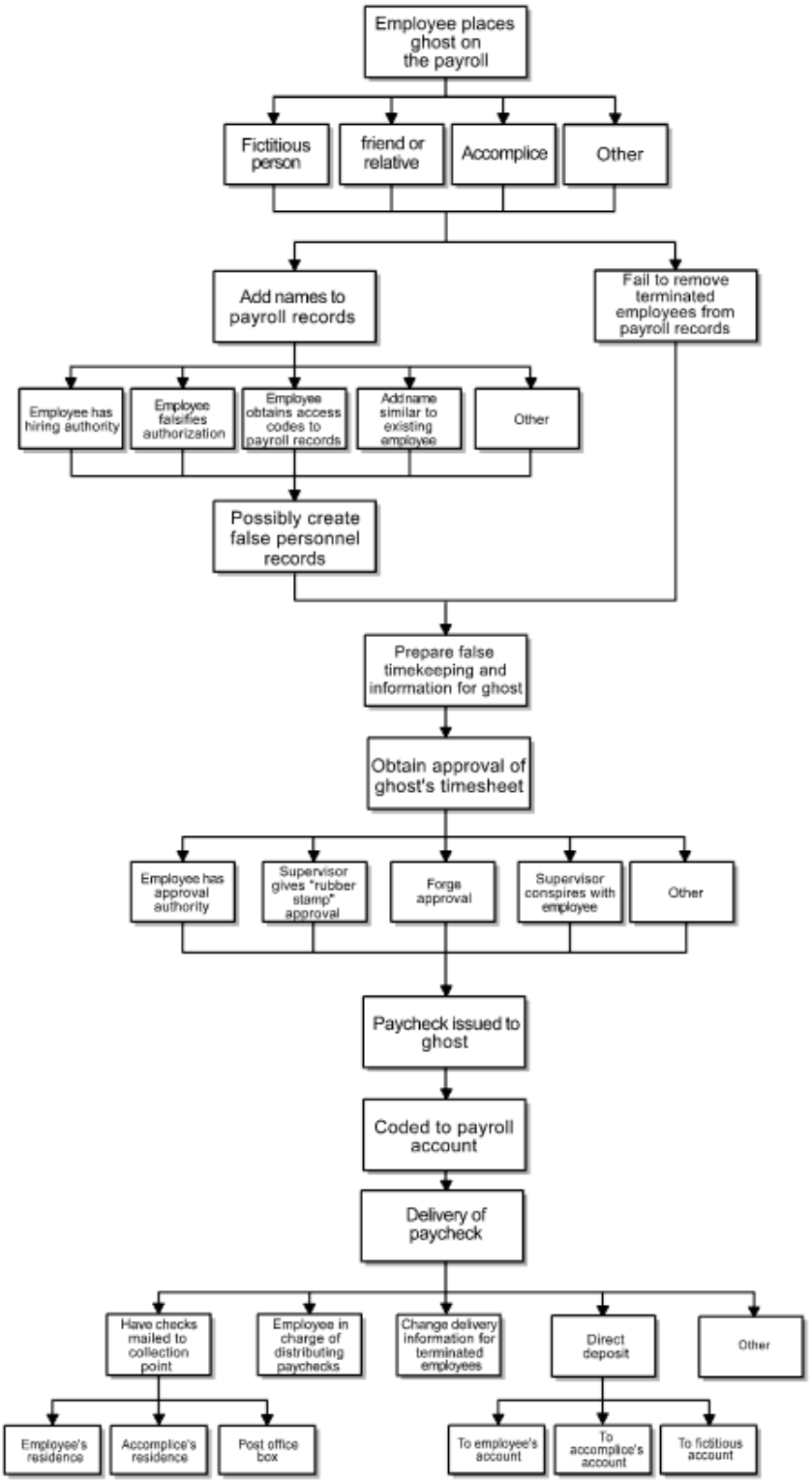
Adding the Ghost to the Payroll

The first step in a ghost employee scheme is entering the ghost on the payroll. In some businesses, all hiring is done through a centralized personnel department, while in others the personnel function is spread over the managerial responsibilities of various departments. Regardless of how hiring of new employees is handled within a business, it is the person or persons with authority to add new employees and remove terminated employees that are in the best position to put ghosts on the payroll.

EXAMPLE

A manager who was responsible for hiring and scheduling janitorial work added over 80 ghost employees to his payroll. The ghosts in this case were actual people who worked at other jobs for different companies. The manager filled out time sheets for the fictitious employees and authorized them, and then took the resulting paychecks to the ghost

employees, who cashed them and split the proceeds with the manager. It was this manager's authority in the hiring and supervision of employees that enabled him to perpetrate this fraud.



Ghost Employees

Employees in payroll accounting also sometimes create ghost employees. In a perfect world, every name listed on the payroll would be verified against personnel records to make sure that those individuals receiving paychecks actually work for the company, but in practice this does not always happen. Thus, people in payroll accounting might be able to create fictitious employees by simply adding a new name to the payroll records. Access to these records is usually restricted, with only high-level employees having the ability to make changes to the payroll. These individuals would therefore be among the most likely suspects in a ghost employee scheme. On the other hand, lower level employees sometimes gain access to restricted payroll information and should not be disregarded as possible suspects.

EXAMPLE

An employee in the payroll department was given the authority to enter new employees into the payroll system, make corrections to payroll information, and distribute paychecks. This employee's manager gave rubber-stamp approval to the employee's actions because of a trusting relationship between the two. The lack of separation of duties and the absence of review made it simple for the culprit to add a fictitious employee into the payroll system.

One way perpetrators try to conceal a ghost's presence on the payroll is to create a ghost with a name very similar to that of a real employee. The name on the fraudulent paycheck will therefore appear to be legitimate to anyone who glances at it. For instance, if a victim organization has an employee named John Doe, the ghost might be named "John Doer."

Instead of adding new names to the payroll, some employees undertake ghost employee schemes when they fail to remove terminated employees' names. Paychecks to the terminated employee continue to be generated even though the employee no longer works for the victim organization. The perpetrator intercepts these fraudulent paychecks and converts them for his personal use.

Collecting Timekeeping Information

The second thing that must occur for a paycheck to be issued to a ghost employee, at least in the case of hourly employees, is the collection and computation of timekeeping information. The perpetrator must provide payroll accounting with a timecard or other document showing how many hours the fictitious employee worked over the most recent pay period. This information, along with the wage rate information contained in personnel or payroll files, will be used to compute the fraudulent paycheck's amount.

Timekeeping records can be maintained in a variety of ways. In many organizations, computer systems are used to track employees' hours. Alternatively, employees might manually record their hours on timecards or might punch time clocks that record the time at which a person starts and finishes his work.

When a ghost employee scheme is in place, someone must create documentation for the ghost's hours. This essentially amounts to preparing a fake timecard showing when the ghost was allegedly present at work. Depending on the normal procedure for recording hours, a fraudster might log into the computerized system and record the ghost employee's hours, create a timecard and sign it in the ghost's name, punch the time clock for the ghost, or so on. Preparation of the timecard is not a great obstacle to the perpetrator. The real key to the timekeeping document is obtaining approval of the timecard.

A supervisor should approve the timecards of hourly employees before paychecks are issued. This verifies to the payroll department that the employee actually worked the hours that are claimed on the card. A ghost employee, by definition, does not work for the victim organization, so approval will have to be fraudulently obtained. Often, the supervisor himself is the one who creates the ghost. When this is the case, the supervisor fills out a timecard in the ghost's name and then affixes his own approval. The timecard is thereby authenticated and a paycheck will be issued. When a non-supervisor is committing a ghost employee scheme, he will typically forge the necessary approval and then forward the fraudulent timecard directly to payroll accounting, bypassing his supervisor.

In computerized systems, a supervisor's signature might not be required. In lieu of the signature, the supervisor inputs data into the payroll system and the use of his password serves to authorize the entry. If an employee has access to the supervisor's password, he can input data for the ghost, which will appear in the payroll system with a seal of approval.

If the perpetrator creates ghosts who are salaried rather than hourly employees, it is not necessary to collect timekeeping information; salaried employees are paid a certain amount each pay period regardless of how many hours they work. Because the timekeeping function can be avoided, it might be easier for a perpetrator to create a ghost employee who works on salary. However, most businesses have fewer salaried employees and they are more likely to be members of management. The salaried ghost might therefore be more difficult to conceal.

Issuing the Ghost's Paycheck

Once a ghost is entered on the payroll and his timecard has been approved, the third step in the scheme is the actual issuance of the paycheck. The heart of a ghost employee scheme is in the falsification of payroll records and timekeeping information. Once this falsification has occurred, the perpetrator does not generally take an active role in the issuance of the check. The payroll department issues the payment—based on the false information provided by the perpetrator—as it would any other paycheck.

Delivery of the Paycheck

The final step in a ghost employee scheme is the distribution of the checks to the perpetrator. Paychecks might be hand-delivered to employees while at work, mailed to employees at their home addresses, or direct-deposited into the employees' bank accounts. If employees are paid in currency rather than by check, the distribution is almost always conducted in person and on site.

Ideally, those in charge of payroll distribution should not have a hand in any of the other payroll cycle functions. For instance, the person who enters new employees in the payroll system should not be allowed to distribute paychecks because this person can include a ghost on the payroll and then simply pocket the fraudulent check when paychecks are disbursed. Obviously, when the perpetrator of a ghost employee scheme is allowed to mail checks to employees or pass them out at work, he is in a perfect position to ensure that the ghost's check is delivered to himself.

In most instances, the perpetrator does not have the authority to distribute paychecks and thus must make sure that the victim organization sends the checks to a place from which he can recover them. When checks are not distributed in the workplace, they are usually mailed to employees or deposited directly into those employees' accounts.

If the fictitious employee was added into the payroll or personnel records by the perpetrator, the problem of distribution is usually minor. When the ghost's employment information is entered, the perpetrator simply lists an address or bank account to which the payments can be sent. In the case of purely fictitious ghost employees, the address is often the perpetrator's own (the same goes for bank accounts). The fact that two employees (the perpetrator and the ghost) are receiving payments at the same destination might indicate payroll fraud. Some fraudsters avoid this duplication by having payments sent to a post office box or to a separate bank account.

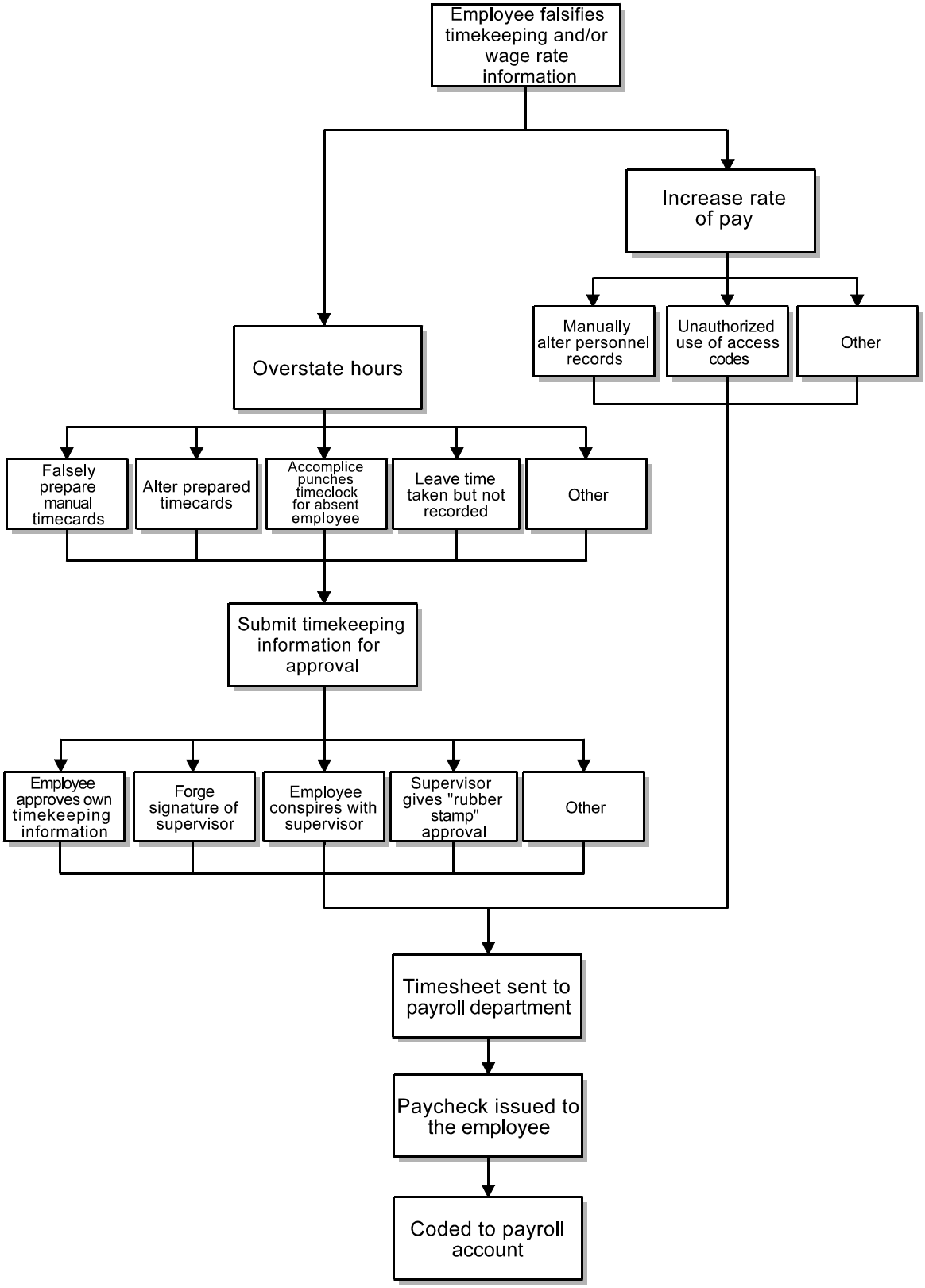
Remember that a ghost employee is not always a fictitious person; it might be a real person who is conspiring with the perpetrator to defraud the company. For example, some employees place their relatives or spouses on the company payroll. When real people conspiring with the fraudster are falsely included on the payroll, the perpetrator typically sees to it that checks are sent to these individuals' homes or bank accounts, thereby avoiding the problem of duplicate addresses on the payroll.

Distribution is a more difficult problem when the ghost is a former employee who was simply not removed from the payroll. If paychecks are distributed through the mail or by direct deposit, the perpetrator will have to enter the terminated employee's records and change their delivery information. In companies in which paychecks are distributed by hand or are held at a central location for employees to collect, the perpetrator can ignore the payroll records and simply pick up the fraudulent paychecks.

Falsified Hours and Salary

The most common method of misappropriating funds from the payroll is the overpayment of wages. For hourly employees, the size of a paycheck is based on two factors: the number of hours worked and the rate of pay. It is therefore obvious that for an hourly employee to fraudulently increase the size of his paycheck, he must either falsify the number of hours he has worked or change his wage rate. (See the "Falsified Hours and Salary" flowchart that follows.) Because salaried employees do not receive compensation based on their time at work, in most cases these employees generate fraudulent wages by increasing their rates of pay.

When discussing payroll frauds that involve overstated hours, one must first understand how an employee's time at work is recorded. Time is generally kept by one of three methods. Time clocks might be used to mark the time when an employee begins and finishes work. The employee inserts a card into the clock at the beginning and end of work, and the clock imprints the current time on the card. In more sophisticated systems, computers might automatically track the time employees spend on the job based on login codes or some other similar tracking mechanism. Finally, paper or computerized timecards showing the number of hours an employee worked on a particular day are often prepared manually by the employee and approved by his manager.



Falsified Hours and Salary

Manually Prepared Timecards

When hours are recorded manually, an employee typically fills out the timecard to reflect the number of hours worked and then presents it to the supervisor for approval. The supervisor verifies the timecard's accuracy, signs or otherwise approves the card to indicate his authorization, and then forwards it to the payroll department so that a paycheck can be issued. Most of the payroll frauds encountered in our study stemmed from abuses of this process.

Obviously, if an employee fills out his own timecard, it might be easy to falsify his hours worked. He simply records the wrong time, showing that he arrived at work earlier or left later than he actually did. The difficulty is not in falsifying the timecard, but in getting the fraudulent card approved by the employee's supervisor. There are basically three ways for the employee to obtain needed authorization.

FORGING A SUPERVISOR'S SIGNATURE

When using this method, an employee typically withholds his paper timecard from those being sent to the supervisor for approval, forges the supervisor's signature or initials, and then adds the timecard to the stack of authorized cards that are sent to the payroll department. In an electronic payroll environment, an employee who learns his supervisor's password can log into the system and authorize his own timecard surreptitiously. The fraudulent timecard then arrives at the payroll department with what appears to be a supervisor's approval, and a paycheck is subsequently issued.

COLLUSION WITH A SUPERVISOR

The second way to obtain approval of a fraudulent timecard is to collude with a supervisor who authorizes timekeeping information. In these schemes, a supervisor knowingly approves false timecards on the employee's behalf. As an incentive to the supervisor, the employee might kick back a portion of the overpaid wages to the supervisor. In some cases, the supervisor might take the entire amount of the overpayment. It might be particularly difficult to detect payroll fraud when a supervisor colludes with an employee because managers are often relied upon as a control to ensure proper timekeeping.

EXAMPLE

A supervisor assigned employees to better work areas or better jobs, but she demanded payment in return. The payment was arranged via the falsification of the employees'

timecards, which the supervisor authorized. The employees were compensated for fictitious overtime, and these funds were then kicked back to the supervisor.

RELYING ON A NEGLIENT SUPERVISOR

The third way to obtain approval of fraudulent timecards is to rely on a supervisor to approve them without reviewing their accuracy. The "lazy manager" method seems risky—so much so that one would think that it would be uncommon—but it actually occurs quite frequently. A recurring theme in occupational fraud schemes is the perpetrators' reliance on the inattentiveness of others. When an employee sees an opportunity to make a little extra money without getting caught, that employee is more likely to be emboldened to attempt a fraud scheme. The fact that a supervisor is known to "rubber stamp" timecards or even ignore them can be a factor in an employee's decision to begin stealing from his company.

EXAMPLE

A temporary employee noticed that his manager did not reconcile the expense journal monthly. Thus, the manager did not know how much was being paid to the temporary agency. The fraudster completed fictitious time reports, which were sent to the temporary agency and which caused the victim company to pay over $30,000 in fraudulent wages. Because the fraudster controlled the mail and the manager did not review the expense journal, this extremely simple scheme went undetected for some time.

Poor Custody Procedures

One form of control breakdown that often occurs is the failure to maintain proper control over timecards. In a properly run system, timecards that have been authorized by management should be sent directly to payroll. Those who prepare the timecards should not have access to them after they have been approved. Similarly, computerized timesheets should be blocked from modification by the employee once supervisor authorization has been given. When these procedures are not observed, the person who prepared a timecard can alter it after the supervisor has approved it but before it is delivered to payroll.

Another way hours are falsified is in the misreporting of leave time. This is not as common as timecard falsification, but it does occur with some frequency. Incidentally, it is one instance in which salaried employees commit payroll fraud by falsifying their hours. A leave time scheme is very simple. An employee takes a certain amount of time off of work as paid leave or vacation, but does not report this leave time. Employees typically receive a certain amount of paid leave per year. If a person takes a leave of absence but does not report it,

those days are not deducted from his allotted days off. In other words, he gets more leave time than he is entitled to. The result is that the employee shows up for work less, yet still receives the same pay.

Time Clocks and Other Automated Timekeeping Systems

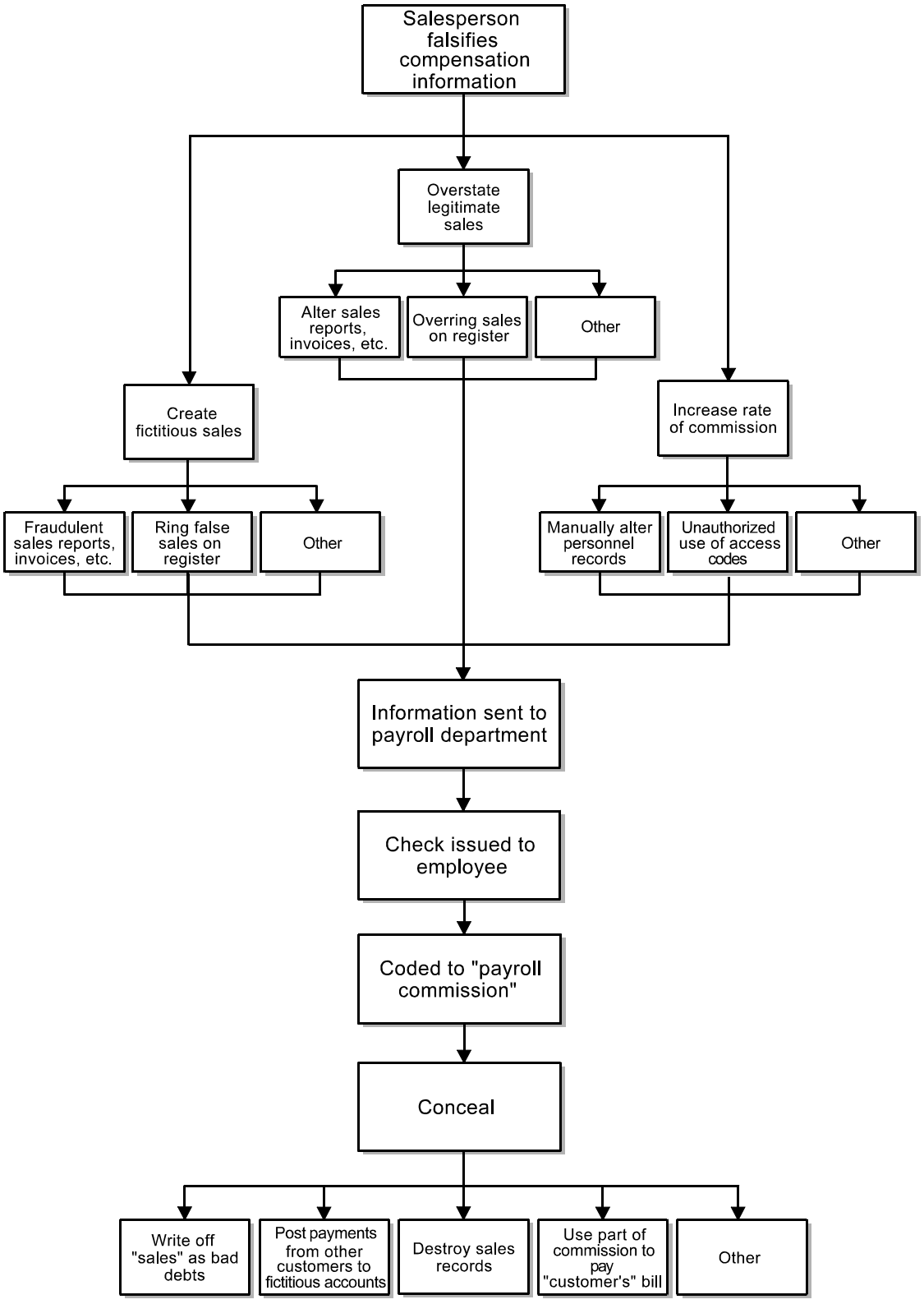
In companies that use time clocks to collect timekeeping information, payroll fraud is usually uncomplicated. In the typical scenario, the time clock is located in an unrestricted area, and a timecard for each employee is kept nearby. The employees insert their timecards into the time clock at the beginning and end of their shifts, and the clock imprints the time. The length of time an employee spends at work is therefore recorded. Supervisors should be present at the beginning and end of shifts to ensure that employees do not punch the timecards of absent coworkers, yet this simple control is often overlooked. Without proper supervision, employees can punch the timecards of absent coworkers so that it appears the absent employee was at work that day. The absent employee is therefore overcompensated on his next paycheck.

Rates of Pay

It should be remembered that an employee can also receive a larger paycheck by changing his pay rate. An employee's personnel or payroll records reflect his rate of pay. If an employee can gain access to these records or has an accomplice with access to them, he can adjust them so that he receives a larger paycheck.

Commission Schemes

Commission is a form of compensation calculated as a percentage of the amount of transactions a salesperson or other employee generates. It is a unique form of compensation that is not based on hours worked or a set yearly salary, but rather on an employee's revenue output. A commissioned employee's wages are based on two factors: the amount of sales he generates and the percentage of those sales he is paid. In other words, there are two ways an employee on commission can fraudulently increase his pay: (1) falsify the amount of sales made or (2) increase his rate of commission. (See the "Commission Schemes" flowchart that follows.)



Commision Schemes

Fictitious Sales

Establishing unattainable sales quotas that employees think are unreasonable will increase the pressure to establish fictitious performance levels. If the pressure becomes significant, the employee might resort to adding fictitious sales and accounts receivable to meet the sales quotas.

An employee can falsify the amount of sales he has made in one of two ways, the first being the creation of fictitious sales. The manner in which fictitious sales are created depends on the industry in which the perpetrator operates. Fictitious sales might be constructed by the creation of fraudulent sales orders, purchase orders, credit authorizations, packing slips, invoices, and so on. Alternatively, a culprit might simply ring up a false sale on a cash register. The key is that a fictitious sale is created, that it appears to be legitimate, and that the victim organization reacts by issuing a commission check to the perpetrator.

EXAMPLE

A dishonest insurance agent took advantage of his company's incentive commissions, which paid $1.25 for every $1.00 of premiums generated in the first year of a policy. The agent wrote policies to fictitious customers, paid the premiums, and received his commissions, which created an illegal profit on the transaction. For instance, if the fraudster paid $100,000 in premiums, he would receive $125,000 in commissions, a $25,000 profit. No payments were made on the fraudulent policies after the first year.

If a salesperson's primary compensation is based on sales, without regard to collection, then there is an incentive to produce quantity rather than quality sales. It is natural for companies to push for higher sales levels to sustain growth. If the salespersons' compensation is based solely on quantity and not on a combination of quantity *and* quality, however, then the compensation incentive is misplaced. This might create an atmosphere which, if coupled with opportunity, will produce inflated or fictitious sales.

Altered Sales

The second way for a fraudster to overstate the amount of sales he has made is to alter the prices listed on sales documents; in other words, the perpetrator charges one price to a customer, but records a higher price in the company books. This causes the victim company to pay a larger commission than the perpetrator deserves. To make these schemes work, the employee might have to intercept and alter the invoices that are sent to the customer. (The invoices the company sends out will reflect a higher purchase price than the customer agreed

to, so if the customer receives these invoices he is likely to complain about the discrepancy.) The employee might also overstate the revenue received from his customers.

Altering Commission Rates

As mentioned previously, the other way to manipulate the commission process is to change the employee's rate of commission. This would likely necessitate the alteration of payroll or personnel records, which should be off-limits to the sales staff.

Detection of Payroll Schemes

Independent Payroll Distribution

Ghost employee schemes can be uncovered by having personnel (other than the payroll department) distribute the payroll checks or paystubs, and by requiring positive identification of the payee. However, as more and more companies are moving to a direct-deposit payroll with pay stubs available for viewing online, hand-delivering paychecks or paystubs is becoming an obsolete method of detecting ghost employees.

Analysis of Payee Address or Accounts

If payroll checks are either mailed or deposited automatically, then a list of duplicate addresses or deposit accounts might reveal ghost employees or duplicate payments.

Duplicate Identification Numbers

Because each employee is required to have a government-issued identification number (such as a Social Security or Social Insurance number), a listing of duplicate numbers might reveal ghost employees.

Overtime Authorization

Requiring employees to have overtime authorized by a supervisor, having the supervisor be responsible for the timecards, and having the supervisor refer the timecards directly to payroll will aid in reducing overtime abuses. In addition, the payroll department should scan the time reports and question obvious abuses, such as only one employee working overtime in a department or excessive overtime on a timecard. By examining the source documentation, one might detect unauthorized overtime and falsified hours.

Commissions

Commission schemes can often be detected with the following techniques:

- Compare commission expenses to sales figures to verify linear correlation.
- Prepare a comparative analysis of commission earned by salesperson, verifying rates and calculation accuracy. Excessively high earnings by an individual could signal fraud.
- Analyze sales by salesperson for uncollected sales amounts.
- Determine proper segregation of duties in calculation of commission amounts. Commissions should be independently provided by personnel outside the sales department.
- Contact a random sample of customers to confirm sales.

TREND ANALYSIS ON WRITTEN-OFF ACCOUNTS RECEIVABLE

Stratify the written-off accounts receivable data and examine it for possible trends and patterns. For example, do any of the following trends appear?

- Same salesperson
- Same accounting period (unless only an annual review of accounts receivable is performed)
- Same collector
- Collection rates by agency or collector

Any of these trends might indicate fictitious accounts receivable, or that only new or good accounts are being assigned to collectors or collection agencies.

Analysis of Deductions from Payroll Checks

An analysis of the payroll withholdings might reveal either ghost employees or trust account abuses. Ghost employees will often have no withholding taxes, insurance, or other normal deductions. Therefore, a listing of any employee without these items might reveal a ghost employee.

An analysis of withholding-tax deposits might reveal that trust account taxes have been "borrowed," even for a short period, before the taxes are deposited. Comparing the disbursement date with the deposit date should reveal if the trust account taxes have been borrowed. Additionally, any delinquent payroll tax notices from the taxing authorities should serve as a red flag to potential trust account tax "borrowings."

Other Detection Methods

Other methods for detecting ghost employees include:

- Reviewing company email address directories to ensure that all employees receiving paychecks have a company email address issued by the IT Department
- Comparing employee names, addresses, government-issued identifications, and bank account numbers to determine if there are any unexpected duplicates
- Comparing employee payroll records to human resources employee files to ensure all individuals receiving payroll checks are employees
- Examining payroll checks for dual endorsements

Prevention of Payroll Schemes

There are two basic preventive measures for payroll-related fraud: segregation of duties and periodic payroll review and analysis.

Separation of Duties

The following duties should be separated:

- Payroll preparation
- Payroll disbursement (into payroll and withholding tax accounts)
- Payroll distribution
- Payroll bank reconciliations
- Human resource departmental functions

If payroll is prepared by personnel not responsible for its distribution and reconciliation, it will be difficult for anyone to successfully add ghost employees. They will also be prevented from "borrowing" the trust account taxes because they will not have access to the disbursing function. In smaller companies, this function is often handled outside the firm at pennies per employee.

After the payroll checks are prepared, the transfer of funds from the general accounts to the payroll accounts should be handled by accounting. The personnel department should distribute checks and require identification in exchange for the payroll checks. This will curtail the opportunity to add ghost employees to the payroll. A suggested form of identification might be company-issued access passes, if available.

If the bank reconciliation function for the payroll account is assigned to someone other than those in the previously described functions, then all the payroll functions have been

segregated. No one is able to add ghost employees or "borrow" the withholding taxes without the opportunity for discovery by someone else.

Periodic Review and Analysis of Payroll

Periodically, an independent review of the payroll might reveal that internal controls are not working as designed. Comparing deposit dates with dates of payroll disbursement or transfer might reveal ghost employees, as could an occasional independent payroll distribution.

The existence of the following might indicate the presence of ghost employees:

- More than one employee with the same address
- More than one employee with the same government identification number
- More than one employee with the same account number (automatic deposit)
- Employees with no withholding

Indicators of Payroll Fraud

In addition, the following audit program will help spot red flags to payroll distribution fraud and help with installing control procedures:

- Are personnel records maintained independently of payroll and timekeeping functions?
- Is the payroll accounting function independent of the general ledger function?
- Are changes to payroll not made unless the personnel department sends approved notification directly to the payroll department?
- Are references and backgrounds checked for new hires?
- Are all wage rates authorized in writing by a designated official?
- Are signed authorizations on file for employees whose wages are subject to special deductions?
- Are bonuses, commissions, and overtime approved in advance and reviewed for compliance with company policies?
- Are sick leave, vacations, and holidays reviewed for compliance with company policy?
- Are appropriate forms completed and signed by employees to show authorization for payroll deductions and withholding exemptions?
- Is the payroll periodically checked against the personnel records for terminated employees, fictitious employees, etc.?
- Is a time clock used for office employees as well as factory workers?
- If a time clock is used, are timecards (1) punched by employees in the presence of a designated supervisor and (2) signed by a supervisor at the end of the payroll period?

- Are timecards and production reports reviewed and compared with payroll distribution reports and production schedules?
- Are payroll registers reviewed and approved before disbursements are made for (1) names of employees, (2) hours worked, (3) wage rates, (4) deductions, (5) agreement with payroll checks, and (6) unusual items?
- Are all employees paid by check out of a separate bank payroll account?
- Are payroll checks pre-numbered and issued in numerical sequence?
- Is access restricted to unissued payroll checks and signature plates?
- Are checks drawn and signed by designated officials who do not (1) prepare payroll, (2) have access to the accounting records, or (3) have custody of cash funds?
- Are payroll checks distributed by someone other than the department head or the person who prepares the payroll?
- Is the distribution of the payroll rotated periodically to different employees without prior notice?
- Is the payroll bank account reconciled by a designated employee who (1) is not involved in the preparing of payroll, (2) does not sign the checks, or (3) does not handle the check distributions?
- Do payroll bank account reconciliation procedures include comparing the paid checks to the payroll and scrutinizing canceled check endorsements?
- Are the payroll registers reconciled to the general ledger control accounts?
- Is a liability account set up for all wages that have remained unclaimed for a certain period of time? If yes, (1) have these wages been redeposited in a special bank account and (2) is identification required to be presented at the time of their subsequent distribution?
- Are distributions of hours (direct and indirect) to activity or departments reviewed and approved by supervisory personnel?
- Are actual payroll amounts reviewed and compared to budgeted amounts, and are variances analyzed regularly?
- Do adequate procedures exist for timely and accurate preparation and filing of payroll tax returns and related taxes?
- Are employee benefit plan contributions reconciled to appropriate employee census data?
- Are adequate, detailed records maintained of the entity's liability for vacation pay and sick pay? Are they reconciled to the general ledger control accounts periodically?

Expense Reimbursement Schemes

Employees can manipulate an organization's expense reimbursement procedures to generate fraudulent disbursements. Companies usually pay expense reimbursements in this manner: An employee submits a report detailing an expense incurred for a business purpose, such as a business lunch with a client, airfare, hotel bills associated with business travel, and so on. In preparing an expense report, an employee usually must explain the business purpose for the expense, as well as the time, date, and location in which it was incurred. Attached to the report should be support documentation for the expense—typically a receipt. In some cases, canceled checks written by the employee or copies of a personal credit card statement showing the expense are allowed. The report usually must be authorized by a supervisor in order for the expense to be reimbursed. The four most common types of expense reimbursement schemes are mischaracterized expenses, overstated expenses, fictitious expenses, and multiple reimbursements.

Mischaracterized Expense Reimbursements

Most companies only reimburse certain employee expenses. Which expenses a company will pay for depends to an extent upon policy, but in general, business-related travel, lodging, and meals are reimbursed. One of the most basic expense reimbursement schemes is perpetrated by simply requesting reimbursement for a personal expense by claiming that the expense is business related. (See the "Mischaracterized Expenses" flowchart that follows.) Examples of mischaracterized expenses include claiming personal travel as a business trip, listing dinner with a friend as "business development," and so on. Employees submit the receipts from their personal expenses along with their expense reports, but concoct business reasons for the incurred costs. The false expense report induces the victim organization to issue a check, reimbursing the perpetrator for his personal expenses.

In cases involving airfare and overnight travel, a mischaracterization can sometimes be detected by simply comparing the employee's expense reports to his work schedule. Often, the dates of the so-called "business trip" coincide with a vacation or day off. Detailed expense reports allow a company to make this kind of comparison and are therefore very helpful in preventing expense schemes.

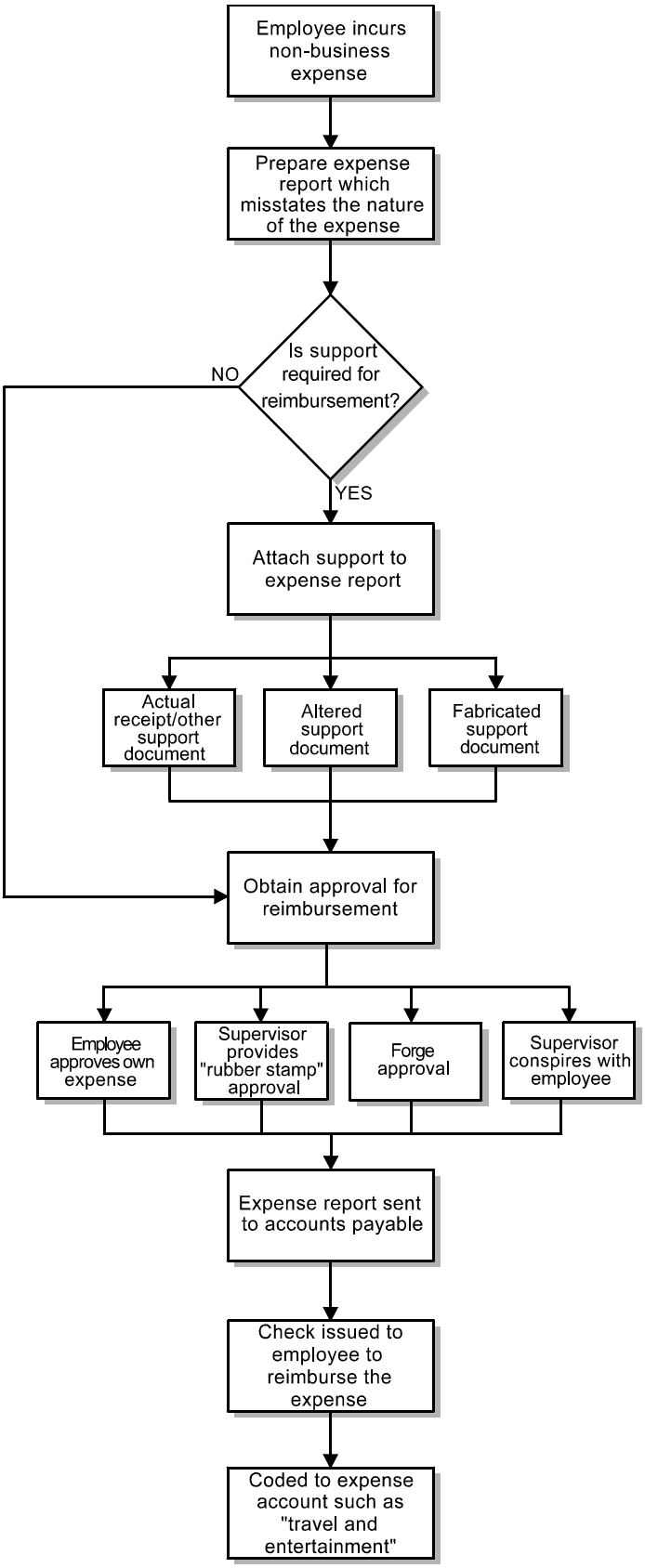
A common element to mischaracterized expense schemes is the failure to submit detailed expense reports, or any expense reports at all. Some companies allow employees to simply turn in receipts without explaining the business purpose of the listed expenses. This makes it exceedingly easy for an employee to turn in a receipt from a restaurant and receive a check

to reimburse him for a "business dinner." Other companies provide employees with company credit cards or procurement cards and allow employees to spend company funds without providing detailed information justifying the purchase, sometimes not even requiring receipts. Requiring detailed information means more than just supporting documents; it should mean precise statements of what was purchased, as well as when, where, and for whom the purchase was made.

EXAMPLE

A fraudster submitted credit card statements as support for expenses, but he only submitted the top portion of the statements, not the portion that describes what was purchased. Over 95 percent of his expenses that were reimbursed were of a personal rather than a business nature.

Even when detailed expense reports are required, it might be difficult to detect a mischaracterized expense reimbursement scheme. For example, suppose a traveling salesman goes on a trip and runs up a large bar bill one night in his hotel, saves his receipt, and lists this expense as "business entertainment" on an expense report. Nothing about the time, date, or nature of the expense would readily point to fraud, and the receipt would appear to substantiate the expense. Short of contacting the client who was allegedly entertained, there might be little a victim organization can do to identify the expense as fraudulent.



Mischaracterized Expenses

Overstated Expense Reimbursements

Instead of seeking reimbursement for personal expenses, some employees overstate the cost of actual business expenses. (See the "Overstated Expenses" flowchart that follows.) This can be accomplished in a number of ways.

Altered Receipts

The most fundamental example of an overstated expense reimbursement scheme occurs when an employee alters a receipt or other supporting documentation to reflect a higher cost than what he actually paid. The employee might use correction fluid, a ballpoint pen, or some other method to change the price reflected on the receipt before submitting his expense report. If the company does not require original documents as support, the perpetrator generally attaches a copy of the receipt to his expense report. Alterations are usually less noticeable on a photocopy than on an original document. Businesses should require original receipts and ink signatures on expense reports for precisely this reason.

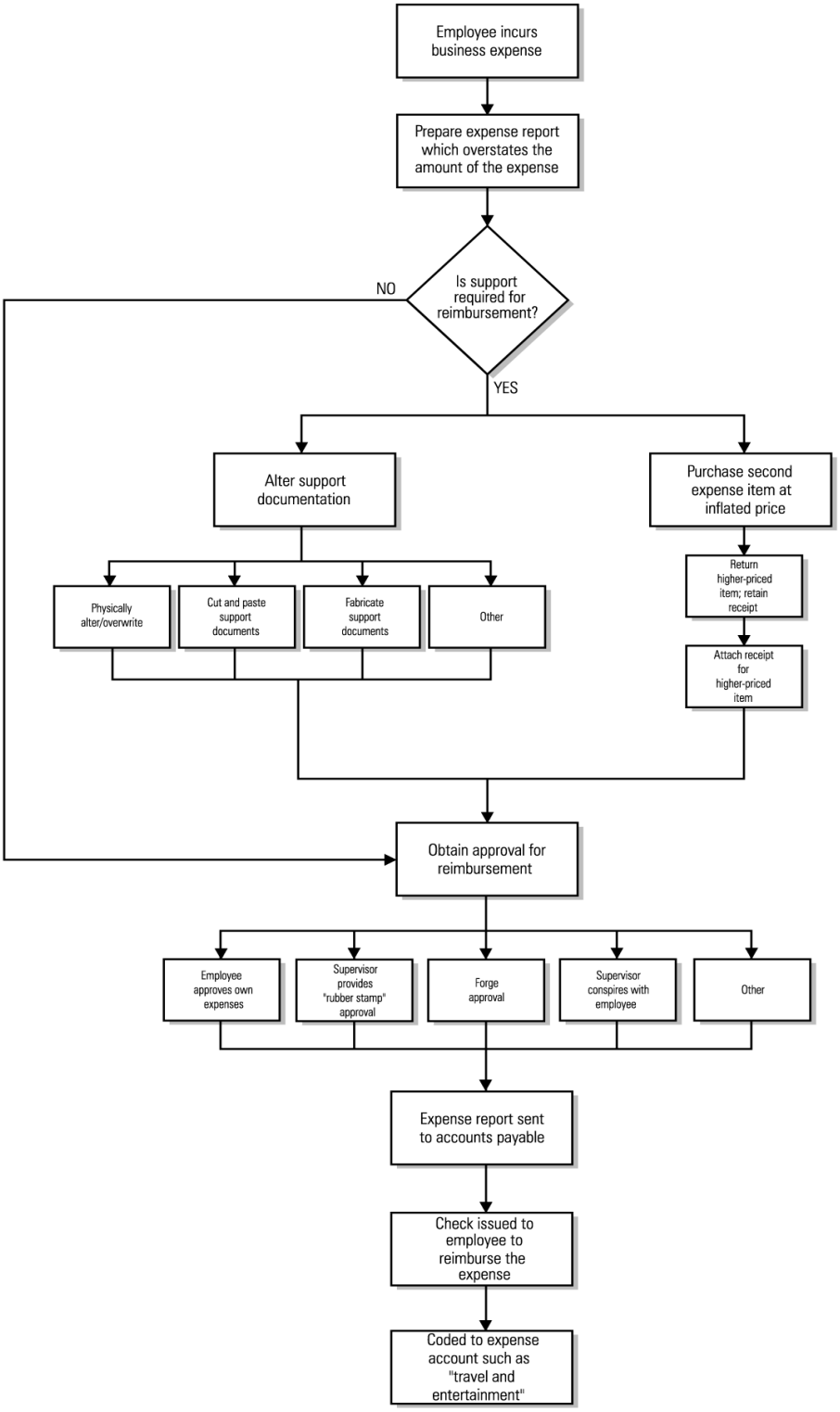
As with other expense frauds, overstated expense reimbursement schemes often succeed because of poor controls. In companies where supporting documents are not required, for example, fraudsters simply lie about how much they paid for a business expense. With no support available, it could be very difficult to disprove an employee's false expense claims.

Overpurchasing

Another way to overstate a reimbursement form is the "overpurchasing" of business expenses. This method is typically used by employees seeking reimbursement for travel expenses. Assume an employee is scheduled to make a business trip to another city. The employee purchases an airline ticket far in advance of the trip when rates are low. When it is close to the day of the trip, the employee purchases another ticket to the same destination. This ticket will be more expensive than the first one. To further increase the price, the second ticket might include several stops and layovers on a very circuitous route. The employee removes the passenger receipt coupon from the second ticket and then returns it for a full refund. He actually flies on the first (less expensive) ticket he purchased, but attaches the receipt from the more expensive ticket to his expense report.

Overstating Another Employee's Expenses

Overstated expense reimbursement schemes are not just committed by the person who actually incurs the expense. They might be committed by a coworker who handles or processes expense reports.



Overstated Expenses

EXAMPLE

A petty cashier covered up other employees' requests for travel advances with correction fluid and inserted larger amounts. The cashier then passed on the legitimate travel advances and pocketed the excess.

This kind of scheme is most likely to occur in a system where expenses are reimbursed in currency rather than by check, since the perpetrator would be unable to extract his "cut" from a single check made out to another employee.

Orders to Overstate Expenses

Finally, some employees knowingly falsify their own reports, but do so at their supervisors' direction. The employees might be threatened with loss of their jobs if they do not go along with the scheme. Sometimes the supervisor splits the proceeds of the fraud with his subordinates. In other cases, the excess money goes into a slush fund or is used for some other business purpose that is not in the company budget. The supervisors who engage in these schemes often believe they are really acting in their companies' best interests.

EXAMPLE

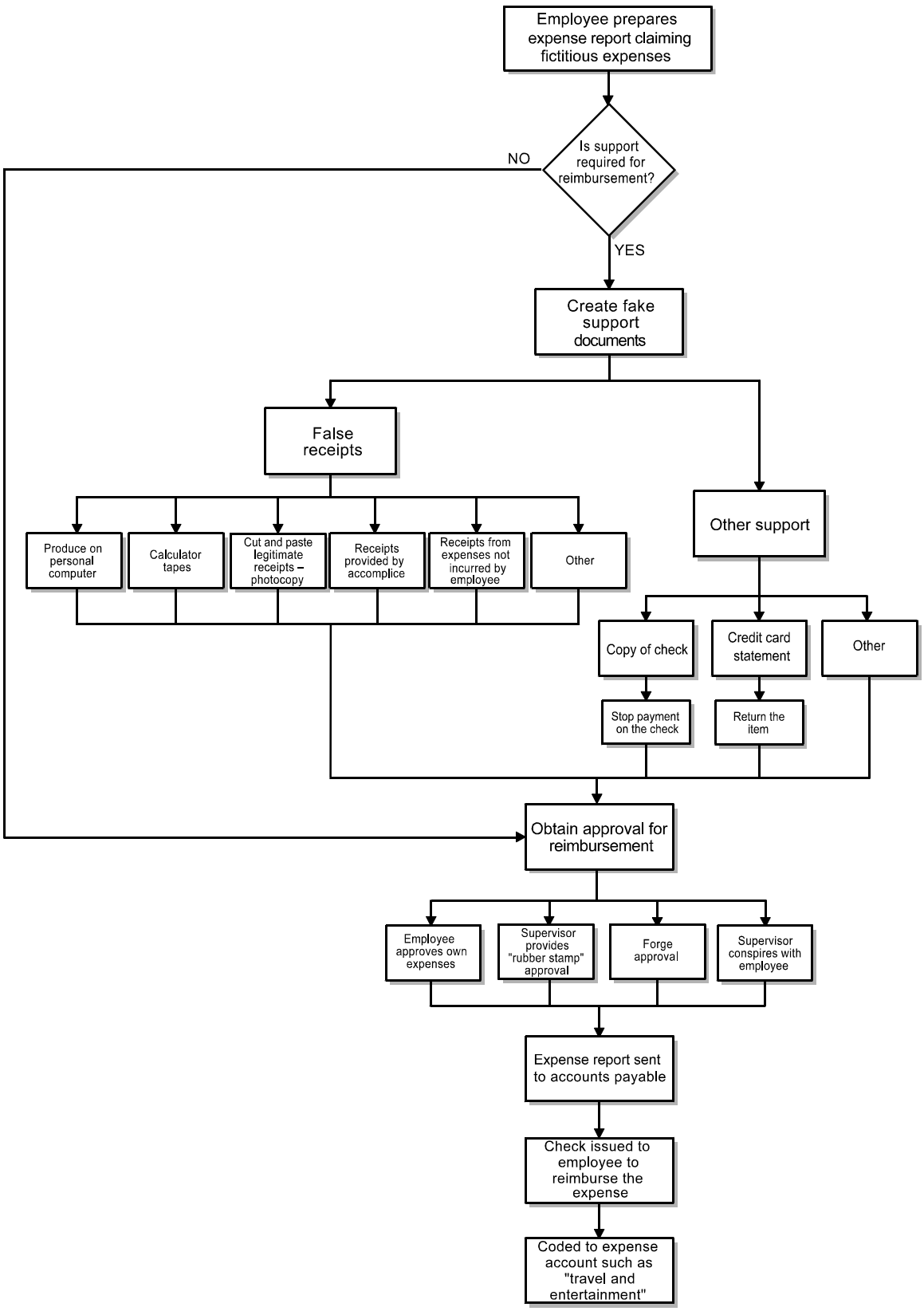
A sales executive instructed his salesmen to inflate their expenses to generate cash for a slush fund. This fund was used to pay bribes and to provide improper forms of entertainment for clients and customers.

Fictitious Expense Reimbursements

Employees sometimes seek reimbursement for wholly fictitious expenses. Instead of overstating a real business expense or seeking reimbursement for a personal expense, an employee just invents an expense and requests that it be reimbursed. (See the "Fictitious Expenses" flowchart that follows.)

Producing Fictitious Receipts

One way to generate a reimbursement for a fictitious expense is to create fraudulent support documents, such as false receipts. Using simple computer software, it is easy for employees to create realistic-looking counterfeit receipts at home. These counterfeits are often very sophisticated, even including the logos of the stores in which goods or services were allegedly purchased. Computers are not the only means of creating support for a fictitious expense. Some employees use calculator tapes, others cut and paste old receipts from suppliers, and some use software to generate fictitious receipts.



Fictitious Expenses

Unfortunately, not all companies require receipts to be attached to expense reports. Checks written by the employee or copies of his personal credit card bill might be allowed as support in lieu of a receipt. Some employees write personal checks that appear to be for business expenses and then photocopy these checks and attach them to reimbursement requests. In actuality, nothing is purchased with the checks; they are destroyed after the copies are made. The perpetrator ends up receiving a reimbursement from his employer without ever actually incurring a business expense. The same method can be used with credit cards, where a copy of a statement is used to support a purchase. Once the expense report is filed, the perpetrator returns the item and receives a credit to his account.

Obtaining Blank Receipts from Vendors

If the perpetrator does not create receipts, they can be obtained from legitimate suppliers in a number of ways. Some employees request blank receipts from waiters, bartenders, taxi cab drivers, etc. These individuals fill in the blank receipts to "create" business expenses. A fraudster might also have a friend, spouse, relative, etc., who can provide receipts for "business expenses" that never really occur.

EXAMPLE

An employee's girlfriend worked at a restaurant near the victim organization. This girlfriend validated credit card receipts and gave them to the fraudster so that he could submit them with his expense reports.

In some cases, a fraudster will steal an entire stack of blank receipts from a hotel, restaurant, etc. He will then fill them in and use them to verify fictitious business expenses over time.

Claiming the Expenses of Others

Another way perpetrators use actual receipts to generate unwarranted reimbursements is by submitting expense reports for expenses that were paid by others. For instance, an employee might save the receipt from a meal that was paid for by another party and then request reimbursement for the meal himself.

Multiple Reimbursements

The least common of the expense reimbursement schemes involves multiple reimbursements. This type of fraud involves the submission of a single expense more than one time. The most frequent example of a multiple reimbursement scheme is the submission of several types of support for the same expense.

EXAMPLE

An employee would use an airline ticket stub and a travel agency invoice on separate expense reports so that he could be reimbursed twice for the cost of a single flight. The fraudster would have his division president authorize one report and have the vice president approve the other so that neither would see both reports. Additionally, the perpetrator allowed a time lag of about a month between the filing of the two reports so that the duplication would be less noticeable.

In cases where a company does not require original documents as support, some employees even use several copies of the same support document to generate multiple reimbursements. Rather than file two expense reports, employees might also charge an item to the company credit card, save the receipt, and attach it to an expense report as if they paid for the item themselves. The victim organization therefore ends up paying twice for the same expense.

Detection of Expense Reimbursement Schemes

Detecting expense reimbursement fraud involves two basic methods. The first of these is a review and analysis of expense accounts. The second detection method is a detailed review of expense reports.

Review and Analysis of Expense Accounts

Generally, expense account review uses one of two methods: historical comparisons or comparisons with budgeted amounts. A historical comparison compares the balance expended this period in relation to the balance spent in prior, similar periods. When performing this review, consider changes to the marketing, servicing, or other company operations.

Budgets are estimates of the money and/or time necessary to complete the task. They are based on past experience with consideration for current and future business conditions. Therefore, when comparing actual and budgeted expenses, determining excessive expenses or inaccurate budget estimates is important.

Detailed Review of Expense Reports

Overall, the best detection method is a detailed review of employee expense reports. This method requires that the fraud examiner have a calendar and a copy of the employee's schedule for the relevant period at the time of the examination. The fraud examiner should

be familiar with the company's travel and entertainment policies. Additionally, the following two steps might help to detect and deter employee expense abuses:

- Require employees to submit their expense reports for a detailed review before payment is reimbursed. If an employee knows that his expense report will be thoroughly reviewed, he will be less likely to include fraudulent expenses on the report.
- Periodically audit travel and entertainment accounts. This is particularly effective shortly before employee performance reviews.

Prevention of Expense Reimbursement Schemes

Detailed Expense Reports: Submission and Review

Detailed expense reports should require the following information:

- Receipts or other support documentation
- Explanation of the expense, including specific business purpose
- Time period when the expense occurred
- Place of expenditure
- Amount

When possible, require that employees submit original paper receipts. Given the amount of electronic and Internet commerce that happens in today's world, this is not always possible. Keep in mind that electronic copies of receipts are often much easier to forge and alter than paper receipts. Special attention should be paid to any receipts that come via email or email attachment. Consider corroborating prices on Internet receipts with those found on the vendor's website.

It is not enough to have the detailed reports submitted if they are not reviewed. A policy requiring the periodic review of expense reports, coupled with examining the appropriate detail, will help deter employees from submitting personal expenses for reimbursement.

ASSET MISAPPROPRIATION: INVENTORY AND OTHER ASSETS

Employees target inventory, equipment, supplies, and other noncash assets for theft in a number of ways. These schemes can range from stealing a box of pens to the theft of millions of dollars' worth of company equipment. The term *inventory and other assets* is meant to encompass the misappropriation schemes involving any assets held by a company other than cash.

Misuse of Inventory and Other Assets

There are basically two ways a person can misappropriate a company asset. The asset can be *misused* or it can be *stolen*. Simple misuse is obviously the less egregious of the two. Assets that are misused but not stolen typically include company vehicles, company supplies, computers, and other office equipment.

EXAMPLE

An employee made personal use of a company vehicle while on an out-of-town assignment. The employee provided false information, both written and verbal, regarding the nature of his use of the vehicle. The vehicle was returned unharmed and the cost to the perpetrator's company was only a few hundred dollars. Nevertheless, such unauthorized use of a company asset does amount to fraud when a false statement accompanies the use.

One of the most common examples of the misuse of company assets occurs when an employee uses company equipment to do personal work on company time. For instance, an employee might use his computer at work to write letters, print invoices, or do other work connected with a business he runs on the side. In many instances, these side businesses are of the same nature as the employer's business, so the employee is essentially using his employer's equipment to compete with the employer.

The Costs of Inventory Misuse

The costs of inventory misuse are difficult to quantify. To many individuals, this type of fraud is not viewed as a crime, but rather as "borrowing." In truth, the cost to a company from this kind of scheme is often immaterial. When a perpetrator borrows a stapler for the night or takes home some tools to perform a household repair, the cost to his company is negligible, as long as the assets are returned unharmed.

But misuse schemes can also be very costly. Take, for example, the situation discussed previously in which an employee uses company equipment to operate a side business during work hours. Since the employee is not performing his work duties, the employer suffers a loss in productivity. If the low productivity continues, the employer might have to hire additional employees to compensate, diverting more capital to wages. If the employee's business competes with the employer's, then lost business could be an additional cost. Unauthorized use of equipment can also mean additional wear and tear, causing the equipment to break down sooner than it would have under normal business conditions. Additionally, when an employee "borrows" company property, there is no guarantee that he will bring it back. This is precisely how some theft schemes begin. Despite some opinions to the contrary, asset misuse is not always a harmless crime.

Theft of Inventory and Other Assets

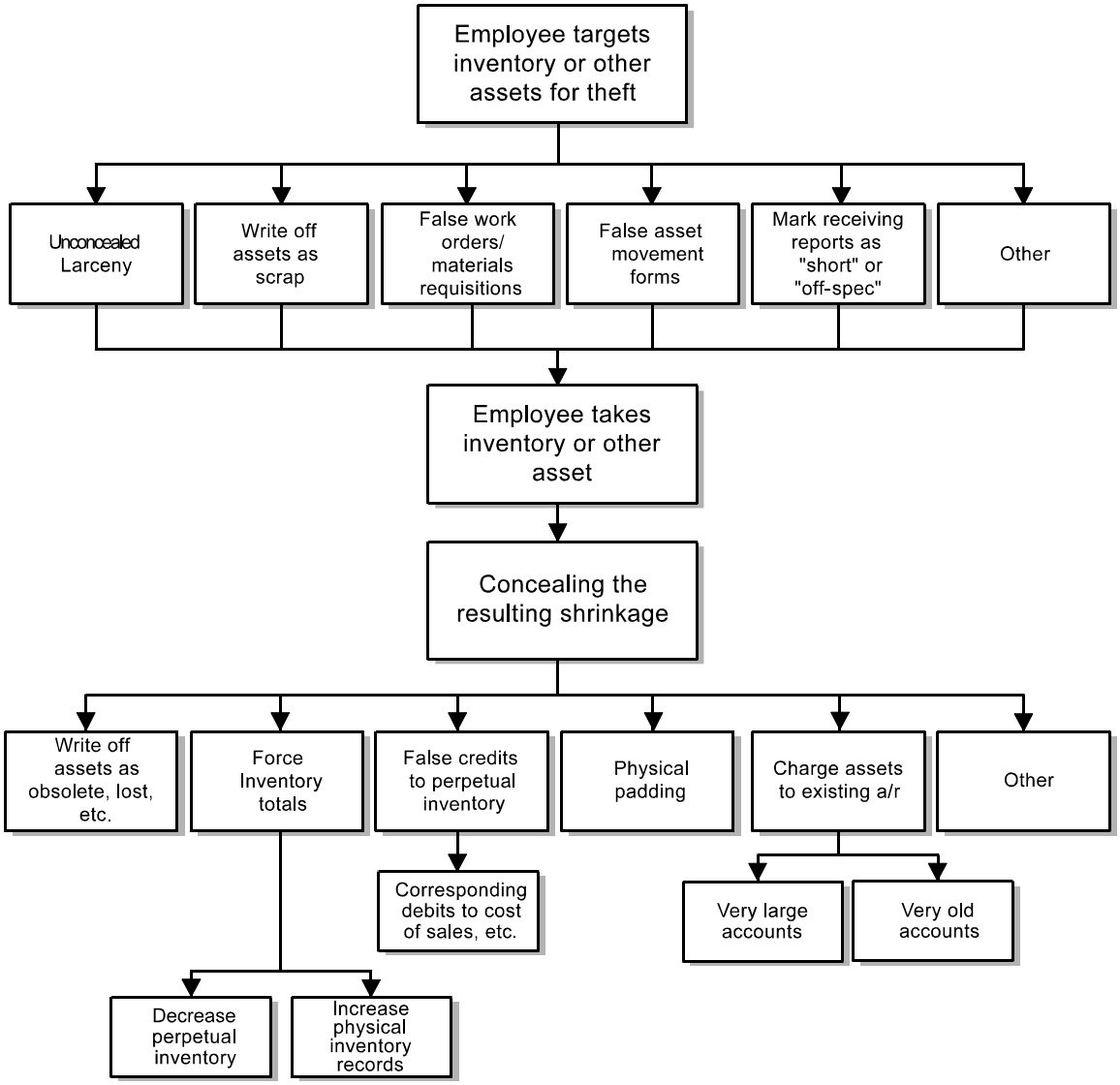
Though the misuse of company property might be a problem, the *theft* of company property is obviously of greater concern. Losses resulting from larceny of company assets can run into the millions of dollars. Most schemes where inventory and other noncash assets are stolen fall into one of four categories: larceny schemes, asset requisition and transfer schemes, purchasing and receiving schemes, and false shipment schemes.

Larceny Schemes

The textbook definition of *larceny* is "Felonious stealing, taking and carrying, leading, riding, or driving away another's personal property, with intent to convert it or to deprive owner thereof. The unlawful taking and carrying away of property of another with intent to appropriate it to use inconsistent with latter's rights."[1] This definition is so broad that it encompasses every kind of asset theft. To gain a more specific understanding of the methods used to steal inventory and other assets, the definition of larceny has been restricted. For the purposes of classifying asset misappropriations, the term *larceny* is meant to refer to the most basic type of inventory theft: the schemes in which an employee simply takes inventory from the company premises without attempting to conceal the theft in the books and records. (See the "Noncash Larceny" flowchart that follows.) In other fraud schemes, employees might create false documentation to justify the shipment of

[1] *Black's Law Dictionary*. Sixth Edition. St. Paul, MN: West Publishing Co., 1990, 792.

merchandise or tamper with inventory records to conceal missing assets. Larceny schemes are more blunt. The culprit in these crimes takes company assets without trying to "justify" their absence.



Non-cash Larceny

Most noncash larceny schemes are not very complicated. They are typically committed by employees (warehouse personnel, inventory clerks, shipping clerks, etc.) with access to inventory or supplies. Many employees simply carry company assets away in open view of

other employees. People tend to assume that their friends and acquaintances are acting honestly. When they see a trusted coworker taking something out of the workplace, most people assume that the culprit has a legitimate reason for doing so.

EXAMPLE

A university faculty member was leaving his offices to take a position at a new school. He was permitted to take a small number of items to his new job, but certainly exceeded the intentions of the school when he loaded two trucks full of university lab equipment and computers worth several hundred thousand dollars. The perpetrator simply packed up these stolen assets along with his personal items and drove away.

Unfortunately, in all too many cases, the perpetrator's coworkers are fully aware that he is stealing company assets, yet they refrain from reporting the crime. There are several reasons that employees might ignore illegal conduct, such as a sense of duty to their friends, a "management vs. labor" mentality, poor channels of communication for whistleblowers, or intimidation of honest employees by the thief. When high-ranking personnel are stealing from their companies, employees often overlook the crime because they fear they will lose their jobs if they report it. In some cases, the coworkers might be assisting in the theft.

EXAMPLE

A school superintendent was not only pilfering school accounts, but was also stealing school assets. A search of his residence revealed a cellar filled with school property. A number of school employees knew or suspected the superintendent was involved in illegal dealings, but he was very powerful and people were afraid to report him for fear of retaliation. As a result, he was able to steal from the school for several years.

Ironically, employees who steal inventory are often highly trusted within their organizations. Because these employees are trusted, they might be given access to restricted areas, safes, supply rooms, or other areas where company assets are kept. This access makes it easy for these employees to steal.

It can be unwise for an employee to physically carry inventory and other assets off company premises. This practice carries with it the inherent risk and potential embarrassment of being caught red-handed with stolen goods on his person. Some employees avoid this problem by mailing company assets from the victim organization to a location where they can retrieve them without fear of being observed.

EXAMPLE

A spare-parts custodian took several thousand dollars' worth of computer chips and mailed them to a company that had no business dealings with the custodian's employer. He then reclaimed the merchandise as his own. By taking the step of mailing the stolen inventory, the fraudster allowed the postal service to unwittingly do his dirty work for him.

The False Sale

In many cases, corrupt employees use outside accomplices to help steal inventory. The false, or fake, sale is one method that depends upon an accomplice. Like most inventory thefts, the fake sale is not complicated. The employee-fraudster's accomplice pretends to buy merchandise, but the employee does not ring up the sale. The accomplice takes the merchandise without paying for it. To a casual observer, it will appear that the transaction is a normal sale. The employee bags the merchandise and might act as though a transaction is being entered on the register when in fact the "sale" is not recorded. The accomplice might even pass a nominal amount of money to the employee to complete the illusion. A related scheme occurs when an employee sells merchandise to an accomplice at an unauthorized discount.

Employees also sometimes enlist accomplices to return goods that the employee has already stolen. This is an easy way for the employee to convert the stolen inventory into cash.

Asset Requisitions and Transfers

Asset requisitions and other documents that allow noncash assets to be moved from one location in a company to another can be used to facilitate the theft of those assets. Employees use internal transfer paperwork to gain access to merchandise that they otherwise might not be able to handle without raising suspicion. These documents do not account for missing merchandise the way false sales do, but they allow a person to move the assets from one location to another. In the process of this movement, the thief steals the merchandise.

The most basic scheme occurs when an employee requisitions materials for some work-related project and then makes off with those materials. In some cases, the employee simply overstates the amount of supplies or equipment it will take to complete his work and pilfers the excess. In more ambitious schemes, the employee might invent a completely fictitious project that necessitates the use of certain assets he intends to steal.

EXAMPLE

An employee of a telecommunications company used false project documents to request approximately $100,000 worth of computer chips, allegedly to upgrade company computers. Knowing that this type of requisition required verbal authorization from another source, the employee set up an elaborate phone scheme to get the "project" approved. The fraudster used his knowledge of the company's phone system to forward calls from four different lines to his own desk. When the confirmation call was made, it was the perpetrator who answered the phone and authorized the project.

Dishonest employees sometimes falsify asset transfer forms so they can remove inventory from a warehouse or stockroom. The false documents allow the employee to remove merchandise from the warehouse, but instead of using it for a work-related purpose, the perpetrator simply takes it home. The obvious problem with this type of scheme is that the person who orders the merchandise will usually be the primary suspect when it turns up missing.

EXAMPLE

A manager requested merchandise from the company warehouse to be displayed on a showroom floor. The pieces he requested never made it to the showroom because he loaded them into a pickup truck and took them home. In some instances, he actually took the items in broad daylight and with the help of another employee. This individual thought he was immune from detection because the merchandise was requested via computer using a management-level security code. The code was not specific to any one manager, so there would be no way of knowing which manager had ordered the merchandise. Unfortunately for the thief, the company was able to record the computer terminal from which the request originated. The manager had used his own computer to make the request, which led to his undoing.

Purchasing and Receiving Schemes

Dishonest employees can also manipulate the purchasing and receiving functions of a company to facilitate the theft of inventory and other assets. It might seem that any purchasing scheme should fall under the heading of false billings, which were discussed earlier. There is, however, a distinction between the purchasing schemes that are classified as false billings and those that are classified as noncash misappropriations.

If an employee causes his company to purchase merchandise that the company does not need, this is a false billing scheme. The harm to the company comes in paying for assets for which it has no use. If, however, the assets were intentionally purchased by the company and later misappropriated by the perpetrator, this is classified as an inventory larceny scheme. Here, the company loses both the value of the merchandise and the *use* of the merchandise.

Falsifying Incoming Shipments

One of the most common examples of an employee abusing the purchasing and receiving functions occurs when a person charged with receiving goods on the victim company's behalf—such as a warehouse supervisor or receiving clerk—falsifies the records of incoming shipments. If, for example, 1,000 units of a particular item are received, the perpetrator indicates that only 900 were received. By marking the shipment short, the perpetrator can steal the 100 unaccounted for units.

The obvious problem with this kind of scheme is the fact that the receiving report does not match the vendor's invoice, which will likely cause a problem with payment. In the previous example, if the vendor bills for 1,000 units but the accounts payable voucher only shows receipt of 900 units of merchandise, then someone will have to explain where the extra 100 units went.

Some employees avoid this problem by altering only one copy of the receiving report. The copy that is sent to accounts payable indicates receipt of a full shipment, so the vendor will be paid without any questions. The copy used for inventory records indicates a short shipment so that the assets on hand will equal the assets in the perpetual inventory.

Instead of marking shipments short, the perpetrator might reject portions of a shipment as not being up to quality specifications. The perpetrator then keeps the "substandard" merchandise rather than sending it back to the supplier. The result is the same as if the shipment had been marked short.

False Shipments of Inventory and Other Assets

To conceal thefts of inventory and other assets, employees sometimes create false shipping documents and false sales documents to make it appear that the inventory they take was sold rather than stolen. (See the "False Shipments of Inventory and Other Assets" flowchart that follows.) The document that tells the shipping department to release inventory for delivery is usually the packing slip. By creating a false packing slip, a corrupt employee can cause

inventory to be fraudulently delivered to himself or an accomplice. The "sales" reflected in the packing slips are typically made to a fictitious person, a fictitious company, or the perpetrator's accomplice.

One benefit of using false shipping documents to misappropriate inventory or other assets is that the product is removed from the warehouse or storeroom by someone other than the perpetrator. The victim organization unknowingly delivers the targeted assets to the perpetrator of the scheme.

False packing slips allow inventory to be shipped from the victim company to the perpetrator, but they do not conceal the fact that inventory has been misappropriated in and of themselves. To hide the theft, fraudsters might create a false sale on the books so it appears that the missing inventory was shipped to a customer. Depending on how the victim organization operates, the perpetrator might have to create a false purchase order from the "buyer," a false sales order, and a false invoice along with the packing slip to create the illusion of a sale.

The result is that a fake receivable account goes into the books for the price of the misappropriated inventory. Obviously, the "buyer" of the merchandise will never pay for it. How do employees deal with these fake receivables? In some cases, the employee simply lets the receivable age on his company's books until it is eventually written off as uncollectible. In other instances, he might take affirmative steps to remove the sale—and the resulting delinquent receivable—from the books.

EXAMPLE

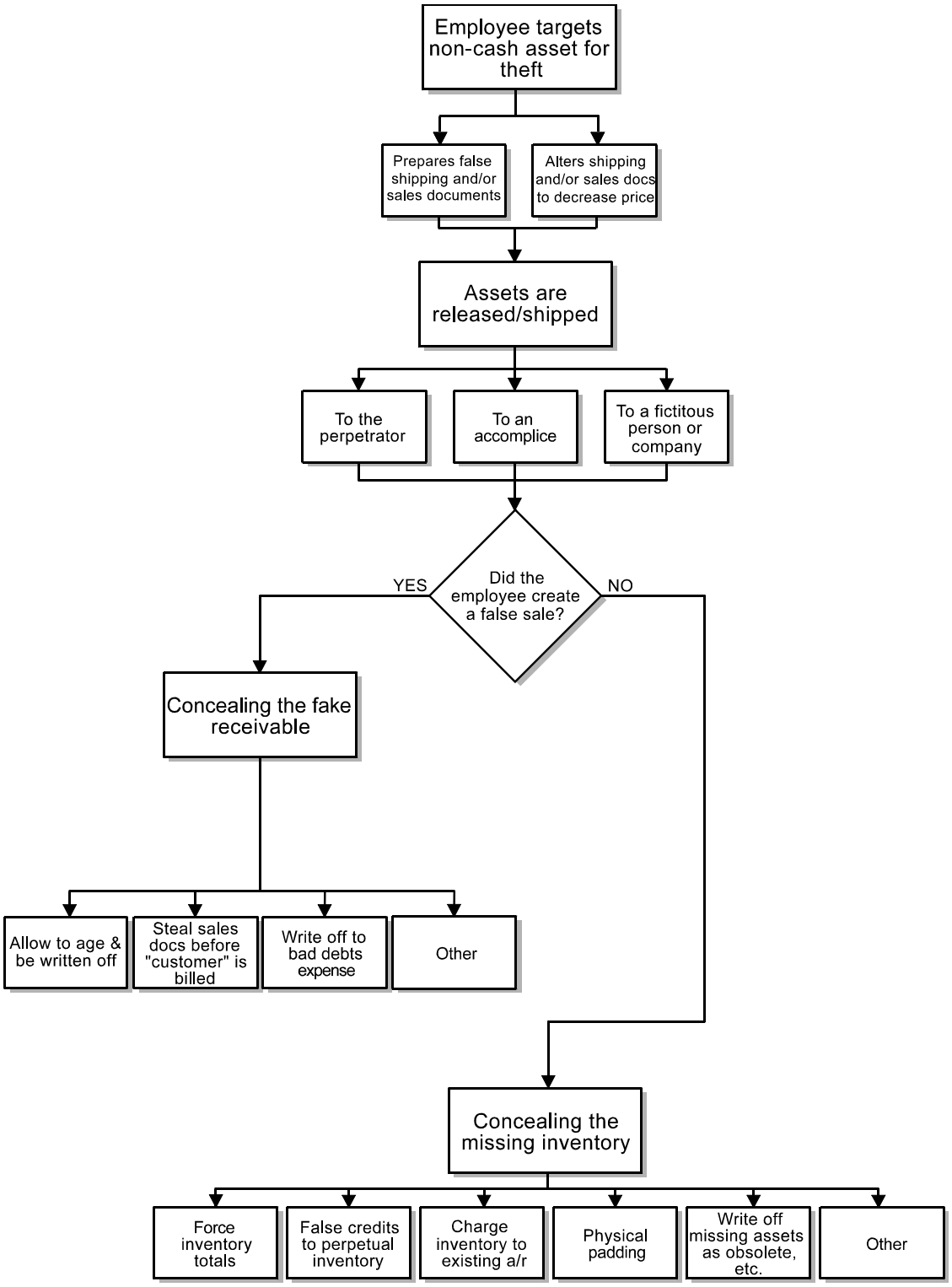
An employee generated false invoices and delivered them to the company warehouse for shipping. The invoices were then marked "delivered" and sent to the sales office. The perpetrator removed all copies of the invoices from the files before they were billed to the fictitious customer.

Another common way to get rid of delinquent receivables that result from theft schemes is to write off the receivables to accounts such as *discounts and allowances, bad debt expense,* or *lost and stolen assets*.

Instead of creating completely fictitious sales, some employees understate legitimate sales so that an accomplice is billed for less than delivered. The result is that a portion of the

merchandise is sold at no cost. In a typical scenario, a salesman fills out shipping tickets, which are forwarded to the warehouse. After the merchandise is shipped, the salesman instructs the warehouse employees to return the shipping tickets to him for "extra work" before they are sent to the invoicing department. The salesman then alters the shipping tickets, reducing either the quantity of merchandise sold or the price per unit sold.

Write-offs are often used to conceal the theft of assets after they have been stolen. In some cases, however, assets are written off to make them available for theft. For instance, an employee with the authority to declare inventory obsolete can write off this inventory as "scrap." Once assets are designated as scrap, it is often easier to misappropriate them. Fraudsters might be allowed to take the "useless" assets for themselves, buy them or sell them to an accomplice at a greatly reduced price, or simply give the assets away.



False Shipments of Inventory and Other Assets

Concealing Inventory Shrinkage

When inventory is stolen, the perpetrator's key concealment issue is shrinkage. *Inventory shrinkage* is the unaccounted-for reduction in the company's inventory that results from error or theft. For instance, assume a computer retailer has 1,000 computers in stock. After work one day, an employee loads 10 computers into a truck and takes them home. Now the company only has 990 computers, but since there is no record that the employee took 10 computers, the inventory records still show 1,000 units on hand. The company has experienced inventory shrinkage in the amount of 10 computers.

Shrinkage is one of the red flags that signal fraud. The perpetrator's goal is to proceed with his scheme undetected, so it is in his best interest to prevent anyone from looking for missing assets. This means concealing the shrinkage that occurs from asset theft.

Inventory and other assets are typically tracked through a two-step process. The first step, the perpetual inventory, is a running count that records how much inventory should be on hand. When new shipments of merchandise are received, for instance, this merchandise is entered into the perpetual inventory. Similarly, when goods are sold, they are removed from the perpetual inventory records. In this way, a company tracks its inventory on a day-to-day basis.

Periodically, a physical count of assets on hand should be made. In this process, someone actually goes through the storeroom or warehouse and counts everything that the company has in stock. This total is then matched to the amount of assets reflected in the perpetual inventory. A variation between the physical inventory and the perpetual inventory totals is shrinkage. While a certain amount of shrinkage might be expected in any business, large shrinkage totals could indicate fraud.

Altered Inventory Records

One of the simplest methods for concealing shrinkage is to change the perpetual inventory record so that it matches the physical inventory count. This is also known as a forced reconciliation of the account. The perpetrator simply changes the numbers in the perpetual inventory to make them match the amount of inventory on hand. For example, the employee might credit the perpetual inventory and debit the cost of sales account to bring the perpetual inventory numbers into line with the actual inventory count. Instead of using correcting entries to adjust the perpetual inventory, some employees simply delete or cover up the correct totals and enter new numbers.

There are two sides to the inventory equation: the perpetual inventory and the physical inventory. Instead of altering the perpetual inventory, a perpetrator who has access to the records from a physical inventory count can change those records to match the perpetual inventory. Returning to the computer store example, assume the company counts its inventory every month and matches it to the perpetual inventory. The physical count should come to 990 computers, since that is what is actually on hand. If the perpetrator is someone charged with counting inventory, he can simply write down that there are 1,000 units on hand.

Fictitious Sales and Accounts Receivable

When the perpetrator makes an adjusting entry to the perpetual inventory and cost of sales accounts as discussed previously, there is no sales transaction on the books that corresponds to these entries. To fix this problem, a perpetrator might enter a debit to accounts receivable and a corresponding credit to the sales account so that it appears the missing goods have been sold.

Of course, the problem of payment then arises because no one is going to pay for the goods that were "sold" in this transaction. There are two routes that a fraudster might take in this circumstance. The first is to charge the sale to an existing account. In some cases, employees charge fake sales to existing receivables that are so large that the addition of the assets that the perpetrator has stolen will not be noticed. Other corrupt employees charge the "sales" to accounts that are already aging and will soon be written off. When these accounts are removed from the books, the perpetrator's stolen inventory effectively disappears. The other adjustment that is typically made is a write-off to *sales discounts and allowances* or *bad debt expense*.

Write-off of Inventory and Other Assets

Writing off inventory and other assets is a relatively common way for employees to remove assets from the books before or after they are stolen. This eliminates the problem of shrinkage that inherently exists in every case of noncash asset misappropriation.

Physical Padding

Most methods of concealment deal with altering inventory records, either changing the perpetual inventory or miscounting during the physical inventory. In the alternative, some employees try to make it appear that there are more assets present in the warehouse or stockroom than there actually are. Empty boxes or boxes filled with bricks or other

inexpensive materials, for example, might be stacked on shelves to create the illusion of extra inventory.

Detection of Inventory Schemes

Statistical Sampling

Companies with inventory accounts typically have enormous populations of source documents. Statistical sampling allows the fraud examiner to inspect key attributes on a smaller portion (or sample) of those documents. For example, the fraud examiner might select a statistically valid, random sample of purchase requisitions to determine that all requisitions in the sample selected were properly approved. Statistical sampling enables the fraud examiner to predict the occurrence rate for the population and, therefore, determine with some accuracy the error rate or the potential for fraud.

Other items that could be sampled on a statistical basis include the following:

- Receiving reports
- Perpetual inventory records
- Raw materials requisitions
- Shipping documents
- Job cost sheets

The attributes tested for on the aforementioned documents might include a specific date, item, or location.

Perpetual Inventory Records

Unexplained entries in the perpetual records might reveal embezzlement losses.

- Are all the reductions to the perpetual inventory records explained by source documents (such as sales invoices, approvals to remove to scrap inventory, or spoilage)?
- Are all increases in perpetual records explained by source documents such as receiving reports?

Shipping Documents

Inventory theft could be uncovered by answers to questions such as:

- Are all sales properly matched with a shipping document?
- Are any shipping documents not associated with a sale?
- Is inventory disappearing from storage?

Physical Inventory Counts

Physical inventory counts can sometimes give rise to inventory theft detection. However, because other explanations satisfy inventory shortages (such as shrinkage), historical analysis of inventory is usually necessary. Furthermore, if the only method used to detect inventory fraud is the year-end physical count, the perpetrators will have had all year to devise concealment methods to circumvent potential detection.

Analytical Review

Inventory fraud might be detected by using an analytical review because certain trends become immediately clear. For example, sales and cost of goods sold should move together since they are directly related. However, if the cost of goods sold increases by a disproportionate amount relative to sales and no changes occur in the purchase prices, quantities purchased, or quality of products purchased, the cause of the disproportionate increase in cost of goods sold might be one of two things: (1) ending inventory has been depleted by theft or (2) someone has been embezzling money through a false billing scheme (i.e., submitting invoices and collecting the payments for inventory that was never delivered).

An analytical review of all the component parts of the cost of goods sold should indicate to the fraud examiner where to direct further inquiries. For example, assume that the type of inventory purchased is the same and there is no change in the manufacturing process or purchase price. If sales and cost of sales change from $5,650,987 and $2,542,944 to $6,166,085 and $2,981,880, respectively, what is the data telling the fraud examiner? For one thing, sales have increased by 9.12 percent, whereas cost of sales increased by 17.26 percent. The profit margin has decreased by 3 percent (from 55 to 52 percent). Based on this data, the fraud examiner might want to look further at the components of inventory (e.g., beginning inventory, purchases, and ending inventory). If beginning inventory was $1,207,898, purchases were $2,606,518 and $2,604,972, respectively, and ending inventory was $894,564, then an inventory matrix would look like the following:

	Year 1	Year 2	Percentage Change
Beginning Inventory	$1,207,898	$1,271,472	5.26%
Purchases	2,606,518	2,604,972	<0.06%>
Goods Available for Sale	$3,814,416	$3,876,444	1.63%
Ending Inventory	<1,271,472>	< 894,564>	<29.64%>
Cost of Sales	$2,542,944	$2,981,880	17.26%

Inventory purchases, as a percentage of sales, have declined from 46.13 to 42.25 percent. From this example, one can hypothesize that: (1) inventory purchases were purposely increased in year one only to be liquidated in year two; (2) the increased sales in year two were unexpected and the purchase of inventory did not keep pace with the sales; or (3) there might be some fraud scheme in inventory. If the fraud examiner is unable to ascertain a reasonable explanation such as (1) or (2) above through an interview, then further examination of the ending inventory might be warranted.

The fraud examiner might next look at the differences in the physical inventory procedures to see if that created a more (or less) accurate inventory count at the end of either year one or year two. If there is no other logical explanation, then further investigation into these and other inventory accounts might be necessary to explain the anomalies occurring in inventory.

Computer-Generated Trend Analysis

The computer can be used to facilitate obtaining lists of items with specified attributes. For example, in a lumberyard operation, the computer can be programmed to list all purchases of four by four cedar fence posts of a certain length. The fraud examiner should check all the source documents that are represented by the listing. By examining the source documents for each of these purchases, the fraud examiner can plot trends to determine the occurrence of the following (or other) patterns:

SEARCHES	SCHEMES
Purchases by vendor	If the same vendor is receiving favorable treatment
Inventory levels by types and dates	If inventory is being purchased at its reorder point or if excess inventory is being ordered
Inventory shipped by address	If the vendor's address matches either an employee address or the address of another vendor
Cost per item	If discounts are properly credited to purchases
Direct labor by item	If there are excess labor hours being added to a particular job or item
Direct materials by item	If materials are properly charged to the job (too much or the wrong materials)
Overhead per inventory item	If overhead is being properly applied, and applied only once
Disposals then reorders	If usable inventory is being prematurely designated as scrap
Shortages by inventory item	If there is inventory theft or the reorder system is not functioning
Returns and allowances	If there is an unusually high incidence of returns and allowances
Sales allowances	If sales allowances are not properly credited to promotional allowances
Buyer	If the buyer is not acting within scope of authority

Detailed Audit Program

The following audit program will also be helpful in establishing inventory control:

- Do adequate, detailed, written inventory instructions and procedures exist? Do inventory procedures give appropriate consideration to the location and arrangement of inventories?
- Do inventory procedures give appropriate consideration to identification and description of inventories?
- Is the method of determining inventory quantities specified (e.g., weight, count)?
- Is the method used for recording items counted adequate (e.g., count sheets, prenumbered tags)?
- Are inventory tags used? If yes: (1) Are they prenumbered? (2) Is accounting for inventory tags adequate and does it include control with respect to tags used, unused, and voided?
- Are adequate procedures in place to identify inventory counted, ensure that all items have been counted, and prevent double counting?
- Are obsolete, slow-moving, or damaged inventories properly identified and segregated?
- Is the inventory reasonably identifiable for proper classification in the accounting records (e.g., description, stage of completion)?
- Are inventory counts subject to (1) complete recounts by persons independent of the ones involved in the initial counts, (2) recounts only of merchandise having substantial value, or (3) spot checks by supervisory personnel?
- Are counts performed by employees whose functions are independent of the physical custody of inventories and recordkeeping functions?
- Do proper accounting controls and procedures exist for the exclusion from inventory of merchandise on-hand that is not property of the client (e.g., customers' merchandise, consignments in)?
- Do proper accounting controls and procedures exist for the inclusion in inventory of merchandise not on-hand, but the property of the client (e.g., merchandise in warehouses, out on repair, consignments out)?
- Will identical inventory items in various areas be accumulated to allow a tie in total counts to a summary listing subsequent to the observation?
- Is the movement of inventory adequately controlled (e.g., shipping and receiving activities suspended) during the physical count to ensure a proper cut-off?
- Are significant differences between physical counts and detailed inventory records investigated before the accounting and inventory records are adjusted to match the physical counts?

- Will inventory at remote locations be counted?
- Will special counting procedures or volume conversions be necessary (e.g., items weighed on scale)?
- How will work-in-process inventory be identified?
- How will the stage of completion of work-in-process inventory be identified?
- Are there any other matters that should be noted for the inventory count?

Prevention of Inventory Schemes

There are four basic measures which, if properly installed and implemented, might help prevent inventory fraud. They are proper documentation, separation of duties (including approvals), independent checks, and physical safeguards.

Proper Documentation

The following items should be prenumbered and controlled:

- Requisitions
- Receiving reports
- Perpetual records
- Raw materials requisitions
- Shipping documents
- Job cost sheets

However, not all inventory requires the purchasing of raw materials. In these cases, the proper documentation might take the form of prenumbered and controlled tickets and receipts for sales.

Separation of Duties

The following duties should be handled by different personnel:

- Requisition of inventory
- Receipt of inventory
- Disbursement of inventory
- Conversion of inventory to scrap
- Receipt of proceeds from disposal of scrap

Independent Checks

Someone independent of the purchasing or warehousing functions should conduct physical observation of inventory. The personnel conducting the physical observations should also be knowledgeable about the inventory.

Physical Safeguards

All merchandise should be physically guarded and locked; access should be limited to authorized personnel only. For example, strategic placement of security guards might aid in the detection and deterrence of potential theft schemes. Electronic methods might also be used, such as cameras and surveillance devices. The effectiveness of any device will, however, depend on the employee's knowledge that physical safeguard controls are adhered to, as well as the type of inventory available for misappropriation.

Misappropriation of Intangible Assets

Misappropriation of Information

In addition to misappropriation of tangible noncash assets, organizations are vulnerable to theft of proprietary information, which can undermine their value, reputation, and competitive advantages and result in legal liabilities. Companies frequently make sizeable technological investments in protecting their information from external information thieves, but often the biggest threats are internal. Employees are the most likely to be in a position to exploit their employers' information security. After all, who has more insider information and access to proprietary records and data than an employee or former employee?

Information misappropriation schemes commonly include theft by employees of competitively sensitive information, such as customer lists, marketing strategies, trade secrets, new products, or details on development sites. In one case, an employee who felt a sense of entitlement for having contributed to a new product design stole the design in an attempt to get ahead in a new job with a competitor. And in another case, a disgruntled former employee sold a company trade secret to a competitor to retaliate for what he felt was unfair treatment.

It is critical that companies identify their most valuable information and take steps to protect it. This process must be a cross-departmental endeavor, involving specialists from corporate security/risk management, information technology, human resources, marketing, research

and development, and so on. If in-house capabilities do not exist, companies can bring in information security experts to assist them in designing an effective information security system, including awareness training for employees. An information security system might include measures such as limiting access to networks, systems, or data to those who have a legitimate need for access; protecting company data through the use of firewalls and virus scanning software; implementing and enforcing confidentiality agreements and restrictive covenants where appropriate; performing adequate background checks on employees; establishing and enforcing a security policy, and much more.

Misappropriation of Securities

Although securities are the least likely asset to be misappropriated, the loss of security misappropriation cases has the potential to be extremely high. To avoid falling victim to a misappropriation of securities scheme, management must maintain proper internal controls over the company's investment portfolio, including proper separation of duties, restricted access to investment accounts, and periodic account reconciliations.

In one example, a misappropriation of securities occurred when the director of accounting and finance, who was responsible for making trades, left his computer unattended for a short time while signed into one of the company's investment accounts. Another employee, a senior accountant, took the opportunity to access the director's computer to sell $15,000 worth of investments and have the proceeds mailed to the company. Due to lax internal controls, she was able to intercept the check and deposit it into her own bank account. Because this employee was in charge of reconciling the investment accounts and had the access needed to enter and post journal entries to the general ledger, she was able to easily hide her scheme by writing off a "loss" on investments to an expense account. It wasn't until almost a year later, when auditors were reviewing the company's books, that the scheme was uncovered. By that time, the thief was nowhere to be found.

BRIBERY AND CORRUPTION

Corruption

Corruption is a term used to describe various types of wrongful acts designed to cause an unfair advantage. It can take on many forms, including bribery, kickbacks, illegal gratuities, economic extortion, and collusion. Generally, it involves the wrongful use of influence to procure a benefit for the actor or another person, contrary to the duty or the rights of others. The various forms of corruption are often used in combination, which reinforces the schemes' potency and makes them more difficult to combat.

Corruption can be found in any business or organization, and it is one of the three major categories of occupational fraud and abuse (along with asset misappropriation and fraudulent statements). The most common area for corruption in an organization is in the purchasing environment, and most corruption schemes involve employees acting alone or in collusion with vendors/contractors.

Corruption is a significant problem for organizations, particularly due to the drive for growth in international markets. Despite the multitude of anti-corruption legislation and increased enforcement efforts around the world, corruption is still prevalent.

Bribery

Bribery may be defined as the offering, giving, receiving, or soliciting of corrupt payments (i.e., items of value paid to procure a benefit contrary to the rights of others) to influence an official act or business decision. For a detailed discussion of the legal elements of bribery and corruption, please see the Law section of the *Fraud Examiners Manual*.

At its heart, a bribe is a business transaction, albeit an illegal or unethical one. A person "buys" influence over the recipient of the bribe to procure a benefit that is contrary to the duty or the rights of others.

Bribery schemes can be difficult to detect.

In the employment context, bribery involves a conflict of interest in which the employee's personal interest overwhelms his professional responsibilities. Though bribery schemes are not nearly as common as other forms of occupational fraud, such as asset misappropriations, they tend to be much more costly.

Additionally, bribery involves collusion between at least two parties.

Bribery schemes are classified into two types: official bribery and commercial bribery.

Official bribery refers to the corruption of a public official to influence an official act of government. The term *official act* stems from traditional bribery statutes that only proscribe payments made to influence the decisions of government agents or employees.

In contrast, *commercial bribery* refers to the corruption of a private individual to gain a commercial or business advantage. In commercial bribery schemes, something of value is offered to influence a business decision rather than an official act, as is the case in official bribery. Commercial bribery may or may not be a criminal offense. For example, in the United States, there is no general federal law prohibiting commercial bribery in all instances; however, there are statutes prohibiting bribery of employees of financial institutions to influence a loan. Additionally, there is a general commercial bribery offense under the UK Bribery Act, which is an Act of Parliament of the United Kingdom. Therefore, the law of the particular jurisdiction and the facts of the case will determine whether bribery in the private sector may be prosecuted criminally. But generally, commercial bribery is a civil offense—meaning the aggrieved party can recover damages and other private remedies—in most jurisdictions, and it can often be pursued in a civil action as breach of fiduciary duty or conflict of interest. See the Law section of the *Fraud Examiners Manual* for more information.

Kickback Schemes

Bribery often takes the form of kickbacks, a form of negotiated bribery in which a commission is paid to the bribe-taker in exchange for the services rendered. Thus, kickbacks are improper, undisclosed payments made to obtain favorable treatment. In the government setting, kickbacks refer to the giving or receiving of anything of value to obtain or reward favorable treatment in relation to a government contract. In the commercial sense, kickbacks refer to the giving or receiving of anything of value to influence a business decision without the employer's knowledge and consent.

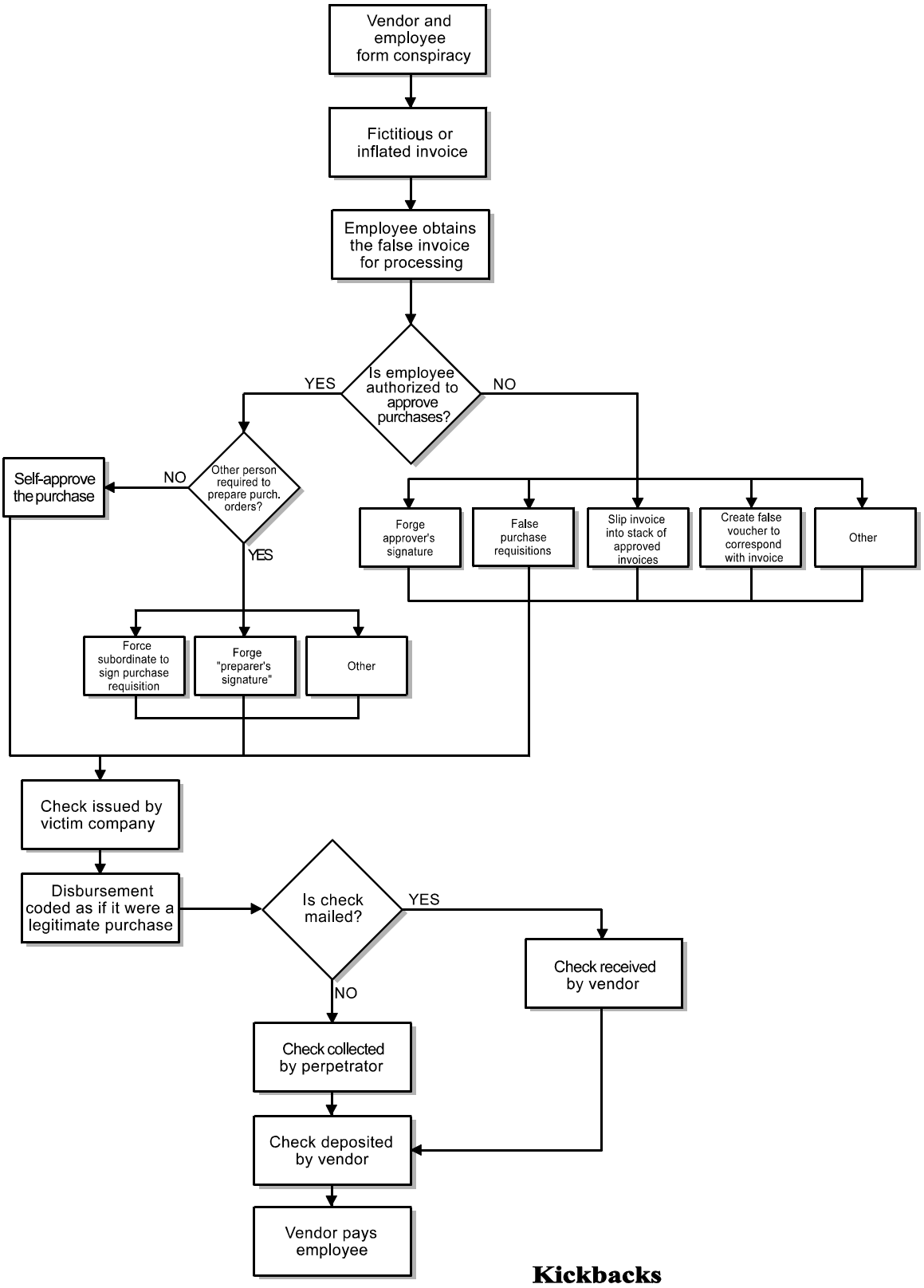
Usually, kickback schemes are similar to the billing schemes described in the "Asset Misappropriation" section. They involve the submission of invoices for goods and services that are either overpriced or fictitious. (See the "Kickbacks" flowchart that follows.) Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and third parties. In a common type of kickback

scheme, a vendor submits a fraudulent or inflated invoice to the victim organization and an employee of that organization helps make sure that a payment is made on the false invoice. For his assistance, the employee-fraudster receives a payment from the vendor. This payment is the kickback.

Most kickback schemes attack the purchasing function of the victim organization; therefore, these frauds are often undertaken by employees with purchasing responsibilities. Purchasing employees usually have direct contact with vendors and therefore have an opportunity to establish a collusive relationship.

EXAMPLE

A purchasing agent redirected a number of orders to a company owned by a supplier with whom he was conspiring. In return for the additional business, the supplier paid the purchasing agent over half the profits from the additional orders.


Vendor and employee form conspiracy
Fictitious or inflated invoice
Employee obtains the false invoice for processing
Is employee authorized to approve purchases?
YES
NO
Other person required to prepare purch. orders?
NO
YES
Self-approve the purchase
Forge approver's signature
False purchase requisitions
Slip invoice into stack of approved invoices
Create false voucher to correspond with invoice
Other
Force subordinate to sign purchase requisition
Forge "preparer's signature"
Other
Check issued by victim company
Disbursement coded as if it were a legitimate purchase
Is check mailed?
YES
NO
Check received by vendor
Check collected by perpetrator
Check deposited by vendor
Vendor pays employee
Kickbacks

Diverting Business to Vendors

In some kickback schemes, an employee-fraudster receives a kickback for directing excess business to a vendor. In these cases, there might not be any overbilling involved; the vendor simply pays the kickbacks to ensure a steady stream of business from the purchasing company.

If no overbilling is involved in a kickback scheme, one might wonder where the harm lies. Assuming the vendor wants to get the buyer's business and does not increase his prices or bill for undelivered goods and services, how is the buyer harmed? The problem is that, having bought off a purchasing company employee, a vendor is no longer subject to the normal economic pressures of the marketplace. This vendor does not have to compete with other suppliers for the purchasing company's business, and thus has no incentive to provide a low price or quality merchandise. In these circumstances, the purchasing company almost always ends up overpaying for goods or services.

EXAMPLE

A travel agency provided free travel and entertainment to the purchasing agent of a retail company, and in return, the purchasing agent agreed to book all of his department's trips through the travel agent. The victim company estimated that it paid $10,000 more for airfare over a two-year period by booking through the corrupt travel agency than if it had used a different company.

Once a vendor knows it has an exclusive purchasing arrangement, it is motivated to raise prices to cover the cost of the kickback.

Most bribery schemes end up as overbilling schemes even if they do not start that way. This is one reason why most business codes of ethics prohibit employees from accepting undisclosed gifts from vendors. In the end, an organization is sure to pay for its employees' unethical conduct.

Overbilling Schemes

EMPLOYEES WITH APPROVAL AUTHORITY

In most instances, kickback schemes involve overbilling. In these schemes, a vendor submits inflated invoices to the victim organization, and the false invoices either overstate the cost of actual goods and services or reflect fictitious sales. To ensure that the inflated invoices get approved, the corrupt vendor offers kickbacks to an employee of the victim organization

who has the authority to approve payment of the fraudulent invoices. By enlisting the help of an employee with such authority, the corrupt vendor ensures that the invoices will be paid without undue hassles.

EXAMPLE

A manager was authorized to purchase fixed assets for his company as part of a leasehold improvement. The materials he ordered were of a cheaper quality and lower price than what was specified, but the contract price he negotiated did not reflect this. Therefore, the victim company paid for high-quality materials, but received low-quality materials. The difference in price between the true cost of the low-quality materials and what the company paid was diverted back to the manager as a kickback.

The ability of the employee to authorize purchases, including the ability to authorize *fraudulent* purchases, is usually a key to kickback schemes. If the fraudster can authorize payments himself, he does not have to submit purchase requisitions to a superior who might question the transaction's validity.

FRAUDSTERS LACKING APPROVAL AUTHORITY

While the majority of kickback schemes involve individuals with authority to approve purchases, this authority is not an absolute necessity. When an employee cannot approve fraudulent purchases himself, he can still orchestrate a kickback scheme if he can circumvent accounts payable controls. In some cases, he can do this by filing a false purchase requisition. If a trusted employee tells his superior that the company needs certain materials or services, this is sometimes sufficient to get a false invoice approved for payment. Such schemes are generally successful when the person with approval authority is inattentive or is forced to rely on his subordinate's guidance in purchasing matters.

Corrupt employees might also prepare false vouchers to make fraudulent invoices appear legitimate. Where proper controls are in place, a completed voucher is required before accounts payable will pay an invoice. To do this, the fraudster must create a purchase order that corresponds with the vendor's fraudulent invoice. The fraudster might forge the signature of an authorized party on the purchase order to show that the acquisition has been approved. If the company's payables system is computerized, an employee with access can enter the system and authorize payments on fraudulent invoices.

In less sophisticated schemes, a corrupt employee might simply take a fraudulent invoice from a vendor and slip it into a stack of prepared invoices before they are input into the accounts payable system. A more detailed description of how false invoices are processed can be found in the "Billing Schemes" section.

Kickback schemes can be very difficult to detect. In a sense, the victim organization is being attacked from two directions—externally and internally. Externally, a corrupt vendor submits false invoices that induce the victim organization to pay for goods or services that it does not receive. Internally, one or more of the victim organization's employees waits to corroborate the false information provided by the vendor.

Other Kickback Schemes

Kickbacks are not always paid to employees to process phony invoices. Some outsiders seek other fraudulent assistance from employees of the victim organization. For instance, inspectors are sometimes paid off to accept substandard materials or to accept short shipments of goods.

Representatives of companies wishing to purchase goods or services from the victim organization at unauthorized discounts sometimes bribe employees with billing authority. The corrupt employees make sales to their accomplices at greatly reduced rates—sometimes even selling items at a loss—and in return, they receive a portion of the discount.

Illegal Gratuities

Illegal gratuities are items of value given to reward a decision, often after the recipient has made the decision. Illegal gratuities are similar to bribery schemes except that, unlike bribery schemes, illegal gratuity schemes do not necessarily involve an intent to influence a particular decision before the fact. That is, an illegal gratuity occurs when an item of value is given for, or because of, some act. Often, an illegal gratuity is merely something that a party who has benefited from a decision offers as a "thank you" to the person who made the beneficial decision.

EXAMPLE

A city commissioner negotiated a land development deal with a group of private investors. After the deal was approved, the private investors rewarded the commissioner and his wife with a free international vacation, all expenses paid.

At first glance, it might seem that illegal gratuities schemes are harmless as long as the business decisions in question are not influenced by the promise of payment. But most organizations' ethics policies forbid employees from accepting unreported gifts from vendors. One reason for such blanket prohibitions is that illegal gratuities schemes can (and do) evolve into bribery schemes. Once an employee has been rewarded for an act such as directing business to a particular supplier, he might reach an understanding with the gift giver that future decisions will also be made to benefit the gift giver. Additionally, even though no outright promise of payment has been made in an illegal gratuity, employees might direct business to certain companies in the hope that they will be rewarded with money or gifts.

Economic Extortion

An extortion case is often the other side of a bribery case. *Extortion* is defined as the obtaining of property from another, with the other party's consent induced by wrongful use of actual or threatened force or fear. Economic extortion is present when an employee or official, through the wrongful use of actual or threatened force or fear, demands money or some other consideration to make a particular business decision. That is, economic extortion cases are the "Pay up or else …" corruption schemes.

To constitute extortion, the threat must be the controlling reason that the victim gives up a right or property. The following types of threats can constitute extortion:

- Physical harm
- Property damage
- Accusing a person of a crime
- Disgracing a person
- Public exposure

Accordingly, a demand for a bribe or kickback, coupled with a threat of adverse action if the payment is not paid, might constitute extortion. In any situation where an employee might accept bribes to favor a particular company or person, the situation could be reversed to a point where the employee extorts money from a potential purchaser or supplier.

EXAMPLE

A plant manager for a utility company started his own business on the side. The manager forced vendors who wanted to do work for the utility company to divert some of their

business to his own company. Those that did not "play ball" lost their business with the utility.

Collusion

Collusion refers to an agreement between two or more individuals to commit an act designed to deceive or gain an unfair advantage. Typically, collusion involves some sort of kickback, which can result in fraudulent billing or inferior goods.

Methods of Making Corrupt Payments

Often, corruption schemes involve corrupt payments—items of value paid to procure a benefit contrary to the rights of others. There are various ways to make corrupt payments, and many do not involve money. Any tangible benefit given or received with the intent to corruptly influence the recipient can be an illegal payment, but there are certain traditional methods of making corrupt payments that fall into the following hierarchical categories.

Gifts, Travel, and Entertainment

Most bribery and corruption schemes begin with gifts and favors. Common early gifts and favors include:

- Wine and liquor (consumable)
- Clothes and jewelry for the recipient or spouse
- Sexual favors
- Lavish entertainment
- Paid vacations
- Free luxury transportation
- Free use of resort facilities
- Gifts of the briber's inventory or services, such as construction of home improvements by a contractor

Cash Payments

Corrupt payments do occur in the form of cash payments, but paying in cash is not a practical method when dealing with large sums. Accordingly, corrupt payers generally avoid using cash when making large payments.

Checks and Other Financial Instruments

Corrupt payments are often made by normal business check, cashier's check, or wire transfer. When such payments are made, they must be disguised. When a payer makes such

payments, they might be disguised as some sort of legitimate business expense (e.g., consulting fees). Also, such payments can be made directly or through an intermediary.

Hidden Interests

Additionally, the payer might give the recipient a hidden interest in a joint venture or other profit-making enterprise.

Such corrupt payments are hard to detect for a number of reasons. The recipient's interest might be concealed through a straw nominee, hidden in a trust or other business entity, or included by an undocumented verbal agreement. Also, even if such payments are identified, proving they originated with corrupt intent is also difficult to demonstrate.

Loans

Corrupt payments often take the form of loans. Three types of "loans" often turn up in corruption cases:

- An outright payment that is falsely described as an innocent loan
- A legitimate loan in which a third-party—the corrupt payer—makes or guarantees the loan's payments
- A legitimate loan made on favorable terms (e.g., an interest-free loan)

Credit Cards

A corrupt payment can be in the form of credit card use or payments toward a party's credit card debt. The payer might use his credit card to pay a recipient's transportation, vacation, or entertainment expenses, or he might pay off a recipient's credit card debt. In some instances, the recipient might carry and use the corrupt payer's credit card.

Transfers Not at Fair Market Value

Corrupt payments might occur in the form of transfers for a value other than fair market. In such transfers, the corrupt payer might sell or lease property to the recipient at a price that is less than its market value, or he might agree to buy or rent property from the recipient at inflated prices. The recipient might also "sell" an asset to the payer but retain the title or use of the property.

Promises of Favorable Treatment

Corrupt payments might come in the form of promises of favorable treatment. Such promises commonly take the following forms:

- A payer might promise a government official lucrative employment when the recipient leaves government service.
- An executive leaving a private company for a related government position might be given favorable or inflated retirement and separation benefits.
- The spouse or other relative of the intended recipient might also be employed by the payer company at an inflated salary or with little actual responsibility.

Detection of Bribery Schemes

Red Flags of Bribery and Corruption Schemes

Corruption can affect politicians, government officials, management, and procurement staff. It can arise from a sense of entitlement, a thirst for power, or a basic need for money. It is an evasive fraud that is difficult to detect, but knowing the red flags is the first step in combating corruption.

Most bribery schemes are detected through tips from honest and disgruntled coworkers or vendors. These allegations can be evaluated by analyzing the red flags associated with the suspect people or transactions. Fraud examiners can identify numerous red flags in the behavior of employees and third parties, as well as in internal control deficiencies.

Red Flags of Corrupt Employees

Some common red flags of a corrupt employee include:

- A high success rate in markets where competitors are known to bribe
- Reputation for regularly accepting inappropriate gifts
- Extravagant lifestyle
- Reputation for taking action on his own or directing subordinates to bend, break, or ignore standard operating procedures or rules to benefit the payer
- Tendency of an employee to insert himself into areas in which he is normally not involved
- Propensity to assert authority or make decisions in areas for which the employee is not responsible
- Inclination to make excuses for deficiencies in a third party's products or services, such as poor quality, late deliveries, or high prices
- Circumstances that generate extreme personal pressures, such as ill family members or drug addiction

- History of not filing conflict of interest forms
- Frequent hospitality and travel expenses for foreign public officials
- Friendly social relationship with a third-party contractor
- Wheeler-dealer attitude

Red Flags of Corrupt Third Parties

Some common red flags of a corrupt third party include a party who:

- Routinely offers inappropriate gifts, provides lavish business entertainment, or otherwise tries to ingratiate himself into an organization
- Consistently receives contracts without any apparent competitive advantage
- Provides poor-quality products or services but is continually awarded contracts
- Charges unjustified high prices or price increases for common goods or services
- Receives or pays fees in cash
- Receives or pays fees in a country different from where the underlying business takes place
- Offers no apparent value to the organization
- Charges high commissions
- Claims to have special influence with a specific buyer
- Displays any of the following indicators suggesting lack of qualification:
  - Inadequate financial resources
  - Operating in a region with a history of corruption
  - Decentralized operations
  - Lack of qualifications or experience
  - Poor performance record
  - Reputation for dishonesty
  - Past complaints or criminal or civil actions against the third party
  - A history of fraudulent conduct
  - Undisclosed interests in a company or business owned by an employee
  - Family ties with an employee
- Does not relate well to competitors
- Has an address or telephone number that matches an employee's address, the address of an employee's outside business, or an employee's relative's address
- Provides an incomplete address (e.g., a PO Box, no telephone number, or no street address)
- Provides multiple addresses

- Has a reputation for corruption or works in an industry or country with a reputation for corruption
- Works as an independent sales representative, consultant, or other middleman who does not have the reporting and internal control requirements of his larger, publicly held competitors

Internal Control Red Flags of Corruption

Common red flags of corruption that occur in an organization's internal controls include:

- Poor internal controls over key areas, such as purchasing, inventory receiving, and warehousing
- Poor recordkeeping
- Poorly defined roles and responsibilities
- Insufficient capacity to monitor high-risk employees or units
- Inadequate anti-corruption control plan
- Poor separation of duties in purchasing
- Lack of transparency in expenses and accounting records
- Poor enforcement of existing policies on conflicts of interest or acceptance of gratuities
- Poor documentation supporting award of contracts or subcontracts
- Inadequate monitoring procedures

Methods of Proving Corrupt Payments

There are three basic ways to prove corrupt payments. First, the fraud examiner may seek to prove illicit funds by turning an inside witness. This approach—assuming the testimony can be corroborated—has obvious advantages and should be pursued whenever feasible.

Second, the fraud examiner may engage in a covert "sting" operation to secretly infiltrate or record ongoing transactions. A covert "sting" operation might be effective if the scheme is ongoing and the subject is not aware of the investigation. But there are legal and security issues associated with this approach, which requires considerable experience.

Third, the fraud examiner may identify and trace the corrupt payments through audit steps. The remainder of this discussion focuses on proving corrupt payments through audit steps.

When identifying and tracing corrupt payments through audit steps, the fraud examiner might focus on the *point of suspected payment* (i.e., from where the funds are generated, earned,

stolen, or otherwise begin their journey), *point of receipt* (i.e., from where the illicit funds are deposited, spent, or invested), or both.

In general, there are two methods used to conceal corrupt payments in a business: on-book schemes and off-book schemes. *On-book schemes* are those that occur within an organization; therefore, these schemes will appear within that entity's financial records. In on-book schemes, illicit funds are drawn from the payer's regular, known bank accounts and recorded on its books and records in a disguised manner as some sort of legitimate trade payable. Usually, such transactions will be disguised as some type of legitimate expense, fee, commission, or payment to a subcontractor. Thus, the records provide a starting point for tracing unknown assets, and once the on-book payments are identified, the fraud examiner can begin tracing them to their destination. But to do this, the fraud examiner must scrutinize the payer's expenditures to determine which ones are used to hide corrupt payments.

Once the fraud examiner has a starting point, he must pick up the paper trail and follow it from there.

Off-book schemes refer to those in which the suspect transactions do not appear anywhere on the payer's books or records. That is, off-book schemes leave no direct audit trail. Therefore, off-book schemes are more difficult to trace than on-book schemes. Even though off-book schemes do not leave a paper trail, business and financial records might contain indirect evidence of off-book sales or income (e.g., unaccounted-for shipping or warehouse expenses, or discrepancies in particular accounts or ratios between certain accounts).

As a general proposition, suspected on-book schemes are best approached from the point of payment, and off-book schemes are most easily identified at the suspected point of receipt, through the use of an inside witness, or through surveillance. Accordingly, a fraud examiner may seek to prove corrupt payments by focusing on the point of receipt, the point of payment, or both.

The point of payment method seeks to prove corrupt payments by focusing on the accounts and records where the funds are generated, earned, stolen, or otherwise begin their journey. And because on-book schemes leave an audit trail, the point of payment method, which focuses on where the funds are stolen, is the preferred method.

Conversely, the point of receipt method focuses on where the illicit funds are deposited, spent, or invested. This method is preferred if the suspected payer is not known or is inaccessible, or if cash payments are suspected. Accordingly, the point of receipt method is preferred when investigating off-book frauds because they do not leave an audit trail. And because there is no audit trail, the fraud examiner must focus on the records about where the illicit funds are deposited, spent, or invested.

When conducting an investigation that involves corrupt payments moving through business accounts, the fraud examiner should develop business profiles of the involved entities. Not only will creating business profiles help the fraud examiner gain an understanding of the involved entities and their industries, but it will help him identify any unusual and noncustomary occurrences that are present in those organizations. Moreover, profiling helps organize and view the information retrieved and assists with the investigation.

The Business Profile—Analysis

The *business profile* begins the examination process. It will contain all the important information about a subject organization, such as its money flow pattern and financial condition, and it will identify prospective witnesses and targets, as well as relevant documents and transactions. It should also provide leads as to whether an on-book or off-book scheme is being used.

To develop the business profile, the fraud examiner should obtain information about the suspect business's organization, personnel, money flow pattern (e.g., source of available funds, related expenditures, etc.), bank account location, financial condition, and recordkeeping system. This information can be obtained through interviews of employees, customers, and competitors; business bank account and loan records; financial statements; tax returns; business reporting companies; and business public filings.

To establish a business profile, fraud examiners should seek to answer the questions listed below.

HOW IS THE BUSINESS ORGANIZED, LEGALLY AND STRUCTURALLY?

Determine how the business is legally and structurally organized because this knowledge will help determine what records are available (e.g., corporate, partnership, etc.) and where to go to obtain them.

WHO ARE THE KEY PERSONNEL ASSOCIATED WITH THE ENTERPRISE?

Identify the key personnel associated with the subject business because doing so will help to identify potential witnesses and informants, as well as possible subjects. Key positions include the owners of the business; the people directly involved in the suspect transactions, including secretarial and clerical staff and present and former employees; the "number crunchers"; the bookkeeper, outside accountants, and tax preparers; outside consultants, sales representatives, and independent contractors (a popular conduit for payoffs); and competitors (often eager witnesses who can identify leads to sources of off-book funds such as customers and rebate practices).

WHAT IS THE MONEY FLOW PATTERN INVOLVED IN THE SUSPECT TRANSACTION?

Identify the money flow patterns—where money comes from and where it goes—of the suspected transactions. Information about the source of funds can provide leads as to whether an on-book or off-book scheme is being employed and the location of off-book accounts. Expenditures related to the suspect transactions might cover on-book payments.

Use the following questions to determine all sources of funds:

- What goods or services does the business provide?
- Who are its customers or clients?
- What mode of payment is used: cash or check?
- What other sources of funds are available, such as rebates from suppliers and shippers or proceeds of insurance claims, liquidation sales, sale of assets, and loans?

Use the following questions to identify all expenditures associated with the suspect transactions:

- What disbursements are made to third parties, such as commissioned sales agents, consultants, subcontractors, suppliers, and shippers?
- Did the business have any extraordinary expenses during the suspect time period, such as extra commissions, advertising allowances (payments made by a manufacturer to the retail customer to assist the customer in meeting its advertising expenses), or inventory losses?
- How are the expenses and disbursements paid: by cash or by check? From which accounts?

- Does the business maintain an account or fund used to pay miscellaneous expenses? If so, where is it located, who keeps the records, and who signs the checks or authorizes payments?
- How are travel and entertainment expenses reimbursed? From which account?
- What is the company's policy toward business gifts? What gifts were given to the suspect and/or recipients? How were they paid for? Which records are maintained regarding them?

WHERE ARE THE COMPANY'S BANK ACCOUNTS?

Identify all of the business's bank accounts. Find out where the business deposits its receipts. This is quickly determined from the bank stamp on checks deposited from customers. Identify all company accounts by bank, account number, and authorized signature.

WHAT IS THE FINANCIAL CONDITION OF THE BUSINESS?

Determine the entity's financial condition. This data might provide evidence of a motive for the fraud or the fruits thereof.

WHAT IS THE COMPANY'S RECORDKEEPING SYSTEM?

Become familiar with the business's recordkeeping system, determining what records the company keeps, for how long, where, and the name(s) of the person(s) who maintains them.

Sources of Information for the Business Profile

Information for the business profile can be obtained through the sources listed below.

PRINCIPALS, EMPLOYEES, AND RECORDS OF SUSPECT BUSINESS

Interview people suspected of making illegal payments. Such individuals might submit to an interview, particularly if they are confident that the payments are well hidden.

Also, interview other key employees (including the financial personnel) involved in the suspect transactions, particularly those who have since left the company. Use the business profile as a guide to questioning.

CUSTOMERS AND COMPETITORS

The "customer" is the employer of the person taking payoffs and the victim of the crime. Customers and competitors can provide valuable information about the payer's business operation, particularly concerning the payer's regular bank account, which can be identified

through canceled checks. The customer might also have invoices and shipping documents that might lead to off-book funds.

BANKS AND LENDING INSTITUTIONS

The business's banker might have credit applications, financial statements, loan files, and bank account information that might help the fraud examiner.

BUSINESS REPORTING COMPANIES

Dun & Bradstreet and other commercial reporting companies disseminate basic information about the size, structure, sales, and employees of a business, and such companies can provide valuable information. Information about larger companies can be found in Standard & Poor's and other business directories. Other information on public record sources is located in the "Sources of Information" chapter in the Investigation section of the *Fraud Examiners Manual*.

Proving On-Book Payments

There are three basic methods for concealing on-book payments of bribes and/or kickbacks: fictitious payables, ghost employees, and overbilling. The following are the examination steps for identifying and tracing these payments.

Fictitious Payables Schemes

In a fictitious payable scheme, a payable is created for a debt that is not owed. Often, fictitious payables are made to entities or persons that do not exist, such as fictitious vendors. Making payments to entities or individuals that do not exist provides an excellent method for hiding corrupt payments.

To examine on-book payments, obtain the following records from the entity suspected of making the illegal payments.

BANK ACCOUNT INFORMATION

- All records of payments, canceled checks, wire transfer receipts, receipts for the purchase of cashier's checks and money orders, and withdrawal slips
- Check registers
- Account statements

SALES BACKUP DOCUMENTATION

- Purchase orders
- Invoices
- Documents showing receipt of goods ordered

ACCOUNTING BOOKS AND RECORDS

Examine the cash disbursement journals and ledgers. The most important of the aforementioned information (and often the only information needed) is the bank account information. Begin by examining the checks, check register, and/or the cash disbursement journal, paying particular attention to the following:

- *Payables and expenses charged to the account (customer) on which the illicit payments were made*—If the fraud examiner suspects that kickbacks were paid on sales to ABC Corporation, for example, look at the payables and expenses charged to that account/customer.
- *Payments for services*—Check payments for services such as sales commissions or consulting fees that do not require the delivery of goods and need relatively little documentation to obtain payment.
- *Anomalous charges*—For the business, an example of anomalous payments can be those for design fees paid by a company that is engaged in business that normally would not require such services.
- *The endorsement on the check*—This might be by signature, or more commonly, by a stamp in the name of the business payee. Note the endorser's identity. (Some corrupt recipients have been known to endorse such checks in their own name.)
- *The location where the check was negotiated*—If it is not obvious from the endorsement, identify the bank where the deposit was made by checking the depository bank's stamp on the back of the check. The geographical location of the depository bank is an important lead that can connect the check to the suspected recipient. Determining the depository bank's identity is critical to obtaining the recipient's bank account information.
- *Checks with a second endorsement*—A typical indication of a phony payable check is one paid to and endorsed by a business, which is then endorsed by an individual, thereby permitting it to be cashed or deposited in a personal account. In a similar fashion, a check payable to a third party can be signed over to the issuer of the check.
- *Cashed (not deposited) checks payable to a business*—Generally, a "For Deposit Only" stamp appears on the back of deposited checks, although this is not always the case. Most banks have a code stamp that indicates whether the check was cashed. These codes vary and can be obtained from the bank where the check was negotiated.

- *Checks that fall into an unexplained pattern*—An example of a suspicious payable scheme is one where checks are drawn once a month in an amount equal to some percentage of the sales against which they are charged and are not otherwise explained. Such a pattern might indicate a kickback scheme.

If an examination of the checks themselves does not yield any clear leads, compare the various records of payment with the backup documentation. Note the following circumstances in particular:

- *The absence of documentation*—The absence of documentation to support a particular payment can include:
  - No invoice appearing in the files for a payment to a supplier or contractor
  - No receipt to indicate that materials paid for were delivered
  - No consultant's work product to substantiate consulting fees paid
- *Discrepancies*—Discrepancies between payment information and backup documentation can include:
  - A check payable to a supplier in an amount different from his invoice
  - A check payable to a person or entity different from that identified on the invoice
- *Anomalies in support documents*—Anomalies in the backup documentation can include invoices from several suppliers in different names that:
  - Have the same business address
  - Are signed by the same person
  - Are returned to a post office box
- *Unnumbered or sequentially numbered invoices*—An example of an invoice scam uses invoices numbered 101, 102, and 103, which are dated 30 days apart. Of course, it is highly unlikely that a legitimate business would refrain from issuing invoices in the interim.
- *Alterations*—Copies of originals can be made for concealing alterations of original documents. Examples can include alterations or photocopies of backup papers.
- *Location and other information on the invoices that tie them to the suspected recipient*—If the aforementioned steps still do not yield any suspect payments, return to the check registers and cash disbursement journals to look for discrepancies between the entries and the checks or backup documentation or their absence. The register and journals might also indicate the purpose of payments made by wire, cashier's check, or cash.

TRACING PROCEDURES

When a suspect payment has been isolated, begin the tracing process. Remember that the phony payable might go directly to the recipient (deposited in a shell account) or through an

intermediary account, person, or entity. It might even be converted to cash by the payer and the cash could be given to the recipient.

In instances where the identity of the individual recipient is not clear from the face of the check (as in checks payable to a business entity), do the following:

- Examine the back of the check. Note where the check was deposited and the account number, if available. If the check is not endorsed, the bank will still be able to locate the account to which it was deposited through its own internal records.
- Obtain the records of the account where the check was deposited. The signature card and the monthly account statement will show the nominal account holder. In the case of business accounts, the bank should also have a copy of the corporate resolution or partnership agreement authorizing the account.
- If the identity of the individual recipient is still not clear, check the public filings required of business entities to determine ownership. Corporate documents (articles of incorporation, annual reports, and some other basic documents) and limited partnerships might also be filed in some jurisdictions at the local level. The fictitious name index, business license files, telephone billing records, and even utility billing records can also lead to the principals' identity.
- If the original check is missing or has been destroyed, a digital copy can be obtained from the bank on which the check was drawn. (The bank where the check was deposited will also have a digital copy of the check. Unless the exact date of deposit and the identity of the depository bank are known, it will be very difficult to locate it.)
- Payments by wire transfer or cashier's check can be traced to the recipient. A wire transfer from an account appears on that account statement as a *debit memo* (often abbreviated as *DM*). The *wire transfer request* should show the name of the purchaser, the payee, and the bank and account number to which the funds were transferred. The sender receives a copy of this request, and the bank also maintains a copy, which is usually filed by date.
- The bank's retained copy of a cashier's check will identify the payee. The bank also keeps the negotiated check when it is returned for payment. It will contain the endorsement and show where it was negotiated. Banks usually file cashier's checks by number, making it necessary to know the approximate date they were issued to link them to the purchasers. Look for a cashier's check or wire transfer on the dates of suspect cash withdrawals, checks to cash, or checks to the issuing bank. Remember that such

instruments can be purchased for cash from any bank, not only from the bank where the payer's account is located.
- If this trail leads to an intermediary, the entire process must be repeated.

Ghost Employee Schemes

Illicit funds can be generated by funneling phony salary payments to fictitious or former employees (i.e., ghost employees), or by making extra payments to presently salaried employees who then either return them to the payer or pass them on to the recipient. To trace such payments, obtain payroll and employee lists, personnel files, employment applications, tax withholding forms, and payroll checks from the suspect payer company.

Attempt to identify the ghost through the following steps:
- Compare a list of all current and former employees from the personnel office to the payroll list. Note discrepancies. Determine whether any employees have failed to execute tax withholding forms or have not elected to receive any health benefits or other optional withdrawals, such as enforced savings plans. The absence of such elections is often an indication that the employee does not exist.
- A regular employee's normal salary might also be inflated or, more commonly, travel and expense reimbursements might be padded to generate illicit funds. Look for unusual disbursements from the accounts in which such checks are deposited.

Once a suspect paycheck has been identified, determine whether the check was cashed or deposited. Note the endorsement, the bank, and the account where the check was deposited. Determine whether there are any second endorsements that might transfer the check to the ultimate recipient.

Overbilling Schemes

In overbilling schemes, the payer adds a corrupt payment to a legitimate business expense or trade payable. And subsequently, a cooperative third party then either forwards the excess payment directly to the intended recipient or returns it, usually in cash, to the payer for distribution.

Thus, illicit funds might be added to legitimate payments for goods or services provided by actual suppliers, subcontractors, engineers, and agents, with the additional amounts being passed on by the supplier or returned to the payer (usually in cash) for distribution.

To trace such payments, obtain the same records required for tracing phony payables—bank account information, backup documentation, and accounting records—from both the original payer and the intermediary. Note the following indicators of suspect payments to the intermediary:

- Notations on invoices or other billing documents breaking out "extra" or "special" charges, particularly those that require no delivery of goods for payment
- Discrepancies between the purchase order or invoice amounts and the amount of payment; note invoices that appear to have been altered or copied
- Unusually large amounts appearing on particular bills, or bills that break a consistent pattern of amounts, schedule, or purpose

Disbursements from the intermediary might be covered in the same ways as in other on-book schemes, such as by means of phony payables, direct cash withdrawals, or disbursements charged to miscellaneous accounts such as travel or entertainment. The tracing process is the same as in any on-book scheme. Remember that the overbilling entity will usually add its own fee for providing such services. Therefore, the disbursements coming from its account might not be in the same amount as the additional payments made to it.

Proving Off-Book Payments

Again, off-book payments refer to those schemes in which the funds used for illegal payments or transfers are not drawn from the regular, known bank accounts of the payer. Thus, off-book payments do not appear anywhere on the payer's books or records.

In contrast to on-book payments, which are proven at the point of payment, off-book payments are typically proven at the point of receipt; that is, they are proven at the point from where the illicit funds are deposited, spent, or invested.

Accordingly, identifying and tracing off-book payments is usually more difficult than locating on-book payments. Success in proving off-book payments generally depends upon identifying the source of the funds or accounts (from which payments can be traced out), using an inside witness, and focusing on the point of receipt. The source of off-book funds might be located through the following indicators.

Indirect Evidence of Unrecorded Sales on the Suspect Company's Books and Records

The suspect company's books and records might reflect unusual costs and expenses not associated with the business's known sales, such as rental payments for an undisclosed warehouse, shipping documents reflecting deliveries to an unlisted customer, and commissions paid to sales agents in a region where sales are not reported. These indicate possible unrecorded sales.

Unbalanced Ratios of Costs to Sales

The cost of producing and selling a particular item usually bears some fixed relationship to the revenue it generates. A significant imbalance in such a ratio, such as in a situation where twice the supplies are ordered than are needed to produce the reported sales (and the extra is not located in inventory), indicates possible unrecorded transactions. This technique is used to identify unreported sales by bars and restaurants.

Investigation in the Marketplace

Customers of the suspect business whose payments might have been diverted to off-book accounts might have records, including canceled checks, that would reflect such sales and the bank and account to which the funds were deposited. Customers might also reveal cash payments that could be used to create a slush fund. Additionally, competitors might be aware of other customers and transactions that could lead to evidence of off-book sales.

Proving Payments in Cash

The following techniques can be used to prove cash payments circumstantially or to corroborate testimony of such payments by an inside witness:

- Match evidence of cash withdrawals or disbursements by the payer with corresponding deposits, expenditures, or visits to a safe deposit box by the recipient.
- Look for the purchase of cashier's checks or wire transfers payable to the recipient at, or shortly after, cash withdrawals or disbursements. Also look for a correlation between cash-generating transactions and money wires or courier services, which are sometimes used to send cash.
- If the scheme is ongoing, consider the use of visual or electronic surveillance (if a member of law enforcement), or try to introduce an undercover agent or implement a sting operation.
- Unexplained or unusual cash disbursements or withdrawals, particularly from a business that does not normally deal in cash, might indicate illicit transactions or corroborate such

testimony. To be effective, the fraud examiner must identify and rebut all legitimate explanations, which usually requires interviewing the payer.
- Focus the investigation on the suspected recipient, as discussed in the following sections.

Examining Off-Book Payments by Focusing on the Point of Receipt

Because the point of receipt focuses on where the illicit funds are deposited, spent, or invested, this method is preferred if the suspected payer is not known or is inaccessible, or if cash payments are suspected. Accordingly, the point of receipt method is preferred when investigating off-book payments because they do not leave an audit trail. And because there is no audit trail, the fraud examiner must focus on the records regarding where the illicit funds are deposited, spent, or invested.

Alternatively, off-book payments may be proven through the use of an inside witness or surveillance. Therefore, if there is no witness and the fraud examiner cannot conduct surveillance, he must prove the illicit transactions by using the point of receipt method.

The personal—financial/behavioral—profile is used when trying to prove illegal payments from the point of receipt.

THE FINANCIAL/BEHAVIORAL PROFILE

The financial/behavioral profile is outlined in the "Tracing Illicit Transactions" chapter in the Investigation section of the *Fraud Examiners Manual*. The financial profile will identify most illicit funds deposited to accounts or expended in significant amounts. It will not reveal relatively small currency transactions, particularly if they were for concealed activities, consumables, or unusual one-time expenses, such as medical bills. The financial profile might give inaccurate or false negative readings unless such activities are identified. This is done through preparation of the behavioral profile.

The behavioral profile contains information about the suspect's personal characteristics (e.g., carries large amounts of cash, wears expensive clothes, or has club memberships), home and furnishings, automobiles, and leisure activities.

Information for the behavioral profile is gathered from interviews and observation of lifestyle and habits, as well as from documentary sources. When conducting interviews, the fraud examiner should be alert and review documents for signs that the target has:

- A drug and/or alcohol addiction
- A gambling habit
- Loan shark or other private debts
- A girlfriend (or boyfriend) supported by the target
- Extraordinary medical expenses
- Significant, regular cash expenses for entertainment and/or travel

The behavioral profile might also provide evidence of a possible motive for the crime, such as large debts, as well as additional evidence of illicit funds. For example, if the suspect spent significant amounts of cash and had no corresponding cash withdrawals from disclosed bank accounts or no admitted sources of cash income, there must be other, undisclosed sources of income.

Generally, when trying to prove illegal payments from the point of receipt, the fraud examiner should interview the suspect recipient and any third-party witnesses.

THE SUSPECT RECIPIENT

Again, when trying to prove corrupt payments from the point of receipt, the fraud examiner should almost always request an interview with the target. When interviewing the target, the fraud examiner should use the target's financial/behavioral profile as a guide. The fraud examiner should try to pin down the target's income, assets, and accounts. If, during the interview with the suspect recipient, the witness claims to have legitimate sources of large sums of currency, the fraud examiner should determine the following:

- What was the source of the cash?
- What was the amount of cash on hand at the starting point of the investigation, at the end of each year thereafter, and on the date of the interview?
- Where was the cash kept?
- Why was the cash not deposited in a financial institution or invested?
- Who knew about the cash?
- What records of the cash exist?
- What were the denominations?
- When and for what was any of the cash spent?
- Will the subject consent to an inventory of the remaining cash during the interview? If not, why not? If so, the cash should be counted at least twice in the presence of another fraud examiner. A list of serial and series numbers should also be made.

If, when interviewing the target, the target claims that the suspect funds were proceeds from a legitimate loan, the fraud examiner should ask:

- Who was the lender?
- When was the loan made?
- What was the amount of the loan?
- What was the purpose of the loan?
- Was the loan repaid?
- How was the loan documented?

Also, the fraud examiner should attempt to interview the subject's spouse separately. Spouses can be an important source of lead information—if handled carefully.

THIRD-PARTY WITNESSES

When trying to prove illegal payments from the point of receipt, the fraud examiner should also interview any third-party witnesses. Potential third-party sources include business colleagues, personal associates, bankers, brokers, real estate agents, accountants and tax preparers, ex-spouses, and romantic interests (particularly former romantic interests). Subjects often boast to their close associates of their new wealth or entertain them with the fruits thereof. Casual remarks by a subject to a colleague (and repeated to a fraud examiner) have undone the suspect, even when intensive audits have failed. Follow the financial/behavioral profile format to the extent feasible. Of course, no single third-party witness is likely to possess all this information, but a complete picture can be assembled from bits and pieces provided by a number of such sources.

TRACING CORRUPT PAYMENTS

Other techniques for tracing corrupt payments can be found in the "Tracing Illicit Transactions" chapter in the Investigation section of the *Fraud Examiners Manual.*

Conflicts of Interest

A *conflict of interest* occurs when an employee or *agent*—someone who is authorized to act on behalf of a principal—has an undisclosed personal or economic interest in a matter that could influence his professional role. These schemes involve self-dealing by an employee or agent and can occur in various ways. For example, a conflict might occur when an employee accepts inappropriate gifts, favors, or kickbacks from vendors, or when an employee engages in unapproved employment discussions with current or prospective contractors or suppliers.

Conflict of interest schemes generally constitute violations of the legal principle that an agent or employee must act in good faith, with full disclosure, and in the best interest of the principal or employer. An *agent* is any person who, under the law, owes a duty of loyalty to a principal or employer. Agents include officers, directors, and employees of a corporation; public officials; trustees; brokers; independent contractors; attorneys; and accountants. A *principal* is an entity that authorizes an agent to act on its behalf. In a principal-agent relationship, the agent acts on behalf of the principal. The agent should not have a conflict of interest in carrying out the act on the principal's behalf.

As with other corruption frauds, conflict schemes involve the exertion of an employee's influence to his principal's detriment. In contrast to bribery schemes, where fraudsters are paid to exercise their influence on behalf of a third party, conflict of interest cases involve self-dealings by employees or agents.

If an employee engages in a transaction that involves a conflict of interest, then the employee might also have breached his *fiduciary duty* to his employer. People in a position of trust or fiduciary relationship—such as officers, directors, high-level employees of a corporation or business, and agents and brokers—owe certain duties imposed by law to their principals or employers, and any action that runs afoul of such fiduciary duties constitutes a breach.

There are two principal fiduciary duties—loyalty and care—but this discussion focuses on the duty of loyalty. An agent (employee) owes a duty of loyalty to his principal. The *duty of loyalty* requires that the employee or agent act solely in the best interest of the employer or principal, free of any self-dealing, conflicts of interest, or other abuse of the principal for personal advantage. Thus, an agent cannot seek to advance personal interest to the principal's detriment.

Breach of fiduciary duty is a civil action that can be used to redress a wide variety of conduct that might also constitute fraud, commercial bribery, and conflicts of interest. Establishing a breach of fiduciary duty claim is easier than establishing a claim for fraud because a breach of fiduciary duty claim does not require proof of wrongful intent.

A plaintiff who brings a successful breach of fiduciary duty claim may receive damages for lost profits and recover profits that the disloyal employee or agent earned—in some instances even the salary paid to the employee or agent during the period of disloyalty. The

plaintiff may recover profits earned by the disloyal agent even if the principal did not suffer an actual loss. The plaintiff also may void contracts entered into on its behalf that were the result of or were influenced by the employee or agent's disloyalty.

Most conflicts of interest occur because the fraudster has an undisclosed economic interest in a transaction, but a conflict can exist when the fraudster's hidden interest is not economic. In some scenarios, an employee acts in a manner detrimental to his company to provide a benefit to a friend or relative, even though the fraudster himself receives no financial benefit.

Conflicts of interest do not necessarily constitute legal violations, as long as they are properly disclosed. Thus, to be classified as a conflict of interest scheme, the employee's interest in the transaction must be undisclosed. The crux of a conflict case is that the fraudster takes advantage of his employer; the victim organization is unaware that its employee has divided loyalties. If an employer knows of the employee's interest in a business deal or negotiation, there can be no conflict of interest, no matter how favorable the arrangement is for the employee.

Any bribery scheme discussed above could occur as a conflict of interest. The only difference in bribery schemes and conflict of interest schemes is the fraudster's motive. For instance, if an employee approves payment on a fraudulent invoice submitted by a vendor in return for a kickback, he has committed bribery. But if an employee approves payment on invoices submitted by his own company (and if his ownership is undisclosed), he has engaged in a conflict of interest.

The distinction between bribery and conflict schemes described above is obvious. In the bribery case, the fraudster approves the invoice in return for a kickback, while in a conflict case he approves the invoice because of his own hidden interest in the vendor. Aside from the employee's motive for committing the crime, the mechanics of the two transactions are practically identical. The same duality can be found in procurement fraud cases, where an employee influences the selection of a company in which he has a hidden interest instead of influencing the selection of a vendor who has bribed him.

Conflict Schemes

Conflict schemes do not always mirror bribery schemes, though. There are a number of ways in which an employee can use his influence to benefit a company in which he has a

hidden interest. This section will discuss some of the more common conflict schemes, including conflicts in:

- Purchase schemes
- Sales schemes
- Delayed billings
- Business diversions
- Resource diversions
- Financial interest in companies under perpetrator's supervision
- Financial disclosures

Conflicts in Purchasing Schemes

Many times, conflicts of interest arise in the purchasing process. For example, an employee can have a conflict if he:

- Has an undisclosed financial interest in a supplier or contractor
- Sets up a bogus contractor or vendor, or buys through a broker or middleman that the employee controls
- Is involved in other business ventures with a supplier or contractor
- Has an interest in a business that competes with his employer
- Accepts inappropriate gifts, travel, entertainment, or "fees" (kickbacks) from a vendor
- Negotiates for or accepts employment with a supplier

Often, such purchasing schemes are very similar to the billing schemes discussed in the "Asset Misappropriation: Fraudulent Disbursements" chapter, so it will be helpful at this point to discuss the distinction drawn between traditional billing schemes and purchasing schemes that constitute conflicts of interest.

While it is true that anytime an employee assists in the overbilling of his company there is probably some conflict of interest (the employee causes harm to his employer because of a hidden financial interest in the transaction), this does not necessarily mean that every false billing will be categorized as a conflict scheme. For the scheme to be classified as a conflict of interest, the employee (or a friend or relative of the employee) must have some kind of ownership or employment interest in the vendor that submits the invoice.

This distinction is easy to understand if we look at the nature of the fraud. Why does the fraudster overbill his employer? If he engages in the scheme only for the cash, the scheme is a fraudulent disbursement billing scheme. If, however, he seeks to better the financial

condition of his business at the expense of his employer, this is a conflict of interest. In the second scenario, the fraudster's *interests* lie with a company other than his employer. When an employee falsifies the invoices of a third-party vendor to whom he has no relation, this is not a conflict of interest scheme because the employee has no interest in that vendor. The sole purpose of the scheme is to generate a fraudulent disbursement.

One might wonder, then, why shell company schemes are classified as fraudulent disbursements rather than conflicts of interest. After all, the fraudster in a shell company scheme owns the fictitious company and therefore must have an interest in it. Remember, though, that shell companies are created for the sole purpose of defrauding the employer. The company is not so much an entity in the fraudster's mind as it is a tool. In fact, a shell company is usually little more than a PO Box and a bank account. The fraudster has no interest in the shell company that would cause a division of loyalty; he simply uses the shell company to bilk his employer. Shell company schemes are therefore classified as false billing schemes.

A short rule of thumb can be used to distinguish between overbilling schemes that are classified as asset misappropriations and those that are conflicts of interest: If the bill originates from a *real company* in which the fraudster has an economic or personal interest, and if the fraudster's interest in the company is undisclosed to the victim company, then the scheme is a conflict of interest.

Now that we know what kinds of billing schemes are classified as conflicts of interest, the question is, how do these schemes work? The answer, unfortunately, is somewhat anticlimactic. The schemes work the same. A billing scheme's mechanics, whether it is a conflict of interest or a fraudulent disbursement, do not change. (See the "Conflicts of Interest" flowchart that follows.)

A corporate employee or agent who has an undisclosed, potentially adverse interest in a customer or supplier might be tempted to favor his own or the third party's interests over the corporation's interests.

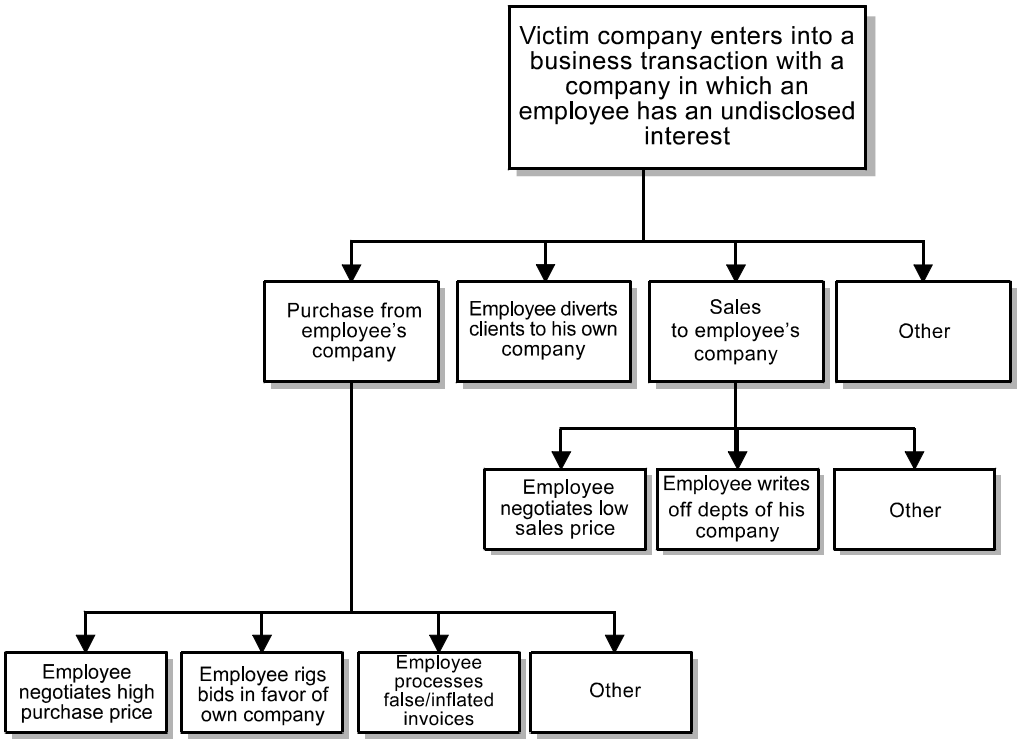
EXAMPLE

A purchasing superintendent defrauded his employer by purchasing items from a certain vendor at inflated prices. The vendor was owned by the purchasing superintendent but established in his wife's name and run by his brother. The perpetrator's interest in the

company was undisclosed. The vendor would buy items on the open market and then inflate the prices and resell the items to the victim company. The purchasing superintendent used his influence to ensure that his employer continued doing business with the vendor and paying the exorbitant prices.

Fraudsters with an interest in a customer or supplier might engage in *bid-manipulation schemes*—purchasing schemes in which an employee of a purchasing entity attempts to influence the selection of a contractor by restricting the pool of competitors from whom bids are sought—on behalf of their own companies. The methods used to manipulate bids are discussed in detail in the "Contract and Procurement Fraud" chapter and will not be explained in depth here. Briefly stated, an employee of the purchasing company is in a perfect position to manipulate bids if he has access to his competitors' bids or helps perform the bidding process. With such access or responsibilities, the employee can influence the bidding process to ensure that his own company wins the contract.

In other cases, a fraudster might ignore his employer's purchasing rotation and direct an inordinate number of purchases or contracts to his own company. Any way in which a fraudster exerts his influence to divert business to a company in which he has a hidden interest is a conflict of interest.



Conflicts of Interest

INTEREST IN THE ACQUISITION OF ASSETS

Not all purchasing conflicts occur in the traditional vendor-buyer relationship. Sometimes purchasing conflicts involve employees negotiating for the purchase of some unique, typically large asset such as land or a building in which the employee had an undisclosed interest. It is in the process of these negotiations that the fraudster violates his duty of loyalty to his employer. Because he stands to profit from the sale of the asset, the employee does not negotiate in good faith to his employer; he does not attempt to get the best price possible. The fraudster will reap a greater financial benefit if the purchase price is high.

For example, an employee in charge of negotiating mineral leases on land that he secretly owns is obviously in a conflict. On the one hand, he is an employee in charge of negotiating the lease, and it is his responsibility to negotiate the best price for his employer. But on the other hand, he owns the land, so it is in his personal interest to lease the land at the highest price possible. And because the employee has a personal interest in the land transaction, he has no financial motive to negotiate a favorable lease on his employer's behalf.

TURNAROUND SALES

A special kind of purchasing scheme sometimes used by fraudsters is called the *turnaround sale*, or the *flip*. In this type of scheme, an employee knows his employer is seeking to purchase a certain asset and takes advantage of the situation by purchasing the asset himself (usually in the name of an accomplice or shell company). The fraudster then turns around and resells the item to his employer at an inflated price.

EXAMPLE

A chief executive officer, conspiring with a former employee, sold an office building to the CEO's company. What made the transaction suspicious was that the building had been purchased by the former employee on the same day that it was resold to the victim company, and for $1.2 million less than the price charged to the CEO's company.

Conflicts in Sales Schemes

There are two principal types of conflict schemes associated with sales of goods or services by the victim company: underselling and writing off sales.

UNDERSELLING

The first and most harmful is the underselling of goods or services. Just as a corrupt employee can cause his employer to *overpay* for goods or services sold by a company in which

he has a hidden interest, so too can he cause the employer to *undersell* to a company in which he maintains a hidden interest.

Also, many employees who have hidden interests in outside companies sell goods or services to these companies at below-market prices. This results in a diminished profit margin or even a loss for the victim organization, depending upon the size of the discount.

EXAMPLE

An employee disposed of his employer's real estate by selling it below fair market value to a company in which he had a hidden interest, causing a loss of approximately $500,000.

WRITING OFF SALES

The other type of sales scheme involves tampering with the victim company's books to decrease or write off the amount owed by the company in which the employee has a hidden interest. For instance, after an employee's company purchases goods or services from the victim organization, credit memos might be issued against the sale, causing it to be written off to contra accounts such as Discounts and Allowances. A large number of reversing entries to sales might be a sign that fraud is occurring in an organization.

EXAMPLE

A plant manager assisted favored clients by delaying billing on their purchases for up to 60 days. When the receivable on these clients' accounts became delinquent, the perpetrator issued credit memos against the sales to delete them. The plant manager issued new invoices on the sales after the "old" receivables were taken off the books. In this way, the receivables could be carried indefinitely on the books without ever becoming past due.

Conflicts Influencing Delayed Billings

In other cases, the perpetrator might not write off the scheme, but simply delay billing. This is sometimes done as a "favor" to a friendly client and is not an outright avoidance of the bill but rather a dilatory tactic. The victim organization eventually gets paid, but loses time value on the payment, which arrives later than it should.

Conflicts in Business Diversions

A number of employees end up starting their own businesses that compete directly with their employers, and when this occurs, such employees might begin siphoning off clients for their own business. This activity clearly violates the employee's duty of loyalty to the

employer, and frequently violates the company's internal policies. There is nothing unscrupulous about free competition, but while a person acts as a representative of his employer, it is improper for him to try to take his employer's clients. Normal standards of business ethics require employees to act in the best interests of their employers.

Conflicts in Resource Diversions

Some employees divert the funds and other resources of their employers to the development of their own businesses. This kind of scheme involves elements of both conflicts of interest and fraudulent disbursements.

EXAMPLE

A vice president of a company authorized large expenditures to develop a unique type of new equipment used by a certain contractor. Another firm subsequently took over the contractor, as well as the new equipment. Shortly after that, the vice president retired and went to work for the firm that had bought out the contractor. The fraudster had managed to use his employer's money to fund a company in which he eventually developed an interest.

While these schemes are clearly corruption schemes, the funds are diverted through the use of a fraudulent disbursement. The money could be drained from the victim organization through a check tampering scheme, a billing scheme, a payroll scheme, or an expense reimbursement scheme. For a discussion of the methods used to generate fraudulent disbursements, please refer to the "Asset Misappropriation: Fraudulent Disbursements" chapter.

Conflicting Financial Interest in Companies Under Perpetrator's Supervision

Sometimes an employee has a direct or indirect financial interest in a company under his supervision. For example, accountants sometimes hold stock in a company they audit. These problems often occur in government.

Conflicts in Financial Disclosures

Management has an obligation to disclose to the shareholders significant fraud committed by officers, executives, and others in positions of trust, but misplaced loyalties might prevent management from making such disclosures.

The inadequate disclosure of conflicts of interest is among the most serious of frauds. Inadequate disclosure of related-party transactions is not limited to any specific industry; it transcends all business types and relationships.

Appearance of Conflict of Interest

A final type of conflict of interest is the *appearance* of such. The appearance of a conflict is nearly as devastating as the existence of a true conflict. Examples involving the appearance of a conflict of interest include ownership in a blind trust, in which the employee has no authority to make investment decisions, or an external auditor owning a minority interest in a company that is audited by the auditor's firm. Such matters are rarely prosecuted as criminal offenses.

Detection of Conflicts of Interest

Conflicts of interest are probably one of the most difficult schemes to uncover. Therefore, there are no fast and easy detection methods for this type of fraud. Some of the more common methods by which conflicts are identified include tips and complaints, comparisons of vendor addresses with employee addresses, review of vendor ownership files, review of exit interviews, comparisons of vendor addresses to addresses of subsequent employers, policies requiring certain employees to provide the names and employers of immediate family members, and interviews with purchasing personnel regarding favorable treatment of one or more vendors.

Review Tips and Complaints

Conflicts are often revealed by tips. If a particular vendor is being favored, then competing vendors may file complaints. Additionally, employee complaints about the service of a favored vendor could lead to the discovery of a conflict of interest. Often, tips include allegations that raise common red flags of conflicts. Such red flags include:

- Unexplained or unusual favoritism of a particular contractor or vendor
- Employee lives beyond his means or displays new wealth
- Employee fails to file conflict of interest or financial disclosure forms or questionnaires
- Employee displays a keen interest in a particular customer, vendor, or supplier
- Employee has discussions about employment with a current or prospective vendor
- Transactions that are not in the best interest of the corporation
- Employee appears to conduct side business
- Vendor address or telephone number matches that of an employee

Compare Vendor Addresses with Employee Addresses

Look for employees posing as vendors by comparing employee and vendor addresses. If nominees or related parties are used as owners of vendors, then the business address of the vendor might match that of the employee. Also, look for PO Box addresses for vendors. This method is similar to that used for locating phony vendors.

Review Vendor Master File

The *vendor master file* is a database that contains a record of all vendors with whom a company conducts business, and it can be used to test for conflict schemes. Review changes to the vendor master file, including new vendors added and address changes. Also, comparing the vendor master file and the employee master file might reveal conflicts of interest. So, match the vendor master file to the employee master file on various key fields, such as address or tax ID number.

Review Exit Interviews and Compare Vendor Addresses to Addresses of Subsequent Employers

If a review of an employee's exit interview yields the name and address of the employee's subsequent employer, compare that employer's name and address with the vendor file to identify any conflicts of interest wherein the employee has obtained employment from a contractor.

Interview Purchasing Personnel Regarding Favorable Treatment of One or More Vendors

Unexplained or unusual favoritism of a particular contractor or vendor is a red flag of a conflict of interest. And because employees are generally the first to observe that a vendor is receiving favorable treatment, purchasing personal should be interviewed for evidence of such favoritism. By asking employees if any vendor is receiving favorable treatment, the fraud examiner might discover conflicts of interest that would otherwise have gone unnoticed.

Also, because evidence that a company accepts inferior products or services from a vendor is a red flag of corruption, purchasing personal should be asked whether any vendor's service (or product) has recently become substandard.

Implement Policies Requiring Certain Employees to Provide the Names and Employers of Immediate Family Members

Where acceptable by law, an organization might require members of management, as well as members of the procurement department, to provide detailed information regarding the names and employers of all immediate family members and household members. With such information, an organization can compare the names and employers of family members to the current position of the employee, and such analysis might lead to information about potential conflicts of interest.

Prevention of Conflicts of Interest

Organizations should take steps to prevent conflicts of interest. They should establish policies clearly defining what constitutes a conflict of interest and prohibiting any such entanglements by officers, directors, employees, or other agents of the organization. A policy requiring employees to complete an annual disclosure statement is an excellent proactive approach to dealing with potential conflicts. Furthermore, such policies will reinforce the idea that engaging in conflicts of interest is unacceptable for employees and will result in severe consequences.

Also, managers must establish an ethical tone for the companies they lead. The tone management sets will have a trickle-down effect on employees of the company. Moreover, organizations must educate their employees about conflicts of interest. In fact, there is no greater tool in the prevention and detection of fraud than a network of employees who are knowledgeable about fraud and look for indicators of their organization's vulnerabilities.

Additionally, organizations should implement monitoring activities to identify red flags of conflicts. For example, comparing the disclosed names and addresses with vendor and customer lists could reveal real conflicts of interest or the appearance of such.

THEFT OF INTELLECTUAL PROPERTY

Today, information is a valuable asset, and organizations must protect their intellectual property. A business's worth is no longer based solely on tangible assets and revenue-making potential; the information it develops, stores, and collects accounts for a large share of a business's value.

To a considerable degree, businesses, administrations, and society as a whole have come to depend on the efficiency and security of information technology, resulting in information acquiring a new and distinct value that cannot be protected in the same way as tangible objects.

Information exists in many forms, and its security is achieved by implementing a process of risk assessment and commensurate controls to ensure the preservation of:

- *Confidentiality*—ensuring that information is accessible only to those authorized to access it and that those parties can only use it for specified purposes
- *Integrity*—safeguarding the accuracy and completeness of information and processing methods
- *Availability*—ensuring that authorized users have access to information and associated assets when required

Intellectual property is a catch-all phrase for knowledge-based assets and capital, but it might help to think of it as intangible proprietary information. Intellectual property can include a business's ideas, designs, and innovations, howsoever expressed or recorded.

This chapter addresses the broad issues relating to the vulnerability and criticality of information and other intangible property. It advocates a mix of procedural, logical, and physical protective measures to combat threats posed by opponents who make it their business to try to obtain an advantage by illegally or unethically abusing another party or entity's intellectual property.

Competitive Intelligence Versus Espionage

While competition in business can generate many positive results, such as increased innovation and reductions in costs for consumers, the high stakes resulting from competitive

business environments also drive organizations to commit corporate espionage as a means to obtain competitive intelligence.

There is often a thin line between competitive intelligence and espionage. *Competitive intelligence* can be defined as the analytical process that transforms disaggregated competitor data into relevant, accurate, and usable knowledge about competitors' positions, performance, capabilities, and intentions. In contrast, *espionage* refers to the use of illegal, clandestine means to gather information; therefore, it does not cover legitimate intelligence collection and analysis using legal means. Espionage, however, can be further subdivided into two categories: traditional and industrial. *Traditional espionage* refers to state-sponsored or sanctioned espionage conducted to collect protected information from a foreign government. *Industrial espionage* (also known as corporate espionage) is the term used to describe the use of illegal, clandestine means to acquire information for commercial purposes.

Competitive intelligence is a legitimate business function that sits comfortably alongside marketing and research and development, as well as general business strategy and the newer discipline of knowledge management. It helps businesses to anticipate competitors' research and development strategies and to determine their operating costs, pricing policies, financial strength, and capacity. Knowledge about competitors is one of the advantages that can help companies to succeed and take the lead in their respective marketplaces.

Competitive intelligence has become a growth industry that is practiced by professionals trained to use information in the public domain or to otherwise use legally available resources to compile information. This information is then collated, processed, and disseminated into intelligence that is usable and has strategic value. Competitive intelligence practitioners mostly work within a code of ethics created by the Society for Competitive Intelligence Professionals (SCIP). Among other things, this strict code requires members to identify themselves during an inquiry and to refrain from using deception in their quest for information.

Common Motivations Driving Corporate Espionage

The following are common motivations for committing corporate espionage:

- Sabotage (e.g., destroying hardware or facilities, entering data incorrectly, "crashing" systems, deleting data, holding data hostage, or altering data)
- Revenge

- Financial gain
- Business advantage
- Knowledge
- Ideological reasons
- Challenge or curiosity
- Ego
- Entrance into (or status within) a social group

Targets of Corporate Espionage

Corporate spies seek any information that is critical to target organizations. Such information includes:

- Intellectual property
- Pricing information and strategies
- Future plans
- Research and development data
- Engineering plans and drawings
- Customer information (e.g., customer lists or customer billing information)
- Patents in progress
- Computer source code
- Bidding systems and data
- Business forms
- Formulas
- Manufacturing plans and strategies
- Testing data
- Trade secret status
- Customer survey results
- Prototypes
- Research data
- Blueprints and diagrams
- Confidential documents
- Software
- Technical records
- Marketing plans
- Sales forecasts
- Executive email and voice mail

- Personnel records
- Confidential financial data

Where Intelligence Professionals Get Information

Intelligence professionals employ a variety of techniques to obtain valuable information. This discussion examines some basic sources of competitive intelligence, including:

- Open-source information
- Scavenging and dumpster diving
- Surveillance
- Human intelligence
- Government sources
- Industry reports and studies
- Periodicals
- Online sources
- Data analysis
- Job postings
- Environmental impact statements
- Commercial filings (e.g., UCC filings)

Open-Source Information

Open-source information is information in the public domain; it is publicly available data that anyone can lawfully obtain by request, purchase, or observation. Open-source information can include:

- Mass media communications (e.g., newspapers, magazines, radio, television, and the Internet)
- Computer-based information
- Public information that a governmental body must maintain and make accessible to the public
- Information derived from professional and academic sources
- Commercial data
- Information produced by the private sector, government, and academia

The term *open*, however, does not necessarily mean free. Many resources that provide access to open sources of information charge for access.

For further clarification, consider how open-source information differs from nonpublic information. The dividing line between open-source information and other, nonpublic information (such as trade secrets) is the right to access it. Open-source information is available to anyone who wants to collect it, without legal consequences. Nonpublic information, however, is not open to the public. Access to nonpublic records is restricted. Obtaining nonpublic records without appropriate authority violates the law.

According to intelligence professionals, most of the information sought on any topic is open and publicly available.

There is only so much that security professionals can do to limit the availability of open-source information relating to an organization. Some forms of information, such as financial statements of publicly traded companies, are legally required to be published. Other pieces of information, such as product descriptions or job listings, are posted out of business necessity. Corporate security professionals do not operate in a vacuum; the need to protect an organization's secrets must always be balanced against the need or duty to make the information available to the public.

Intelligence professionals can use open-source information for various means, including:

- Obtaining as much information as possible about the target
- Gathering information needed to plan and carry out an attack
- Locating targets
- Finding legal records about targets
- Obtaining financial or credit information about targets
- Obtaining personal information about targets (e.g., names, ages, positions, contact information, hobbies, telephone listings, interests, addresses, banks, or friends)
- Identifying a target's marital status
- Uncovering a target's litigation history
- Locating a target's assets
- Conducting background research on targets

Scavenging and Dumpster Diving

Intelligence professionals might scavenge or dumpster dive for sensitive information (e.g., credit card receipts, bank statements, or discarded media drives). *Scavenging* involves collecting information left around computer systems (e.g., on desks or workstations). *Dumpster diving* refers to gleaning sensitive information from trash receptacles and dumpsters.

Surveillance

Intelligence professionals can conduct *surveillance*—the planned observation of people, places, or objects—to obtain information about targets.

Intelligence gatherers can engage in physical or technical surveillance.

Physical Surveillance

Physical surveillance is the real-time observation of a target's actions or communications. Observing and recording a target's movements is useful for a number of reasons. Such surveillance can be used to identify real property or other assets; additional targets; individuals who might possess valuable information, such as lawyers, accountants, or bankers; businesses; patterns of conduct; and other forms of information that can be exploited for commercial purposes.

There are two general types of physical surveillance: mobile and fixed.

MOBILE SURVEILLANCE

Mobile surveillance involves observing and following persons. When conducting mobile surveillance, an intelligence professional must be flexible and imaginative. For example, placing a reflective stripe on the back of the subject's car makes it more distinctive at night and therefore easier to follow. If legally permissible, an intelligence professional might place a GPS tracking device on the subject's car so that its path can be traced 24 hours a day. Also, if an intelligence professional follows a subject into a bar or restaurant, the professional should order food or a drink so that he can blend in.

FIXED SURVEILLANCE

Fixed surveillance is a situation in which an individual secretly observes an area or a person from a distance. This method, however, has a key disadvantage: the base from which the surveillance is conducted might be spotted by the target or other people passing by. Therefore, intelligence professionals must camouflage fixed surveillance campaigns, and to do so, they must be familiar with their surroundings and choose a cover that will not draw attention.

Technical Surveillance

Technical surveillance is the practice of covertly acquiring audio, visual, or other types of data from targets through the use of technical devices, procedures, and techniques. Technical

surveillance, however, can be costly; it is labor intensive, highly intrusive, and fraught with legal pitfalls.

For more information on surveillance, see the discussions on physical and technical surveillance in the "How Information Is Lost or Stolen" section of this chapter.

Human Intelligence

Intelligence professionals might gather data through human intelligence (i.e., through direct contact with people). Generally, human intelligence is gathered from subject matter experts and informed individuals. Such efforts typically target individuals who can provide the most valuable information. For example, to gain intelligence about a target organization, an intelligence professional might contact the organization's:

- Employees
- Competitors
- Vendors, suppliers, and retailers
- Consultants
- Retired executives
- Former employees

Additionally, an intelligence professional might seek to gain intelligence by contacting:

- Industry experts
- Industry associations
- Reporters who cover the industry

There are various other approaches available for gathering human intelligence. For example, an intelligence professional might gather intelligence by posing as a customer of the target entity. This approach exploits two weaknesses of corporate culture: (1) all salespeople want to make a sale and (2) many salespeople will do almost anything to make a sale. Other approaches include:

- Employment interviews (real and fake)
- False licensing negotiations
- False acquisition or merger negotiations
- Hiring an employee away from a target entity
- Planting an agent in a target organization
- Social engineering

Government Sources

Government entities maintain a lot of information, some of which can be accessed by the public, and thus, government sources can be a valuable information resource for intelligence professionals. They can supply invaluable background information on target organizations, and they can provide information about the lifestyles of individuals.

Some valuable government sources include filings with national securities associations and business filings.

Filings with National Securities Associations

Companies whose stocks are traded on a stock exchange, among others, are required by law to file certain documents with securities regulatory authorities, and such filings might contain valuable information. Often, these filings are available to the public, and in such circumstances, they can provide a wealth of information about the filing company, including its type of business, history, organizational structure, auditor, balance sheets, and income statements.

In the United States, publicly traded companies must make such filings with the Securities and Exchange Commission (SEC), and SEC filings may be obtained from EDGAR (Electronic Data Gathering, Analysis, and Retrieval). EDGAR is a system that collects SEC filings, and it performs automated collection, validation, indexing, acceptance, and forwarding of SEC filings. Intelligence professionals can use the EDGAR system to obtain the target's Form 10-K, which contains the company's income statement and balance sheet, information on its debt structure, foreign ownership, properties owned, subsidiaries, industry descriptions, depreciation, dilution, and other key business information.

Business Filings

Most jurisdictions require that public companies, nonprofits, and some private companies submit financial filings and various types of organizational filings to the government. These filings can contain valuable information; for instance, they can reveal the real property, vehicles, equipment, and intellectual property registered in an organization's name.

In the United States, for example, companies are formed by filing articles of incorporation with the secretary of state (or state corporation bureau or corporate registry office) in the state in which the company does business, and these records are public record. Articles of

incorporation can reveal who owns or controls a particular business and verify the state(s) in which a company is registered as a corporation.

Such business filings can be valuable to intelligence professionals. They can identify the companies within a jurisdiction in which a person serves as an officer or director, and an intelligence professional can use such records to map out the officer's business interests and uncover lesser-known or hidden connections between businesses.

Industry Reports and Studies

Industry reports and studies provide summaries of primary and secondary market research within various industries, and many of these reports and studies can be valuable to intelligence professionals. They often provide statistical benchmarks that can show where a company stands in its industry, and they can be used to estimate a target company's financial status. In addition, they help delineate the standards for evaluating successful companies in specific industries. The basic resources for industry reports and studies are government sources, commercial databases, and directories. In the United States, for example, the government provides free access to numerous resources offering industry data and statistics.

Periodicals

There are thousands of periodicals (e.g., magazines, journals, newsletters, newspapers directories, and yearbooks) that provide information on businesses, and these publications can be excellent sources of information, particularly for background information on an individual or a business.

Some recognized categories of business periodicals include:

- Trade resources (e.g., association and industry publications, studies, surveys, newsletters, and directories)
- Publications by academic institutions
- Speaker presentations and speeches
- Conference presentations
- Security analysts' reports

Additionally, local newspapers often run profiles of local businesses and groups, and most newspaper companies provide searchable online databases of their publications.

Moreover, there are a number of commercial database vendors that offer wide access to newspapers and periodicals. These information database providers offer online access to the text of hundreds of newspapers worldwide, and although most providers are available for a fee, many can be accessed for free at most libraries.

Online Sources

A great deal of information can be accessed through the Internet for little or no cost, and intelligence professionals can use the Internet to obtain valuable information about target entities.

For example, public records maintained by government entities can be obtained online from a number of online databases, but typically, public records can be searched online through:

- Government websites
- Public record vendors

More information about online sources is contained in the "Sources of Information" chapter in the Investigation section of the *Fraud Examiners Manual*.

Data Analysis

Intelligence professionals might use data analysis software for intelligence purposes. The functions performed by analytical software programs can easily be translated to business intelligence needs, uncovering patterns related to corporate filings, corporate officer/director (O/D) searches, patent and trademark applications, and other diverse compilations of data that, when pieced together, can indicate the potential direction in which a competitor is headed.

To illustrate, consider how an intelligence professional might use data analysis to identify hidden relationships between key scientists and companies in a particular industry. To show the companies for which key scientists serve as directors, the intelligence professional can use an analytic program to cross-check patent authors that he extracted from a patent database against an O/D search. He can also use the software to generate visual displays of the relationships between the companies.

Job Postings

Job postings can contain valuable information. They can provide information about the job skills that a target company needs and the number of employees it is seeking to hire. With

such information, an intelligence professional can infer a target company's success over time, the kinds of projects it is developing, or where it is devoting personnel resources. Moreover, large-scale hiring could indicate that a competitor has signed or expects to sign a large contract. In some cases, employment ads also point out defections of key personnel.

Employment ads also indicate what companies pay their employees, and this could be valuable for competitors in recruiting coveted personnel. It could also help identify employees who might be susceptible to recruitment tactics because of low pay or a high rate of employee dissatisfaction (as evidenced by a high rate of turnover in a particular department).

Environmental Impact Statements

Environmental impact statements are required for certain actions that significantly affect the quality of the human environment, and they contain large amounts of historical, financial, and operational information. The company filing an environmental impact statement not only has to supply this background data, but also has to explain its actions in detail. Details on emissions, hazardous materials used, and possible accidents stemming from operations provide a wealth of information that can provide an excellent picture of the size and operational capability of a plant or company. Often, this kind of information can be used to identify the date an organization's project will commence.

Commercial Filings

Commercial filings can provide valuable information about a target's business transactions. Commercial filings are records that banks, finance companies, and other lenders generate when they provide loans or leases to borrowers who use property as collateral for the loans.

Commercial filings can provide valuable information about a target's business transactions. They can help identify personal property that an individual or business has financed, and they can provide operational details by describing equipment and materials that have been purchased or pledged for a loan.

The availability of such records largely depends on whether the relevant jurisdiction is a common law or civil law country, however. The majority of countries in which commercial filings are publicly searchable have common law systems in place. Civil law countries rarely have a public registration system for commercial filings.

In the United States, the Uniform Commercial Code (UCC) governs commercial filings. UCC filings are maintained and searchable at the state level by each secretary of state. UCC filings are public records that document loans or leases obtained with secured assets.

Favorite Employee Targets of Intelligence Professionals

Again, intelligence professionals might seek out a target organization's employees during their quest for information. Information provided by employees in the following departments can prove particularly valuable: research and development, marketing, manufacturing and production, human resources, sales, and purchasing.

Research and Development

Organizations that perform research and development (R&D) are at risk of corporate espionage because the value of R&D data depends on its exclusivity.

Often, intelligence professionals target R&D personnel because they are almost always in the flow of information. The open exchange of information is part of the nature of their job. They participate in conferences, attend trade shows, and work with academic institutions; however, at each of these functions, they leave themselves open for intelligence spies to listen, mingle, and ask questions.

Also, researchers who publish their findings in industry journals might inadvertently include details of a project on which they are working. This is particularly true in the case of academic professionals who might be hired by a company to perform research or conduct a study. If a company hires an academician to conduct research, management must make sure that the academician understands that he must keep the results confidential. In addition, management must make sure that the academician's use of teaching assistants or graduate students is kept to a minimum and that those individuals understand the confidentiality requirements.

Marketing

Insight into a company's marketing plan is valuable to its competitors. Being careless with vital information such as test marketing results, promotional strategies, and planned introduction dates can be disastrous.

Manufacturing and Production

A company's manufacturing and production information can be valuable to its competitors, and production managers are often good sources of such information.

Human Resources

Job interviews might result in leaks. Intelligence professionals often pay close attention to job postings and announcements. More ominously, they might use this information to arrange a job interview to get information about the target firm and what the job will entail.

Sales

Salespeople are an excellent source of information on pricing, product innovations, and market programs.

Purchasing

Purchasing agents are helpful in divulging suppliers, information about what is selling, and the costs of raw materials and services.

How Information Is Lost or Stolen

Information thieves use a wide variety of methods—not all of which are legal—to gain access to an organization's business secrets. The following are common ways for information to fall into the wrong hands:

- Accident and negligence
- Loss of physical media
- Poor information security procedures
- Improper disposal of documents and media
- Malicious insiders
- Insider spies
- Sleepers
- Computer attacks
- Physical infiltration
- Transactional intelligence
- Social engineering
- Physical surveillance
- Technical surveillance

Accident and Negligence

Employees sometimes inadvertently expose sensitive information due to accident or a lack of awareness. Employees might unknowingly disclose sensitive company information via social media, when talking with friends, or while delivering a speech at an industry conference. It is important that employees are trained to understand what information is considered proprietary so that mistakes of this kind can be more easily avoided.

Additionally, publications such as newsletters or reports to shareholders and speeches or papers that are presented at conferences can inadvertently provide valuable information to competitors. Organizations should implement a system of advance review whereby technical or security staff examine all works prior to their publication or presentation.

Accidental leaks might also occur via the press. Executives eager to brag about their companies often reveal more than they should about research, new products, sales levels, and so on. Furthermore, a company's website might also contain accidental leaks. Corporate spies frequently visit their targets' websites to gather information that these companies have unknowingly made public. Employee telephone and email directories, financial information, key employees' biographical data, product features and release dates, details on research and development, and job postings can all be found on many corporate websites. In some cases, this information provides direct access to company secrets; in other instances, it can be used to build an intelligence campaign. Businesses should pay attention to information published on their websites and in other marketing materials. Generally, anything that does not forward an organization's marketing mission should be excluded or removed.

Loss of Physical Media

Sensitive data is often loaded onto laptops, USB flash drives, memory cards, tablets, mobile phones, and other portable media devices, any of which can be easily lost. It is important that information on these devices be encrypted, protected by a password, and enabled for remote deletion when possible.

Poor Information Security Procedures

To ensure data security and prevent accidental data loss, organizations should employ and regularly update a system for protecting and disposing of confidential information. Classifying data, limiting logical access, and ensuring that policies are in place for emerging trends are all examples of processes that can be implemented to avoid putting sensitive information at unnecessary risk.

Improper Disposal of Documents and Media

Intelligence professionals might obtain sensitive information from documents and media that are not disposed of using proper means. Documents containing sensitive information are often disposed of without first being shredded. Additionally, a business might sell, return, or dispose of machines such as personal computers, mobile devices, or copy machines without first ensuring that all sensitive data has been removed or sufficiently overwritten.

Malicious Insiders

Insiders—individuals with access or inside knowledge about an organization—represent one of the largest threats to an organization's information, and malicious insiders cause a significant number of breaches.

Employees who feel cheated, bored, harassed, endangered, or betrayed at work might seek job satisfaction by sabotaging their employer's data.

Insider Spies (Moles)

Often, a corporate spy will try to obtain information by recruiting an existing insider to act as his agent on the inside. An employee recruited to spy against his employer is known as a *mole*. The mole agrees to betray his employer's trust by handing over confidential information that belongs to his organization.

A corporate spy might recruit a mole through any of the following techniques:

- Bribe the target.
- Extort (blackmail) the target.
- Use romantic or sexual seduction.
- Exploit the target's strong social or political feelings.
- Convince the target that spying is moral or justified. These attacks often target people who feel like victims. An employee who is bitter at having been passed over for a promotion, for example, is a good target. Other typical targets include employees who resent their employers because they feel underpaid or unrecognized.
- Trap a target so that he is essentially forced to spy on his employer.

Because corporate spies use complex methods to turn employees into moles, management must train employees, especially key employees with access to valuable information, to report any suspected recruitment effort made against them as early as possible. Specifically, management must train key employees to be wary of people who:

- Encourage and finance an employee's vice.
- Express a great deal of sympathy for a cause that is important to an employee.
- Offer to help an employee with a serious financial problem.
- Attempt to seduce an employee.
- Attempt to blackmail an employee.

Sleepers

If an information thief has a very long-range interest in monitoring a company, he might place a spy in that target company as a permanent employee. This employee, known as a *sleeper*, keeps a low profile and regularly reports to his control about the company's operations. This kind of spy, especially if well-schooled in corporate espionage, will be extremely difficult to detect.

A sleeper functions like a mole. The difference between the two is that a sleeper is a person who is deliberately planted as an employee in a company to extract information. In contrast, a mole is usually an existing employee of the targeted organization who is somehow compromised and has agreed to turn over his company's secrets to the intelligence professional.

Computer Attacks

Information thieves might access an organization's sensitive information by bypassing its information security mechanisms.

Physical Infiltration

Corporate spies might use physical infiltration techniques to obtain sensitive information. *Physical infiltration* is the process whereby an individual enters a target organization to spy on the organization's employees. Often, corporate spies use physical infiltration when there is a tight time schedule, a lack of available recruits, or expense constraints; however, a spy might also use physical infiltration when he has specialized knowledge that makes him the best spy for the job. Generally, spies with advanced technical knowledge are the best at committing such campaigns.

One common infiltration technique is to secure a position, or pose, as an employee or contract laborer of the target organization. For example, a spy might obtain work as a security officer or a member of the janitorial crew for the target organization.

Another common physical infiltration technique is to steal or fabricate employee badges belonging to the target organization.

Warning Signs of Physical Infiltrations

Detecting physical infiltration can be difficult, but there are some signs that organizations can look for that might indicate there is a spy in their midst:

- Vendors, janitorial personnel, security guards, trash collectors, and other non-employees are seen loitering unescorted around file rooms, offices, mail rooms, shipping docks, computer media storage areas, or other sensitive areas.
- Service technicians show up without having been called.
- There are employee reports of lost security badges, access cards, passwords, and so on.
- Data containing sensitive information is missing.
- Employee desks or offices have been tampered with.
- Individuals try to enter a facility without proper identification or authorization.
- Individuals attempt to gain access to a physical area by *piggybacking* (i.e., gaining access to a secured physical area by exploiting a false association with another person who has legitimate access to the area).
- Reports of trespassing or other criminal activity have been made near a secure facility.

Countermeasures to Physical Infiltration

Security officers can implement specific countermeasures to thwart a spy's attempts at infiltrating their company. These countermeasures are as follows:

- Avoid storing proprietary data in areas visible to the public.
- Establish a procedure for tracking and locking up sensitive data.
- Properly bond and identify cleaning personnel and control their access to the facility.
- Verify vendors' credentials and have a company representative escort them during their visit.
- Encrypt any proprietary lists.
- Educate employees to properly store sensitive data and to question the credentials of anyone visiting the site.
- Instruct employees as to what information they may disclose over the telephone.
- Require that employees sign nondisclosure agreements.

Transactional Intelligence

Intelligence professionals can obtain valuable intelligence by observing just about any mundane business transaction. For example, frequent flyer miles document where an

executive has traveled. Credit card receipts record a trip's itinerary and goods or services purchased. Any one piece of transactional information by itself has minimal value, but taken together, this type of information can provide an extensive profile on a target.

Spies might develop a network of paid informants who can obtain transactional intelligence on their behalf. These informants come from a wide range of businesses and include:

- Travel agents
- Airline reservation personnel
- Major credit card companies
- Staff at major Internet providers
- Employees at video, music, and other entertainment outlets
- Staff of adult entertainment providers that the target frequents
- Telephone company employees with access to telephone records
- Employees of commercial database providers such as Dialog and Dun & Bradstreet who have access to transactional records

These informants will, for a fee, provide transactional intelligence on a subject that can tell a corporate spy about:

- A person's vices
- Details of a target's business travel
- Hotels where the target stayed and where he is likely to stay again in the future (this can be useful for setting up surveillance)
- Whom the target has called
- Interests and hobbies (another way to edge into the target's confidence)
- Companies or subjects the target has researched

This type of intelligence is really a hybrid of documentary source intelligence (combining purely open sources available to the public and gray sources) and human intelligence. The corporate spy needs an inside contact to obtain the target information, but once he has the information, he can analyze it without additional assistance.

Transactional intelligence is very helpful in the collection of human intelligence. If, for example, a spy knows a subject's hobbies, he can use that knowledge to strike up a conversation or possibly a friendship with the target.

A spy can also be his own source of transactional intelligence.

Social Engineering

Rather than infiltrate a company to extract needed information, a spy might use social engineering to induce target employees to divulge sensitive information. *Social engineering* is the act of using deceptive techniques to manipulate people into taking certain actions or disclosing information. Corporate spies use social engineering to collect sensitive information about a target.

People are the biggest vulnerability in information security, and social engineering schemes prey on this vulnerability. Social engineering does not exploit technical vulnerabilities in information technology; instead, it exploits social psychological weaknesses in individuals. Consequently, spies do not need a high level of technical expertise to carry out social engineering schemes, but they do need decent social skills.

In social engineering schemes, social engineers use various forms of trickery, persuasion, threats, or cajolery to encourage their targets to release information that the engineers can use and exploit to achieve their goals.

Attackers engage in social engineering to achieve various means. Some use social engineering to gain unauthorized access to systems or obtain confidential communication so they can commit fraud, intrude into networks, gain access to buildings, steal another party's secrets, commit identity theft, or engage in some other nefarious act. In some situations, spies use social engineering to procure information that will give them a competitive advantage, whereas others might engage in social engineering to find ways in which they can install malware.

Why Social Engineering Attacks Succeed

Social engineering attacks succeed for several reasons. For one thing, these attacks leverage characteristics of human nature, making them hard to prevent. That is, social engineering attacks exploit certain traits of ordinary human nature, such as:

- The tendency to trust people
- The reluctance to be (or seem) disagreeable
- The desire to help
- The desire to avoid appearing paranoid
- The desire to be cooperative
- The fear of consequences for not doing something right or for doing something wrong
- The reluctance to refuse requests

- The desire to be nice
- The tendency to avoid making others feel bad

Social engineering attacks also tend to succeed because combating them is difficult.

How Social Engineering Works

Social engineering attacks tend to follow a phased approach, and for purposes of simplicity, the phases can be arranged as follows:

- Gather intelligence about the target.
- Select the tactic.
- Contact and build trust with the target.
- Elicit information by exploiting the relationship.

GATHER INTELLIGENCE ABOUT THE TARGET

To conduct a successful social engineering attack, social engineers must gather information about the target and the target's environment. The more information a social engineer has about his target, the greater the chances that his attack will be successful. For example, a social engineer will have a greater chance of success if he knows his target's internal processes, jargon, and organizational structure.

Accordingly, in this phase, the social engineer gathers as much information as possible to obtain the information needed to plan and carry out the attack. That is, the social engineer seeks information regarding the target organization, its employees, and its vulnerabilities. Once the social engineer has obtained this information, he can use it to make the target more susceptible to manipulation.

Often, the social engineer's goal in this stage is to learn as much information as possible about the target organization so he can sound like an employee, contractor, vendor, or other party related to the target organization.

In this phase, the social engineer gathers information passively (i.e., without contacting the target directly) by focusing on finding, selecting, and acquiring publicly available information about a target. The information gathered might include any available personal information, such as employee names, ages, positions, hobbies, interests, addresses, banks, friends, and so on.

SELECT THE TACTIC

Once the social engineer has collected an appropriate amount of information about the target, he will determine which tactic would be most suitable to achieve the desired goals. Social engineers use various tactics, including:

- Pretexting
- Shoulder surfing
- Phishing
- Spam and chain emails
- Reverse social engineering

PRETEXTING

Pretexting is the act of impersonating someone else or making false or misleading statements to persuade a target to release information or perform some action. Pretexting can occur in-person, over the phone, or through some other form of communication.

Social engineers often engage in pretexting by posing as a person of authority, a member of tech support, someone who has legitimate access to the target's network, an individual who needs help, a government employee, and so on.

SHOULDER SURFING

Shoulder surfing involves watching and listening to an unsuspecting target from a nearby location while the target enters his username and password into a system, talks on the phone, fills out financial forms, or performs some other task from which the engineer can obtain valuable information.

SPAM AND CHAIN EMAILS

Social engineers use spam and chain emails to carry out their attacks. Email is a common method used in social engineering attacks because it is widely used, and social engineers can send emails designed to look like they come from popular, trusted sources. Also, social engineers can include infected attachments or links directing targets to malicious sites in such emails. Moreover, social engineers can design emails to contain specific content particular to target users. Engineers know that emails with personally interesting messages are going to get more attention than those with broad messages.

PHISHING

Phishing is a popular scheme that involves tricking businesses or individuals into providing passwords, account numbers, or other sensitive data by falsely claiming to be from an actual business, bank, ISP, or other entity with which the targets do business.

REVERSE SOCIAL ENGINEERING

In reverse social engineering schemes, social engineers make targets think that the engineers can help them by providing security-related services. These schemes involve three phases. First, social engineers sabotage the target's network or make the target think that his network has been sabotaged. This can be done by launching a network attack against a target website or by sending an email from a spoofed email address telling target users that their systems are infected with malware. Thus, in the first step, social engineers create a problem (or give the impression of a problem) in the target's network.

Second, social engineers place themselves in a position to help the target with an actual or perceived problem by advertising their services as security consultants. After seeing the advertisement, the target organization, under the false assumption that the social engineer is a legitimate security consultant, hires the engineer and allows him to work on the network.

Finally, when working on the target's network, the social engineer gives the impression that he is assisting the target with its security issue, but in reality, the engineer is performing some malicious act on the network.

CONTACT AND BUILD TRUST WITH THE TARGET

Once social engineers have collected an appropriate amount of information about their targets and selected the tactic, they will contact their targets, seeking to build trust with them. The trust that social engineers gain will be used to elicit information that can be exploited to reach the goals of their attack.

Building trust serves several purposes, including:

- Putting targets at ease and making them more comfortable
- Making targets more susceptible to listen
- Building the targets' confidence in the social engineer

Social engineers begin building trust by establishing rapport with their targets. Social engineers use their communication skills to develop rapport with targets so that the targets will feel comfortable talking to them. Conversations without rapport tend to fail.

Often, social engineers establish rapport by:

- Having a genuine interest in their target
- Making "small talk"
- Presenting a professional, trustworthy appearance
- Being a good listener
- Being aware of how they affect other people
- Keeping the conversation on topics other than themselves
- Demonstrating empathy
- Being knowledgeable
- Expressing curiosity
- Finding ways to meet their targets' needs
- Breathing at the same rate as their targets
- Matching their targets' vocal tones and speech patterns

Social engineers also build trust by avoiding suspicious, sensitive questions, and they might use a piecemeal approach by instigating a series of conversations with the target, seeking to gain small pieces of information over time.

Additionally, social engineers can build trust by:

- Projecting confidence and control
- Being likeable (e.g., sharing common interests)
- Being believable
- Making fun of someone together with targets
- Sharing common interests with targets
- Helping targets with their problems
- Using humor

It is important to note that the larger the target organization, the easier it is to establish trust. In smaller organizations, targets are more likely to know whether the attacker is who he claims to be.

EXPLOIT THE TARGET'S TRUST TO ELICIT INFORMATION

Once the social engineer has built rapport and established trust with the target, he will elicit information that he can use and exploit to reach the goals of his attacks. *Elicitation* is the process of extracting information from something or someone.

Thus, in this stage, social engineers use conversational skills and various other tactics to encourage their targets to release information that can be used and exploited to achieve particular goals.

Typically, social engineers elicit information subtlety in seemingly normal and innocent conversations. This type of elicitation is preferred because it works well, is low risk, and is hard to detect.

When engaging in elicitation, social engineers want their targets to take action; the more information a social engineer has, the more likely it is that his elicitation efforts will succeed.

ELICITATION SKILLS

Although social engineering does not require a high level of technical expertise, it does require social skills and other components. The social skills and components needed to be a successful elicitor include:

- Communication skills
- Adaptability (i.e., ability to adapt communications to fit the environment and situation)
- Relationship and bonding skills (i.e., ability to build bonds or relationships with other people)
- Interrogation skills (i.e., the ability to ask questions that will generate a response)
- Influence skills (i.e., the ability to influence other people)
- Manipulation skills (i.e., the ability to manipulate other people)
- Lack of fear when talking to people in abnormal situations
- Care for other people
- A nonjudgmental ear

COMMON ELICITATION TACTICS

Social engineers use numerous tactics to elicit information. Some common elicitation tactics include:

- *Appealing to the target's ego*: Social engineers often appeal to their targets' egos to coax them into a conversation that otherwise would not take place. Likewise, appealing to a target's

ego will tend to make the target more emotionally sure of himself, which tends to remove logical awareness that a potential breach might be occurring.

- *Expressing mutual interest*: Expressing mutual interest is a valuable tactic because it extends the relationship between the engineer and target beyond the initial conversation.
- *Making deliberate false statements*: During conversations, social engineers can make deliberate false statements to elicit responses containing correct statements.
- *Volunteering information*: Social engineers may volunteer useful information to their targets, which triggers a compulsion in their targets to respond with equally useful information.
- *Assuming knowledge*: This tactic exploits the common assumption that if someone has knowledge about a specific topic, it is acceptable to discuss that topic with him. Social engineers exploit this assumption by confidently presenting information about a specific topic to a target and then building a conversation around that topic.
- *Exploiting the desire to be helpful*: Organizations train their people to be helpful, and social engineers can exploit this to further their schemes. In their desire to be helpful, people might try to solve other people's questions and give out sensitive information, and this can give social engineers information with which they can exploit.
- *Exploiting feelings of fear*: Often, social engineers take advantage of human fear. When people experience fear, they often feel panicked and rushed, and such emotions affect the logical functioning of human judgment. Frequently, social engineers will impersonate a person of authority to exploit employees' fear of authority. Likewise, social engineers will exploit employees' fear of getting in trouble. Nobody wants to be the employee that causes problems, and this can be exploited to extract sensitive information.
- *Encouraging action based on a chance for some benefit:* Social engineers might also elicit information by persuading targets that they will likely receive a benefit by complying with the engineers' requests.
- *Encouraging action based on moral duty*: Social engineers can also elicit information by encouraging targets to act based on a sense of moral duty or outrage. In this approach, social engineers try to convince their targets that their act of compliance will mitigate some wrong.
- *Exploiting desires to avoid guilt*: Most people seek to avoid feelings of guilt. Social engineers can exploit this desire by making requests that manipulate empathy or create sympathy, the compliance with which will lead to the avoidance of guilt.
- *Making unreasonable requests*: Some social engineers will elicit information by appealing to targets' desires to compromise. In this tactic, the social engineer makes an unreasonable request that he knows will be rejected. Once the request is rejected, he makes a follow-up request that is more reasonable. Thus, this approach uses an "if you can't help me

with this, can you help with something else" tactic. After rejecting the first request, the target will feel more obligated to comply with the follow-up request.
- *Asking well-informed questions*: By asking the right questions, the social engineer can obtain valuable information.

Red Flags of In-Person Social Engineering Schemes

Here are some red flags of in-person social engineering schemes that employees should look for:

- A person makes an unusual request
- A person engages in meandering conversation and then makes an urgent request
- A person making a request:
  - Is overly flattering (e.g., "You are the only person who knows this stuff.")
  - Refuses to give his contact information (e.g., "I'll call you back in a few minutes.")
  - Rejects any possibility of a callback
  - Asserts that the request is urgent
  - Claims to have the same interests or a similar background
  - Uses intimidation to drive the request
  - References higher-ups to drive the request
  - Asserts that the request has been approved by management
  - States that negative consequences will result if his request is not complied with
  - Is quick on and off the phone
  - Is chatty even though they have never met
  - Fails to use standard industry jargon or otherwise sounds like an outsider
  - Sounds unnatural or stilted
  - Offers to help with an unknown problem
  - Brags about his authority within the organization
  - Threatens reprimands if requests are not granted
  - Overemphasizes details
  - Volunteers information
  - Answers questions that were not asked

Preventing Social Engineering Schemes

Because social engineering attacks leverage characteristics of human nature, they are hard to defend against. Nevertheless, there are ways organizations can prevent becoming victims of such attacks.

Common ways to combat social engineering schemes include:

- Have clear security policies and procedures.
- Conduct security awareness training.
- Educate employees about how social engineering attacks are tied to psychology and human nature.
- Train employees to identify social engineering attacks and be aware of how social engineering works, the data that social engineers will seek, and the types of information that employees are allowed to disseminate.
- Educate employees so they understand the value of information that social engineers seek.
- Educate employees as to why security protocols are essential.
- Train employees on an ongoing basis to keep security fresh in their minds.
- Train employees to focus on the nature of requests, not the context in which requests are made.
- Train help desk employees to ask specific identifying questions before they give out any information over the phone.
- Train employees to verify the identity of people making requests, and give employees a list of minimum identification requirements that people making requests must meet before information can be distributed to them.
- Tailor employee training to the audience.
- Promote employee compliance with security policies.
- Make employees aware of social engineering threats and educate them about actual instances of social engineering attacks (e.g., maintain an internal website or distribute employee newsletters that contain stories about social engineering schemes and prevention tips).
- Prohibit employees from giving out passwords or personal identification information.
- Inform employees that they should not leave confidential information and computers unattended.
- Keep references to key administrative, technical, and billing contacts for the organization's Internet domain as anonymous as possible.
- Verify all emails for authenticity.
- Shred all trash containing confidential information before disposal.
- Encrypt all sensitive data.
- Test employees' security readiness (e.g., security personnel might call their own organization's help desk to see what information they can obtain without identifying themselves).

- Train employees to document suspicious events.
- Undertake social engineering audits.
- Issue security alerts when suspicious activity occurs.
- Train employees on how to mitigate problems that occur.
- Conduct penetration tests that use social engineering.

Physical Surveillance

Again, a corporate spy might conduct *physical surveillance,* which is the real-time observation of a target's actions or communications.

Spies sometimes perform surveillance on targets to obtain information on human sources. There are a number of goals for this kind of surveillance. They include:

- To discover:
  - Who they are
  - Where they live
  - What they do in their spare time
  - What they want to keep secret
  - Who their friends are
  - Who their enemies are
- To look for:
  - Cars
  - Homes
  - Recreational activities
  - Levels of income and debts
  - The subject's importance to the organization
- To uncover what they throw in the trash, such as:
  - Financial papers
  - Information regarding medical problems
  - Information regarding family problems
- To learn about their enemies, such as:
  - Ex-lovers
  - Fired employees
  - Political opponents
  - Competitors
  - People owed money

- To make contact with the target:
  - By finding out what he thinks about his job, family, or life in general
  - By determining the degree to which the target will confide in others

Technical Surveillance

Again, *technical surveillance* is the practice of covertly acquiring audio, visual, or other types of data from targets through the use of technical devices, procedures, and techniques. When corporate spies resort to the use of technical surveillance, it is usually to gather nondocumentary evidence, or information that cannot be found through open sources.

Experienced corporate spies know what they are looking for and devise carefully protected collection plans before initiating any surveillance campaign. They know that the more time they spend planning, the more likely they will not be detected and the greater their intelligence yield will be.

Also, most intelligence professionals adhere to the following rules for using technical surveillance:

- Any device left on site must not be traceable back.
- Wiretaps and wiretap devices must blend into their surroundings so nothing appears out of the ordinary.
- Radio transmitters must not send signals in those parts of the electromagnetic spectrum that are in common commercial use.
- Nothing about an intelligence campaign should be revealed to anyone except one's client, even after the job is finished.
- All documentary evidence of an electronic surveillance campaign should be destroyed once a job is finished.

Corporate spies might employ various forms of technological surveillance. Some of those forms are discussed below.

Aerial Photography

Though its origins lie in the military sector, aerial photography has emerged as a valuable tool in business intelligence. Google Earth, a free online tool that enables users to obtain an aerial photo of properties by satellite, has made gathering this type of intelligence quite easy. Additionally, there are private aerial photography firms that have fairly complete negatives for land in their service area. These firms also accept special assignments to photograph

specific ground areas on a schedule specified by the client. Aerial photography is used by spies to gather information on a competitor's construction or expansion products, to measure the size of its shipments, or to determine the number of employees that the company has working for it, among other things.

Bugging and Wiretapping Devices

Hidden microphones, wiretaps, and other forms of electronic surveillance equipment have become common means by which intelligence professionals keep tabs on their competition. The spy has two primary considerations in a wiretapping campaign: where to insert the surveillance equipment and which of the various technologies to employ.

THE INSERTION POINT

In identifying the insertion point, the spy must choose an area where proprietary information is likely to be discussed or displayed and where background noise and electronic interference remain minimal. Spies frequently choose areas with proximity to computers and telecommunications equipment carrying proprietary data as an insertion point.

Spies might also target areas conducive to employee conversations. This can include any place inside or outside the targeted company where key personnel gather and chat. Examples include smoking areas; recreational areas such as bars, lounges, and coffeehouses; employee cafeterias; relaxation areas; exercise rooms; and meeting rooms. To target particular operations such as information services, spies might wire the offices of key managers, which are likely to provide access to a large portion of human information flow.

THE TECHNOLOGY

In determining which technologies to employ, the spy must factor in environmental conditions such as lighting (if video surveillance is employed), noise levels, and distance from the source. Other factors include the risk of the sensing device being discovered, power supply problems, and access to the device for servicing after installation.

Some of the more common forms of electronic eavesdropping devices include:

- Satellite tracking systems
- Drop-in telephone bugs
- Carbon microphones
- Electronic and magnetic microphones
- Spike and cavity microphones

- Infinity transmitters
- Shotgun or parabolic microphones
- Wiretaps

SATELLITE TRACKING SYSTEMS

Satellite tracking systems track time and location information. In most satellite tracking systems, a small transmitter is surreptitiously attached to the subject's vehicle. The transmitter communicates with global positioning satellites (GPS) and converts the coordinates of the vehicle onto a map. The spy can view maps that show the vehicle's location and path. These systems are capable of generating event lists and plain-text histories of where the vehicle has traveled. A variation on this tracking design is that in some satellite tracking software, the system creates a trail of electronic clues on the map display. The map can be a powerful tool in tracking the movements of executives and key company employees.

DROP-IN TELEPHONE BUGS

Spies frequently use drop-in telephone bugs, which have the advantage of blending in with everyday existing telephone equipment. Drop-in bugs are simply inserted into the handset device on a normal telephone, and once inserted, the target's conversations are transmitted to a remote receiver where they are recorded.

Drop-in bugs are rarely detected because most people never bother to check their phones for bugs. Thus, a drop-in telephone bug offers minimal risk of exposure. When a spy has access to the physical premises of a target and wants to listen to conversations on a particular telephone line, he usually chooses this type of device.

CARBON MICROPHONES

Carbon microphones provide good pick-up if properly hidden and located. They offer excellent coverage of fixed locations: smoke rooms, employee lounges, and other gathering spots. As with other forms of listening equipment, these microphones are usually equipped with a transmitter that relays intercepted conversations off-site to a recorder. From the spy's perspective, this is much safer than maintaining a recorder on-site. With a remote transmitter, even if the microphone is detected, the target cannot locate or recover the recorded material.

ELECTRONIC AND MAGNETIC MICROPHONES

Electronic and magnetic (or dynamic) microphones provide good close-range coverage. Both types of microphones are smaller than the standard carbon microphone, though they tend to offer a lower range of coverage. Magnetic microphones can be very small, and to be useful, the spy must place them close to the speakers and hide them inside something small.

SPIKE AND CAVITY MICROPHONES

Spike and cavity microphones work best when the spy has access to an adjoining area and needs to conduct surveillance in an adjoining room. For example, if a spy has free range in a utility room next door or in an adjacent hotel or motel room, a spike microphone can be inserted through the adjoining wall to monitor conversations in the target's room. This type of microphone is so small at its insertion point that it is virtually undetectable to the casual observer.

INFINITY TRANSMITTERS

Infinity transmitters are a special kind of device used to monitor conversations in a room through a telephone line.

SHOTGUN OR PARABOLIC MICROPHONES

Spies can use shotgun microphones, parabolic microphone devices, and laser audio detection equipment to listen to conversations occurring far away.

WIRETAPS

Wiretapping involves splicing a listening or recording device into a wire (such as a telephone wire, a PBX cable, an alarm system, or a local area network cable) that the target uses for communication. Standard phone systems, in particular, are very vulnerable to wiretapping. Taps are usually placed at the telephone box in the basements of buildings, on lines outside buildings, or on telephone pole junction boxes near the target's offices. The different types of wiretaps that can be used include hardwired wiretap, soft wiretap, record wiretap, and transmit wiretap.

WARNING SIGNS OF BUGGING AND WIRETAPPING

Covert eavesdropping might be difficult to detect, particularly because most people do not know what signs to look for. James M. Atkinson of the Granite Island Group, a technical surveillance countermeasures firm in the United States, has compiled a list of 27 warning

signs that might indicate that an organization is the target of an electronic eavesdropping campaign.[1] Those red flags are as follows:

1. Others seem to know your confidential business or trade secrets.
2. Information discussed in secret meetings or contained in secret bids does not remain secret.
3. People seem to know about your organization's activities when they should not.
4. Strange sounds or volume changes are detected on your phone lines. This is a common byproduct of wiretaps or activation of a similar listening device.
5. You notice unusual static, popping, or scratching on phone lines. This is another common sign of a wiretap or bug.
6. You can hear sounds coming from your phone handset when it is hung up. This is typically caused by a device called a "hook switch bypass," which turns a telephone receiver into an eavesdropping microphone and speaker and allows a spy to monitor conversations near the phone (usually within 20 feet, or five to six meters).
7. Your phone rings and nobody is on the other end of the line, but you hear a very faint tone or a high-pitched squeal and beep. This is an indicator of a slave device, or line extender, being used on your phone line. This is also a key indicator of a harmonica bug or infinity transmitter being used.
8. You hear a tone on your line when your phone is off the hook (by using an external amplifier).
9. An office radio suddenly develops strange interference. This could be caused by eavesdropping devices that use frequencies within or just outside the FM radio band. These signals tend to drift and will quiet FM radios in the bug's vicinity.
10. A car radio suddenly starts "getting weird."
11. An office television suddenly develops interference. Eavesdropping devices can tend to interfere with television reception.
12. Your office appears to have been burglarized, but nothing was taken. Someone could have entered the premises to plant a listening device.
13. Electrical wall plates (covering outlets, switches, smoke alarms, and lighting fixtures) appear to have been moved slightly. These are among the most popular locations for hiding listening devices, and they require that the plates be removed. Watch for slight variations in the color or appearance of the power outlets or light switches, as these are often swapped out by an eavesdropper.

[1] This list is provided courtesy of James M. Atkinson and The Granite Island Group, 127 Eastern Avenue, #291, Gloucester, MA 01930, (978) 546-3803. (www.tscm.com).

14. A dime-sized discoloration appears on an office wall or ceiling. This is a sign that a pinhole microphone or video camera has been installed.
15. One of your vendors gives you an electronic device such as a desk radio, alarm clock, CD player, or small television. These gifts frequently contain secret eavesdropping devices.
16. A small bump or deformation has appeared on the baseboard by the floor. This is a strong indicator that someone might have concealed covert wiring or a microphone imbedded into the adhesive that holds the molding to the floor.
17. A smoke detector, clock, lamp, or exit sign in your office or home looks slightly crooked, has a small hole in the surface, has a quasi-reflective surface, or otherwise appears to have been tampered with. These items are also common places for concealing bugs.
18. Certain items just appear in your office without anyone knowing how they got there. Typical items to watch for and beware of are clocks, exit signs, sprinkler heads, radios, picture frames, and lamps. They might contain listening equipment and could have been placed in your office by a spy.
19. Drywall dust or debris is found on the floor next to a wall. This could be a sign that a pinhole microphone or video camera has been installed nearby.
20. Small pieces of ceiling tile or grit are found on the floor or on a desk. Also, a cracked, chipped, or gouged ceiling tile, sagging ceiling tiles, or ceiling tiles not properly set into track might be observed. This indicates that a ceiling tile has been moved, possibly because someone has installed a technical surveillance device above your ceiling.
21. Phone company trucks and utilities workers seem to be spending a lot of time near your home or office. These workers could actually be corporate spies in disguise.
22. Telephone, cable, plumbing, or air conditioning repair people show up to work when no one called them. This is a very common method for an eavesdropper to plant a bug.
23. Service or delivery trucks are often parked nearby with nobody in them. These vehicles might be listening posts for spies. In particular, look for vehicles that have ladders or pipe racks on the roof, have tinted windows, and are large enough to conceal a person in the back.
24. Your door locks suddenly do not "feel right," become "sticky," or fail altogether. This is evidence that the lock has been picked, manipulated, or bypassed by an intruder.
25. Furniture appears to have been moved slightly and no one knows why. Eavesdropping devices are commonly hidden behind or inside furniture.
26. Things seem to have been rummaged through, but nothing is missing. This could be a sign that someone has been looking through your papers, perhaps even copying them

before returning them to your work area. The most common "rummaging" targets are the backs of desk drawers, the bottom of file cabinets, closets, and dresser drawers.

27. An eavesdropper sends you a copy of your private conversations. As simple as it seems, this is the strongest indicator and solid proof of eavesdropping. An eavesdropper will sometimes send a victim a copy of a private conversation he intercepted in an attempt at blackmail, or in an attempt to terrorize or stalk the victim. This is commonly seen in civil lawsuits, criminal court cases, marital problems, shareholder disputes, custody battles, and other situations in which one side has a position of weakness and is psychologically trying to undermine its opponent.

Video Surveillance

Video surveillance can also be used in corporate espionage campaigns. The role that video cameras play in such campaigns has several dimensions. Cameras can be placed in a room with computers to record passwords, logins, user manuals, text specifics, error messages, document contents, and keyboard overlays. Cameras can be used to monitor activity on receiving and shipping docks. Planted microcameras can track activity on production lines or presentations in meeting rooms. They can also capture executives or key employees engaging in embarrassing activities.

Video cameras can be used to track security patrols, access to special areas like labs, the emptying of security wastebaskets, and other activities, and such information can aid a spy in penetrating restricted or sensitive areas.

Photographic Cameras

Corporate spies can use cameras to obtain a company's secrets.

MINICAMERAS

With the advent of copy machines in almost every office, the need to employ the minicamera to capture information from documents dramatically declined. But documents such as maps, schematics, diagrams, and engineering drawings frequently cannot be easily copied due to their size, and the minicamera is a viable option for capturing the information on these items.

INFRARED CAMERAS

Infrared cameras contain night vision technology that increases visibility without a visible light source, and they have value when the spy is conducting surveillance under very low

light or needs to examine damaged or erased documents. Even the contents of burned documents can be detected under the right conditions with infrared technologies.

DIGITAL CAMERAS

A good digital camera is the mainstay in a spy's surveillance arsenal. Digital photos of things like signs, lettering on the side of vehicles, the configuration of buildings and streets, license plates, and other important details is valuable. Photographs of key target employees can also be valuable in many intelligence campaigns.

To avoid attracting attention when using digital cameras, the intelligence specialist generally uses telescopic or reflective lenses to zoom in on details from a safe distance. In building a visual file on a plant site, a spy will take ground-level photographs from around the entire circumference of the targeted area. He will even photograph computer screens that are visible through windows.

To aid in analyzing photographs at a later date, the specialist will catalogue all photographs as to:

- Subject matter
- Date/time of day
- Direction of a shot
- Number in a sequence of shots
- Important features in a shot

This data can be stored in a database like Microsoft Access, and photographs themselves can be incorporated into the database. Photographic images; excerpts from videotape surveillance; aerial photographs; and relevant diagrams, document images, or drawings can also be integrated into one database for extensive analysis. Analytical investigative databases like i2 allow for the organization of visual data. A database generates various narrative reports, charts, diagrams, and chronologies. The opportunities for an information multiplier effect are tremendous.

Cell Phones

While analogue cellular telephone networks could easily be scanned by anyone with basic tools, modern digital cellular technology is significantly more complicated to monitor. Most analogue cellular networks have been shut down or replaced by digital networks, although analogue roaming services are occasionally present in rural areas. The most common mobile

phone platform is Global System for Mobile Communications, commonly known as GSM, which transmits communications that are fully digital and highly encrypted. Despite the relative difficulty of monitoring digital mobile communications, digital networks can be penetrated by someone who is suitably motivated. Additionally, mobile communications are commonly monitored by government agencies and are potentially vulnerable to surveillance at their network's switches and trunks. Employees should always keep in mind that someone could be listening to their conversations. Sensitive information should not be conveyed by cellular phone.

Monitoring Computer Emanations

Information professionals can also monitor computer emanations, which form detectable and decodable patterns.

For example, a detector or receiver, known as a Van Eck unit, can reproduce keyboard entries on a computer screen even from a considerable distance. A Van Eck unit consists of a directional antenna, logic circuits, and two adjustable oscillators (one for the vertical and one for the horizontal). With proper adjustments, a van parked across the street that is equipped with a Van Eck receiver can eavesdrop on the contents of a CRT or LCD display by detecting its electromagnetic emissions.

To prevent competitors from monitoring computer emanations, organizations can shield their computer equipment and transmission lines—a process known as *Tempesting*. While this process is used extensively in the military and by certain defense contractors, *Tempest* procedures are expensive, and their high costs prevent many private sector businesses from employing them.

Computer System Penetrations

In some cases, information thieves will attempt to extract information by penetrating a company's computer defenses. This can be part of an organized intelligence campaign, or in some cases, it is simply a random attack by a hacker. For more information on how outsiders attempt to penetrate computer systems, see the "Computer and Internet Fraud" chapter in this section of the *Fraud Examiners Manual*.

Electronic Countersurveillance

If management has a reasonable suspicion that its organization has been bugged or is the target of electronic surveillance, it should consider hiring an expert to conduct a technical surveillance countermeasures (TSCM) survey. A TSCM survey (commonly referred to as "debugging") is an expert examination designed to detect, identify, and locate electronic eavesdropping devices, security hazards, or security weaknesses in a specific area. A TSCM is designed to help the organization achieve two goals: (1) to detect the presence and location of technical surveillance equipment and (2) to identify existing and potential security weaknesses.

In choosing TSCM professionals, management should make sure that the professionals are competent in electronics and have extensive knowledge of design, engineering, and maintenance. They must also be trained in eavesdropping techniques, practiced in RF (radio frequency) allocation and propagation, and knowledgeable about all techniques of modulation, electrical wiring, and installation principles.

TSCM sweeps are sensitive operations that should be conducted with as much secrecy as possible. It is best to limit the number of people within the organization who are notified of the operation because it is always possible that a mole might exist. TSCM operatives normally operate under a cover story to explain their presence at the facility.

When possible, TSCM sweeps should be scheduled after hours to limit the number of personnel who encounter the survey team. TSCM experts should be accompanied at all times during their sweep.

Insider Threats to Proprietary Information

Insiders represent one of the largest threats to an organization's information resources. *Insiders* are individuals with access or inside knowledge about an organization, and such access or knowledge gives them the ability to exploit that organization's vulnerabilities.

Insiders enjoy two critical links in security that put them in a position to exploit organizations' information security vulnerabilities:

- Trust of their employers
- Access to facilities

Information theft by insiders is especially a concern when employees leave an organization. Often, employees leave one organization for another, taking with them the knowledge of how that particular organization operates, as well as its pricing policies, manufacturing methods, customers, and so on.

Types of Insiders

Insiders can be classified into three categories:

- *Employees*: Employee insiders are employees with rights and access associated with being employed by the organization.
- *Associates*: Insider associates are people with physical access to an organization's facilities, but they are not employees of the organization (e.g., contractors, cleaning crews).
- *Affiliates*: Insider affiliates are individuals connected to pure insiders or insider associates (e.g., spouse, friend, client), and they can use the credentials of the insiders with which they are connected to gain access to an organization's systems or facilities.

Categories of Insider Threats

There are many types of insider threats, and they can be organized into the following categories:

- Traitors
- Zealots
- Spies
- Browsers
- Well-intentioned insiders

Traitors

A *traitor* is a legitimate insider who misuses his insider credentials to facilitate malicious acts. When a trusted insider misuses his privileges to violate a security policy, he becomes a traitor.

Below are some signs that an insider is a traitor:

- Unusual change in work habits
- Seeking out sensitive projects
- Unusual work hours
- Sloppy security habits
- Scoffing or even mocking security policies and procedures
- Rationalizing inappropriate actions

- Changes in lifestyle
- Living beyond his means

Zealots

Zealots are trusted insiders with strong and uncompromising beliefs that clash with their organization's perspectives on certain issues and subjects. Zealots pose a threat because they might exploit their access or inside knowledge in an attempt to "reform" their organizations. Zealots might attempt reform by:

- Exposing their organization to the public by making unauthorized disclosures of information to outsiders or granting access to outsiders
- Destroying information
- Halting services or products

Zealots believe that their actions are just, no matter how much damage they cause.

Spies

A *spy* is an individual who is intentionally placed in a situation or organization to gather intelligence. A well-placed corporate spy can provide intelligence on a target organization's product development, product launches, and organizational developments or changes.

Spies are common in foreign, business, and competitive intelligence efforts.

Browsers

Browsers are insiders who are overtly curious about information for which they do not need access to, knowledge of, or possession of to carry out their work duties. Their curiosity drives them to review data not intended for them.

Browsers might "browse" through information that they have no specific need to know until they find something interesting or something they can use. Browsers might use such information for personal gain, or they might use it for:

- Obtaining awards
- Supporting decisions about promotions
- Understanding contract negotiations
- Gaining a personal advantage over their peers

Browsers can be the hardest insider threat to identify, and they can be even harder to defeat.

Well-Intentioned Insiders

The *well-intentioned insider* is an insider who, through ignorance or laziness, unintentionally fosters security breaches. Well-intentioned insiders might foster security breaches by:

- Disabling anti-virus software
- Installing unapproved software
- Leaving their workstations or facilities unlocked
- Using easy-to-crack passwords
- Failing to shred or destroy sensitive information

While well-intentioned individuals might be stellar employees when it comes to work production, their ignorance or laziness toward information security practices can be disastrous.

Motivations for Insider Attacks

Motivations for insider attacks include:

- Work-related grievances
- Financial gain
- Challenge
- Curiosity
- Spying for competitors
- Revenge
- Ego
- Opportunity
- Ideology (e.g., "I don't like the way my organization conducts business.")

Ways to Combat Insider Threats

There are various ways organizations can combat insider threats. The CERT Insider Threat Center, which conducts comprehensive and authoritative research on insider threats, published The CERT Top 10 List for Winning the Battle Against Insider Threats to help organizations prevent, detect, and respond to malicious insider activity. The 10 mitigation strategies recommended by the CERT team are as follows:

- *Create an insider threat program*. To combat insider threats, management should form an insider threat team, create policies, develop processes and implement controls, and regularly communicate the policies across their organizations.

- *Work together across the organization*. To be successful, efforts to combat insider threats should be communicated across management, IT, data owners, software engineers, general counsel, and human resources.
- *Address employee privacy issues with general counsel.* Because employees have certain privacy rights that can affect numerous contexts involving the employer-employee relationship, and because such rights may stem from, and be protected by, various sources of law, management should consult legal counsel in addressing employee privacy issues.
- *Pay close attention at resignation/termination*. Because leaving an organization is a key issue of concern for insider threats, management should be cautious of underperforming employees, employees at risk of being terminated, and employees who will likely resign.
- *Educate employees regarding potential recruitment*. Management should train employees to exercise due diligence in hiring prospective employees.
- *Recognize concerning behaviors as a potential indicator*. Management must train employees to recognize certain behaviors or characteristics that might indicate employees are committing or are at risk of committing a breach. Common behavioral red flags are living beyond financial means, experiencing financial difficulties, having an uncommonly close relationship with vendors or customers, and demonstrating excessive control over their job responsibilities.
- *Mitigate threats from trusted business partners*. Management should subject their organization's contractors and outsourced organizations to the same security controls, policies, and procedures as their own employees.
- *Use current technologies differently*. Most organizations have implemented technologies to detect network intrusions and other threats originating outside the network perimeter, and organizations with such technologies should use them to detect potential indicators of malicious insider behavior inside the network.
- *Focus on protecting the most valuable assets*. Management should dedicate the most effort to securing the most valuable organizational assets and intellectual property against insider threats.
- *Learn from past incidents*. Past incidents of insider threats and abuse will suggest areas of vulnerability that insiders will likely exploit again.

Additionally, Patrick Reidy, the Chief Information Security Officer at the Federal Bureau of Investigation (FBI), emphasized five strategies for combatting insider threats in a 2013 brief at Black Hat USA:

- Focus on deterrence, not detection. In other words, create a culture that deters any aberrant behavior so that those who continue to practice that behavior stand out from

the "noise" of normal business and the limited investigative resources that can be focused on them.
- Know your people—know who your weak links are and who would be most likely to be a threat. Use your HR data to narrow down threats rather than looking for a needle in a stack of needles.
- Identify information that is most likely to be valuable to someone else and protect it to a greater degree than the rest of your information.
- Monitor ingress and egress points for information (e.g., USB ports, printers, network boundaries).
- Baseline normal activity and look for anomalies.

Other measures organizations can take to combat insider threats include:
- Educate employees as to what information is proprietary and confidential.
- Require that all employees and third-party vendors and contractors sign *nondisclosure agreements*—written agreements providing that all proprietary and confidential information learned during their relationship must be kept confidential and must not be disclosed to anyone—upon the commencement and termination of employment or contracts.
- Ensure that all of an organization's third-party vendors and contractors perform background checks on all employees that will have access to the organization's information systems.
- Prohibit employees, contractors, and trusted business partners from printing sensitive documents that are not required for business purposes.
- If possible, avoid connecting information systems with trusted business partners.

Also, when possible, management should conduct exit interviews with departing employees. During an exit interview, the departing employee should be advised about the organization's trade secrets and confidential information, as well as any obligation not to disclose or use such information for his own benefit or the benefit of others without express written consent. Also, the employee should be given a form to sign stating that he was informed that any proprietary information should not be disclosed and that he agrees not to disclose any such information without consent.

Finally, when management terminates its relationship with an insider, it should immediately deactivate the insider's access to company tools and resources.

Investigating Corporate Espionage

Investigations into corporate espionage activity can be challenging, but this discussion provides some helpful tips. When an organization is the victim of corporate espionage, management should first determine how the sensitive information was compromised. Knowing how the theft occurred often reveals who stole the information.

When management suspects that confidential information has been misappropriated, it should take the following actions:

- Involve legal counsel.
- Consider engaging any outside consultants that are needed to conduct an effective investigation.
- Secure all of the organization's confidential information (e.g., installing physical barriers, limiting users' access to information, changing locks and other controls used to obtain access to information system components).
- Consider whether to report the incident to government authorities.
- Collect and analyze relevant documents.
- Identify employees with access to confidential information, and interview them about their knowledge of the relevant facts.
- Interview non-suspect employees who are responsible for protecting confidential information.
- Interview any third party who might have relevant information.

But more specifically, when investigating corporate espionage, those responsible should determine how the sensitive information was compromised.

To determine how the sensitive information was compromised, investigators should begin by determining whether the incident was the result of negligence, accident, or some procedural matter (e.g., inadequate security controls).

If the investigators determine that the incident was not caused by negligence or accident, they should look for evidence of insider theft. In most corporate espionage investigations, the investigators should begin looking at the people closest to the sensitive information at issue and then work outward. For example, if a company's marketing list was stolen, the investigators should begin with employees who manage the list. The investigators should perform background investigations on these employees, looking for red flags of corporate spies (e.g., unusual recent financial or lifestyle changes, unusual work hours). After

investigating employees closest to the sensitive information, the investigators should move outward to other employees, vendors, customers, and visitors.

If the investigation fails to develop any leads on employees, vendors, or visitors, the investigators should look for signs of an external attack using deception. They should interview employees in the affected areas to find out if they observed any suspicious activities or received any suspicious telephone calls or emails at or near the time of the loss. Also, they should ask employees if anyone has approached them for information.

If an external attack using deception does not appear likely, the investigators should look for evidence of physical penetration. They should review surveillance tapes of traffic in and out of the affected area, and they should ask employees if they remember observing anyone who appeared suspicious. They should check internal records for any incidents of criminal activity on site at or near the time of the loss, and they should review security personnel reports for any suspicious activities (e.g., people trying to get into the trash or loitering in the parking lot).

If, after performing these actions, the investigators still do not know how the sensitive information was compromised, they should look for evidence that the information was misappropriated using some form of electronic surveillance.

Program for Safeguarding Proprietary Information

To prevent the loss or misuse of sensitive data or proprietary information, organizations should develop and implement risk-based information-security systems designed to detect and prevent unauthorized access to sensitive information. An information security system requires controls that are designed to ensure that data is used as intended, and such controls will depend on the combination and coordination of people, processes, technologies, and other resources.

The information security system should be developed and managed by the entity's corporate information officer (CIO), but the entity could also hire a security management consultant to develop the system and maintain it on an annual basis. The CIO should have information management skills and be knowledgeable about trade secret protection.

To be effective, a system for safeguarding sensitive and proprietary information should include the following:

- Task force
- Security risk assessments
- Security policies and procedures
- Awareness training
- Nondisclosure agreements
- Noncompetition agreements
- Data classification
- Data retention and destruction policies
- Data minimization
- Security controls
- Measures to guard manual file systems
- Monitoring of visitor access
- Quiet room

The failure to include any of these measures is a poor information security practice that can contribute to the loss of proprietary information.

Task Force

To coordinate a company-wide program for safeguarding proprietary information, management should establish a task force and charge it with developing the program. The task force should include managers and staff from departments that deal with proprietary information (e.g., staff from the research and development and the production departments). The task force should also include representatives from the following departments: corporate security, human resources, records management, data processing, and legal.

Once the task force is assembled, it must identify the information that is to be protected. To make this determination, the task force should identify those areas that give the company its competitive edge (e.g., quality of the product, service, price, manufacturing technology, marketing, and distribution). When doing so, the task force should ask, "What information would a competitor like to know?"

Once the proprietary information has been identified, the task force should focus on the information security procedures for each department. That is, the task force should identify

where proprietary information is kept and survey the risk if such information was lost to a competitor.

Security Risk Assessments

Organizations' information security programs should feature solutions based upon their individual security risk assessments; therefore, organizations should conduct security risk assessments to identify threats to, and vulnerabilities of, their information systems.

A *security risk assessment* is the process whereby responsible parties identify an organization's security risks, assess the probability that those risks will materialize, calculate the damage that would result if the risks materialized, and determine the costs of applying the necessary safeguards to mitigate the identified risks.

For more information on security risk assessments, see the "Computer and Internet Fraud" chapter in this section of the *Fraud Examiners Manual*.

Security Policies and Procedures

To prevent harm to data, organizations must establish security policies and procedures that protect sensitive information and mitigate risks associated with information security breaches.

Generally, a *security policy* is a document that outlines specific requirements or rules designed to provide information security. Security policies should:

- Contain employee responsibilities.
- Require compliance (i.e., compliance is mandatory).
- Define consequences for compliance failures.

An organization's security policies should reflect management's commitment to information security. Thus, security policies should contain guiding principles that convey management's over-arching beliefs on information security.

Moreover, security policies provide the foundation for security in an organization. They provide a framework that ensures that informational assets are secured within a governing policy.

However, to be effective, security policies must be:

- Implemented and communicated to all employees in an effective manner
- Easy to understand

Effectively communicated information security policies provide employees with guidance on the proper use of information assets, which allows management to mitigate the risks associated with the inappropriate use of computer systems, software, email, and the Internet.

In short, an organization's security policies should state, in writing, what policies and standards must be followed by employees, vendors, and business partners with regard to network and communications security. These policies should outline what must be done, who must do it, and the consequences of not complying.

Also, to help ensure compliance, management should ask every employee to sign an agreement to follow the company's security policies.

In the information security field, security policies are usually topic-specific, covering a single subject. The following is a list of key policies that most organizations need:

- *Information classification policy*: This policy establishes a framework for categorizing information according to the perceived risk to the organization and assigns responsibility for its identification and classification. This policy seeks to ensure that information is properly identified, classified, and handled according to its value, legal requirements, sensitivity, and importance to the organization.
- *Acceptable use policy*: This policy covers the rules establishing the appropriate use of the organization's computer equipment.
- *Minimum access policy*: This policy provides rules based on the principle that individuals should be authorized the minimum amount of access they need to accomplish their job responsibilities.
- *Network access policy*: This policy sets access criteria for all wired and wireless network data ports within any facility owned or operated by the organization.
- *Remote access policy*: This policy outlines and defines acceptable methods of remotely connecting to the organization's internal network.
- *Acceptable encryption policy*: This policy contains standards defining the organization's rules for acceptable encryption.
- *Server security policy*: This policy imposes standards to ensure that basic server security safeguards are used by all server administrators.

- *Extranet policy*: This policy establishes the security requirements and processes pursuant to which users outside the organization, usually partners, vendors, and suppliers, must comply with before connecting to the organization's internal networks.
- *Application service provider policy*: This policy contains the security requirements for the organization's use of software-based services and solutions by any third-party entity that manages and distributes such products and services.
- *Authentication policy*: This policy establishes the rules by which network access is granted to users who request access to the organization's network.
- *Wireless policy*: This policy defines the standards for wireless systems connected to the organization's network.
- *Email security policy*: This policy contains the rules establishing what constitutes acceptable and unacceptable use of the organization's email system.
- *BYOD policy*: This policy establishes the guidelines by which employee-owned devices are allowed to access the organization's networks and systems.

The SANS Institute provides downloadable information security policy templates on its website. For more information, visit www.sans.org.

For more information on security policies, see the "Computer and Internet Fraud" chapter in this section of the *Fraud Examiners Manual*.

Awareness Training

Educating employees is a key part of preventing data from being compromised. Thus, management should give all personnel awareness training so that they know their role in furthering security. Organizations should strive to make sure that employees are aware of the importance of information and data security and are trained to protect sensitive information, and they should ensure that employees at satellite offices, temporary help, seasonal workers, contractors, and vendors are included in the training.

Employees must be educated about what information is proprietary. It is difficult to protect information if no one knows that it needs protecting. For example, employees might know that their employer's secret formula is proprietary, but they might not know that certain topics of discussion are trade secrets that would be valuable to competitors.

EXAMPLE

Daniel Harris worked as an engineer for a software company that was developing insurance claims processing software for the health care industry. While attending a trade association conference, Harris entertained other attendees with war stories about his company's software development process, regaling them with stories about what worked and what didn't work in his company's efforts to develop the new software. Later, Harris was reprimanded for his disclosure, but he was genuinely unaware that the information he provided was proprietary and valuable to his company's competitors.

Moreover, organizations must educate their employees about the dangers of electronic communications and how to protect proprietary information when using such methods of communication.

Employees traveling out of the country should be especially knowledgeable about security controls. Many foreign governments operate huge and sophisticated intelligence-gathering operations. Therefore, when traveling abroad, employees should take precautions under the assumption that any mobile electronic devices, such as laptops, mobile phones, and tablets, will be subject to review. The following are some steps an individual can take when traveling abroad:

- Ensure that the software on all devices is patched and up to date.
- Password- or passcode-protect all devices.
- Minimize the data contained on any devices.
- Avoid using public computers when abroad.

Moreover, leaders should train their employees on common issues and directives addressing how to identify red flags and how to deal with the high-risk issues the employees are likely to encounter, and training should be based on the organization's operations and needs.

Management should also consider providing advanced instructions for personnel assigned to higher-risk areas or responsibilities, and management should update employees as new risks and vulnerabilities are discovered.

In short, security awareness training should cover points such as:

- The organization's information security policies and procedures and the reasons behind such policies and procedures
- The dangers of data breaches

- Real-world examples of how data has been compromised and what could have been done to prevent such instances
- Social engineering awareness
- Techniques that hackers use to access sensitive data
- How to avoid phishing attacks
- Appropriate measures for handling and protecting sensitive data
- Techniques for safeguarding portable data
- Password construction and management
- Tips for secure Web browsing
- The appropriate use of social networking sites
- Guidance on data encryption
- Document and data control
- How to recognize security threats
- Procedures for reporting suspected breaches
- Ways to identify and avoid situations that could lead to data breaches
- Guidance on applicable laws
- Disciplinary measures for violating security policies

Moreover, awareness training should be ongoing, user-friendly, and easily understood. Management should regularly provide reminders about the importance of information security in company newsletters, bulletin boards, memos, and other form of communication. Also, training must be presented in a manner appropriate for the targeted learners. Such approaches will make it more likely that employees will buy into the program, understand it, and appreciate it.

For more information on security policies, see the "Computer and Internet Fraud" chapter in this section of the *Fraud Examiners Manual*.

Nondisclosure Agreements

Management should consider making nondisclosure agreements a mandatory part of their information security programs. Generally, a *nondisclosure agreement* is a written agreement providing that signatories must keep all trade secrets and proprietary information learned during their employment confidential.

Nondisclosure agreements serve the following functions:

- They delineate the confidentiality expectations the employer has for its employees.
- They demonstrate that the employer is serious about protecting trade secrets and proprietary information.
- They show the reasonable efforts that the employer takes to maintain the secrecy of its confidential information.

Nondisclosure agreements should be signed at the outset and upon termination of employment.

Lack of employee education concerning nondisclosure agreements is one of the primary reasons employees communicate confidential information to outside parties. Often, employees are willing to abide by nondisclosure agreements, but they do not understand that the information they are communicating might be confidential. To more effectively implement nondisclosure agreements, employees must be clearly informed as to what information is considered confidential upon hiring, upon signing a nondisclosure agreement, and during exit interviews.

Moreover, everyone involved with the organization should sign nondisclosure agreements. This includes all employees, subcontractors and their employees, clerical staff, consultants, suppliers, distributors, and temporary employees.

Nondisclosure agreements are one of the least expensive and most efficient methods for controlling the loss of proprietary information.

Noncompetition Agreements

Management should consider using noncompetition agreements. A *noncompetition agreement* is an agreement whereby an employee agrees not to work for competing companies within a certain period of time after leaving his current employer.

While noncompetition agreements can be useful in some circumstances, there are a number of legal issues that limit their effectiveness. For example, courts in some jurisdictions have held that such agreements are against public policy because they limit a person's future employment; therefore, in these jurisdictions, noncompetition agreements are unenforceable. Moreover, even in jurisdictions that uphold these agreements, they will only do so if the agreements are part of an otherwise valid employment agreement. That is, the employment

agreement and the noncompetition agreement must be signed at the same time or the noncompetition agreement is unenforceable. Additionally, if the noncompetition agreement is signed by an at-will employee who is not covered by an employment agreement, any noncompetition agreement signed by such an employee would be unenforceable. Furthermore, some noncompetition agreements are drawn in terms of geographic, rather than time, parameters.

Therefore, before instituting a noncompetition agreement, consult with legal counsel to make sure that the agreement is valid and enforceable under the applicable laws.

If an organization uses a noncompetition agreement, management should remind its employees about the agreement's provisions during exit interviews conducted before the end of their employment. When an employee is leaving a company, it is a good idea to have him sign a statement in which he acknowledges that he understands the noncompetition agreement's terms and that he will abide by its provisions. Noncompetition agreements are typically employed along with a nondisclosure agreement, although nondisclosure agreements are not always tied to a noncompetition agreement.

Data Classification

Organizations should have a data classification policy that establishes what protections must be afforded to data of different value and sensitivity levels. Data classification allows organizations to follow a structured approach for establishing appropriate controls for different data categories. Moreover, establishing a data classification policy will help employee awareness.

In short, classifying an organization's data involves:

- Organizing the entity's data into different security levels based on the data's value and sensitivity
- Assigning each level of classification different rules for viewing, editing, and sharing the data

For more information on data classification, see the "Computer and Internet Fraud" chapter in this section of the *Fraud Examiners Manual*.

Data Retention and Destruction Policies

Organizations should implement data retention and destruction policies that detail how information should be created, obtained, used, saved, and stored, as well as how long information should be maintained and when it should be destroyed. Such policies are especially important given the growing amount, locations, and formats of digital information, which create additional risks and costs for companies that do not have such policies in place.

A data retention and destruction policy formalizes the procedures an organization takes to save and destroy documents received or created in the ordinary course of business, and these policies are an important component of any information security program.

Having such policies in place will help organizations:

- Avoid any adverse consequences resulting from failure to preserve information.
- Minimize the amount of data retained.
- Reduce the cost associated with retaining information.
- Improve information security and reduce the risk of data breaches.
- Minimize the amount of information to produce in response to subpoenas.
- Aid in litigation.
- Minimize the risk of destroying documents that should have been retained.
- Reduce the search, retrieval, and production costs of litigation-related discovery.

Accordingly, organizations without retention and destruction policies or with poorly implemented policies face serious risks and consequences. They could face monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of their claims or defenses. Specifically, companies must be aware of preservation and spoliation of evidence. Courts can award sanctions for failing to preserve or mismanaging (spoliation) key documents or data.

Thus, organizations should institute policies and procedures for deciding which documents should be kept and which documents should be deleted.

Data Minimization

Organizations should practice data minimization. *Data minimization* refers to collecting and storing the minimal amount of information necessary to perform a given task. Data minimization is important to data security because thieves cannot steal what an entity does not have.

Data minimization is especially important for personal data. Individual expectations and privacy laws and regulations obligate organizations that collect personal data to maintain data security, and data minimization can be a practical and effective approach for meeting data privacy obligations.

Data minimization has long been enshrined in various privacy principles and related laws. For example, the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which sets out general principles for protecting personal information, contains a collection limitation principle: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." Likewise, the EU *Directive on Personal Data Protection* addresses data minimization in Article 6, which states that personal data must be "collected for specified, explicit and legitimate purposes."

Security Controls

Computer networks and communications are inherently insecure and vulnerable to attack and disruption, and it follows that management must use security controls to protect systems against threats such as unauthorized use, disclosure, modification, destruction, or denial of service.

The objective for securing computer systems and communication networks is to provide connectivity with acceptable response times, user-friendly access, and a secure mode at an acceptable cost to the organization.

Common controls used to secure computer systems and communication networks include:

- Physical access controls (e.g., hiring security guards, using locks, and physical access control devices)
- Logical access controls
- Network security
- Encryption
- Application security
- Separation of duties

For more information on information security controls, see the "Computer and Internet Fraud" chapter in this section of the *Fraud Examiners Manual.*

Measures to Guard Manual File Systems

Organizations must take reasonable measures to protect manual file systems, which are composed of all human-readable files and documents. These include items like contact lists, schedules, and calendars. To attack a manual file system, an information thief might pilfer trash, act as a cleaning crew member, or commit theft or burglary.

Reasonable measures to protect manual file systems include the following:

1. Place sensitive documents in high-grade locked filing cabinets. It might be advisable to lock sensitive documents in a safe when not in use.
2. Use a cross-cut shredder for sensitive documentary waste, or have sensitive trash disposed of by a bonded waste-disposal company.
3. Receive and send mail at a secure site (e.g., mail drops, post office boxes, or locked mailboxes). The key is that the site remains secure.
4. Provide reasonable perimeter security for offices by using an alarm system and securing locks to doors and windows.
5. Pay attention to securing auxiliary materials such as:
   - Calendars
   - Specialized internal telephone directories
   - Notebooks and expense logs from sensitive cases
   - Works in progress, such as reports, notes, and graphics on sensitive cases
   - Mailing lists—all such lists that have proprietary value should have trapped names placed on them as a safeguard. A *trapped name* is a fictitious name with an address that the organization controls. If mail is ever delivered to the trapped name, it will be apparent that the list has been compromised. Furthermore, the nature of the mailing will probably indicate who bought the list, and might help the victim determine where the security breach occurred.
   - Dry erase boards or other meeting room displays that might contain diagrams, charts, or sensitive notes (if such displays cannot be easily locked up, take a photo of them and secure these photographs)
   - Writing tablets that have impressions from notes on sensitive topics (shred them every day)
   - Computer printouts of sensitive data (keep them locked up and use a cross-cut shredder to dispose of them)

Organizations concerned about the possibility of corporate espionage should establish procedures for classifying and marking sensitive items and should have provisions for their

short- and long-term storage, as well as their disposal or destruction. Large offices should have a structured log-out procedure for sensitive files so it is always possible to determine who had what document, as well as where and when they had it.

Monitoring of Visitor Access

Management should monitor and limit visitor access. Visitors should be required to sign in and out of an organization logbook. It is considered a best practice to issue visitors a badge that identifies them as a non-employee. Also, visitors should be escorted by a host at all times, and visitors should not be allowed into areas containing sensitive information.

Similarly, management should designate security personnel or someone to monitor maintenance work done in areas that might contain sensitive information.

Additionally, locks on doors leading to secure areas should be changed or reprogrammed regularly, especially if an employee has recently quit or been terminated.

Quiet Room

Management can prevent corporate spies from listening in on meetings through the use of a quiet room. A *quiet room* is an area that is acoustically and radio-frequency shielded so that conversations that occur within the room cannot be monitored or heard from outside the room.

Minimizing the Risks of Misappropriation Claims

Organizations must also prevent their employees from appropriating the proprietary information belonging to others.

A new hire from a competitor, for example, might expose the new employer to liability by using or disclosing secrets from his previous employer in the course of his employment.

Moreover, a company can be held liable for misappropriation of proprietary information even if it is not aware that its employee is using or disclosing secrets in the course of his employment.

EXAMPLE

Novopharm, Inc. was found guilty of stealing trade secrets from its rival, Apotex, Inc. Court documents stated that a biochemist left Apotex and "secretly joined" Novopharm, bringing with him Apotex's valuable trade secrets. Even though Novopharm's officers claimed that they were not aware that the employee was using Apotex's trade secrets, the court held Novopharm liable, finding that its chief executive officer "closed his eyes to what was going on around him."

Management can take various actions to prevent misappropriation by its employees. For one thing, management should carefully screen potential employees during the hiring process. They should seek to determine the potential employee's knowledge about another party's trade secrets, and they should learn about any restrictions on employment. Human resources personnel should ask potential employees whether they are subject to any agreements that bar them from competing with any current or former employer. If the employee is subject to any such agreement, legal counsel should review the agreement before any hiring decision is made.

For another thing, management should conduct new hire training on the importance of protecting information assets.

FINANCIAL INSTITUTION FRAUD

External fraud schemes are those committed by outside organizations, typically by individuals or groups of individuals against organizations. Fraud schemes committed by outsiders usually occur within specific industries. Therefore, the following chapters are organized by type of industry, starting with financial institution frauds. Because some schemes are committed by collusion between an organizational insider and an outsider, some frauds can be classified as both internal and external schemes.

Financial institutions include banks, savings and loans, credit unions, and other governmentally insured repositories. Financial institution fraud is also known by the more generic term of *bank fraud*. Check fraud and credit card fraud, as applied to both merchants and financial institutions, are discussed in the "Check and Credit Card Fraud" chapter.

A *bank* is defined as an organization engaged in any or all of many financial functions, such as receiving, collecting, transferring, paying, lending, investing, dealing, exchanging, and servicing (via safe deposit, custodianship, agency, or trusteeship) money and claims to money, both domestically and internationally.

Embezzlement Schemes

Embezzlement is defined as the wrongful taking or conversion of the property of another by a person to whom it has been lawfully entrusted (or to whom lawful possession was given). *Misapplication of bank funds* is a type of embezzlement in which bank employees wrongfully take or convert another party's property for the benefit of the employee or someone else.

Types of Embezzlement Schemes

There are various embezzlement schemes that have been used over time against financial institutions and their customers. The following examples are not an exhaustive list, but are rather a summary of the more commonly employed schemes.

False Accounting Entries

Some employees are in positions of trust in which they have the ability to use or relocate funds on behalf of customers or the financial institution itself. In false accounting entry schemes, employees debit the general ledger to credit their own accounts or cover up a theft from a customer account.

Suspense Account Schemes

A *suspense account* refers to the section of an organization's books where unclassified debits and credits are recorded. Placing an entry in a suspense account is designed to be a temporary measure, pending the ultimate disposition of the transaction. Employees often use suspense accounts to perpetrate fraud against their employer at both financial institutions and other types of organizations. However, financial institutions make heavy use of various types of suspense accounts, making such schemes a unique fraud risk in this industry.

In a suspense account scheme, the employee makes a fictitious debit entry to a suspense account and offsets the entry with a credit to an end point—a means to remove funds from the financial institution—under the control of the individual (e.g., a checking account, an official check account, or a wire account). These entries are continuously cleared by future, and often increasingly large, fictitious debit entries (similar to a lapping scheme). There are several types of suspense accounts at financial institutions that fraudsters might use, including:

- Loans in process
- Interdepartmental transfers
- Currency in transit
- Refunds on insufficient funds charges
- Due from banks

False or Unauthorized Transfers from Internal Accounts

There are several types of normal transfers using internal accounts, especially in operating account and general ledger account transactions. A person with the ability to make such transactions might substitute a personal account for one of the internal accounts.

Unauthorized Withdrawals

In a relatively simple scheme, employees make unauthorized withdrawals from customer accounts. These schemes are hard to conceal because the customer will complain, but the subject might plan to flee once the funds are transferred or target a customer who is unlikely to notice the missing funds right away.

Unauthorized Disbursement of Funds to Outsiders

Additionally, employees might abuse their authority to approve fraudulent (counterfeit, forged, stolen, etc.) instruments or otherwise make an unauthorized disbursement of funds

to an outsider. While the employee often has a financial incentive for doing so, there have been many cases where the employee made an improper disbursement in a misguided attempt to be cooperative with customers.

Paying Personal Expenses from Bank Funds

An officer or employee causes the bank to pay personal bills and then causes amounts to be charged to bank expense accounts.

Theft of Physical Property

Employees or contractors remove office equipment, building materials, and furnishings from bank premises.

Moving Money from Customers' Dormant or Inactive Accounts

Persons with apparent authority create journal entries or transfer orders not initiated by customers to move money among accounts. The accounts used are typically *dormant* or *inactive* accounts, which are those accounts that show little or no activity. Often, contact with the account holder by confirmation, letter, or telephone is not possible. Such accounts are to be transferred to dual control and recorded in an inactive accounts ledger.

Dormant funds are highly susceptible to embezzlement. The rationale is that funds embezzled from active accounts are likely to be missed quickly, while dormant account holders are less likely to report problems. Many financial institutions lock dormant accounts after a certain time period (e.g., one year of inactivity), requiring manual override to conduct additional transactions. However, this process can be manipulated. Typically, the perpetrator first identifies accounts that are or are about to be dormant. Next, he might somehow manipulate the account to make it appear that it is not dormant, such as by creating a nominal and fictitious transaction. Then, the employee creates journal entries or transfer orders to move the funds into an account that the employee controls (often a shell organization).

Unauthorized, Unrecorded Cash Payments

A director, officer, or employee causes cash to be disbursed directly to himself or accomplices and does not record the disbursements.

Theft and Other Unauthorized Use of Collateral

Custodians steal, sell, or use collateral or repossessed property for themselves or accomplices.

Skimming of Irregular Receivables

As with any organization, a financial institution's receivables are vulnerable to skimming schemes in which the fraudster intercepts incoming payments before they are entered into the institution's books. The nature of financial accounts creates some unique risks due to the relatively large proportion of irregular accounts receivable. Receivables that are long past due or that have already have been written off are prime targets for fraudsters because no one is surprised when those funds never show up in the books.

Detection Methods

There are several methods by which embezzlement can be detected. Generally, if the dollar amount of the embezzlement scheme is small enough such that the financial statements will not be materially affected, embezzlement fraud can be most effectively detected through the review of source documents (e.g., receipts, deposit slips). There can be many types of clues in the source documents, and often the particular situation will determine what the fraud examiner needs to look for. The following are common red flags in source documents that might indicate that embezzlement has occurred:

- Missing source documents
- Payees on source documents (e.g., checks) do not match entries in the general ledger
- Receipts or invoices lack professional quality
- Duplicate payment documents
- Payee identification information that matches an employee's information or that of his relatives
- Apparent signs of alteration to source documents
- Lack of original source documents (photocopies only)

If the scheme is so large that the institution's financial statements are affected, then a review of the source documents will serve to confirm or refute an allegation that an embezzlement scheme has occurred or is occurring. Generally, for large embezzlements, the most efficient method of detection is an analysis of the financial statements (which is also a review of documents). Some common suspicious items in financial statements are:

- An abnormal increase in accounts receivables that are past due or written off
- Master accounts that do not equal the sum of their individual customer accounts

- Excessive voids or credits
- An abnormal increase in reconciling items

Many embezzlement frauds are detected when the financial institution regularly conducts reconciliation. It is also important to conduct independent review of high-risk accounts, such as new customer accounts and suspense accounts.

Loan Fraud

Loan fraud is a multifaceted activity that includes several types of criminal activities. Larger loan fraud schemes often involve real estate lending and collusion between insiders and outsiders. Loan fraud represents the highest risk area for financial institutions. Although the number of occurrences might be small, the dollar amount per occurrence tends to be large.

Common Loan Fraud Schemes

Loans to Nonexistent Borrowers

False applications, perhaps with inaccurate financial statements, are knowingly or unknowingly accepted by loan officers as the basis for loans. These types of loan fraud can be perpetrated by people either external to the lending institution ("external fraud") or by officers, directors, or employees of the victim institution ("internal fraud").

Sham Loans with Kickbacks and Diversion

Loan officers will sometimes make loans to accomplices, who then share all or part of the proceeds with the lending officer. In some instances, the loans are charged off as bad debts; in other instances, the bogus loans are paid off with the proceeds of new fraudulent loans.

Double-Pledging Collateral

Borrowers pledge the same collateral with different lenders before liens are recorded and without telling the lenders.

Reciprocal Loan Arrangements

Insiders in different banks cause their banks to lend funds or sell loans to other banks with agreements to buy their loans—all for the purpose of concealing loans and sales.

Swapping Bad Loans—Daisy Chains

In a daisy chain, a bank buys, sells, and swaps its bad loans for the bad loans of another bank, creating new documentation in the process. Its purpose is to mask or hide bad loans by making them look like they are recent and good.

Linked Financing

Large deposits (usually brokered deposits) are offered to a bank on the condition that loans are made to particular individuals affiliated with the deposit broker. High returns are promised, but the loans are of a longer term than the deposits (hot money). Sometimes kickbacks are paid to the broker or banker.

Loan Applications with False Credit Information

Sometimes loan applicants provide false information about their credit situation and/or overstate their assets.

Credit Data Blocking

In some countries, financial institutions largely rely on credit reports to determine whether to extend credit to customers. Fraudsters might attempt to manipulate these reports in order to receive loans that they otherwise could not. In a credit data blocking scheme, the perpetrator first applies for and obtains loans for property, vehicles, etc., but intentionally defaults on them. Rather than allowing his credit report to reflect the defaulted loans, the perpetrator asserts that the initial loans were instances of identity theft. While the validity of the fraud claims are being checked, the perpetrator's negative credit history is temporarily removed from his credit report. This allows the perpetrator to take out more loans, which he will also intentionally default on.

Single-Family Housing Loan Fraud

In this scheme, unqualified borrowers misrepresent personal creditworthiness, overstate ability to pay, and misrepresent characteristics of the housing unit. Such acts might include reporting inflated income, moving debt into a dependent's name, reporting inflated square footage of the collateral, or even bribing an appraiser to value the home at a higher amount than the market value.

Construction Loans

Construction lending has different vulnerabilities than other permanent or interim lending. More risks are associated with construction projects than with already-built projects.

Construction loan fraud schemes are numerous; the more common ones are related to estimates of costs to complete, developer overhead, draw requests, and retainage/holdback schemes.

ESTIMATES OF COSTS TO COMPLETE

When borrowers approach a lending institution for construction financing, they typically have a development plan, complete with an engineering report, appraisal, and budget for construction costs. The construction cost budget is, by definition, an estimate. As the project is built out, the budget will be revised to reflect actual expenses. Budgets are delineated by specific line item, such as slab, exterior glass, grading, landscaping, and tenant improvements. As the project proceeds, certain over- and under-budget costs are incurred. These costs should be represented by a change order.

If the loan agreement has been properly documented and enforced, no material differentiation from the budget should occur without the lender's knowledge and consent. However, the developer/borrower might misrepresent the true nature of the under- or over-budget amount to mislead the lender. The architect/engineer and the lender's inspector should examine all budget changes. The impact of change orders might result in the loan becoming out of balance (cost to complete exceeds available loan and equity funds). Generally, developers hide or conceal their over-budget construction costs in two common places. The first place is contingency and the second is to remove allocations from tenant improvements and apply them to shell construction.

Most budgets contain a contingency line item in the event actual costs exceed the budgeted amounts. Unfortunately, many developers and lenders do not monitor the total impact on removing allocations from the contingency budget. In addition, savings are not allocated to the contingency line item when under-budget costs are realized. It is also common to rob one account to make up for a shortfall in another account. Generally, tenant finish is estimated at a particular dollar amount per square foot. This allows the developer considerable latitude in negotiating with tenants.

However, before the entire space has been leased and the construction costs have been incurred, the amount allocated to tenant improvements remains budgetary. If the developer is allowed to reallocate amounts from this budget line to shell construction, then when it comes time to negotiate leases and finish out the space, the developer might be short of available funds. If the tenant finish is treated as a hold-back and not to be reallocated or

disbursed except for its intended purpose, then there is a greater chance of the loan not becoming over-disbursed (cost to complete exceeding the available financing).

DEVELOPER OVERHEAD

It is not uncommon in construction financing to have a budget line item for developer overhead (also called *general conditions*). This is a ripe area for abuse. The purpose of developer overhead is to supply the developer with operating capital while the project is under construction. This overhead allocation should not include a profit percentage, as the developer realizes profit upon completion.

In essence, the overhead budget is as if the lender is making two types of loans: a real estate loan and a working capital loan for the overhead. Unfortunately, there is seldom, if ever, any separate underwriting for the overhead portion. The overhead is merely added as a construction cost, whose ultimate collateral is the property and not some other short-term collateral. Historically, troubled construction loans or foreclosures due to fraud have been totally disbursed in the developer overhead category.

DRAW REQUESTS

Construction loan advances are generally supported by draw requests. A draw request is the documentation substantiating that a developer has incurred the appropriate construction expenses and is now seeking reimbursement or direct payment. A typical fraud scheme in this area involves requesting advances on the loan for inappropriate costs, such as personal expenses and/or construction costs for an unrelated project. Draw requests provide the greatest opportunity for a developer to commit fraud against the lender because the lender relies upon the developer's documentation.

Generally, a draw request or pay application is made once a month and is verified by a quantity surveyor (QS) or other authorized entity as agreed to by the financial institution. The request should be accompanied by the following documents:

- Paid invoices for raw materials
- Lien releases from each subcontractor
- Inspection reports
- Canceled checks from previous draw requests
- Bank reconciliation for construction draw account for previous month
- Loan balancing form, demonstrating that the loan remains in balance
- Change orders, if applicable

- Wiring instructions, if applicable
- Proof of developer contribution, if applicable

The documentation required as support for each draw request will vary depending on the payment method (such as direct, dual payment, disbursing agent, wire transfer, or reimbursement). Any missing or altered documentation is a red flag that something is amiss with the draw request. All advances on the loan should be adequately documented.

Some or all of the following steps should be performed before advancing funds on a construction loan. These steps are not represented as being all-inclusive, but rather the preliminary disbursement questions that the disbursing party should address.

- Examine the draw and determine if sufficient supporting documentation has been submitted.
- Reconcile the amounts requested with the approved budget. Account for any differences.
- Determine that the amounts requested have been properly inspected and approved.
- Determine if the proper lien releases have been submitted for work performed.
- Reconcile any change orders with the approved budget. Determine if the change orders have been approved.
- Prove the clerical accuracy of the documentation submitted.
- Ensure that work completed has been inspected by the lender's architect/engineer.
- Determine if there are any requests for soft (nonconstruction) costs and whether they are appropriate.
- Determine if there are any budget changes. If so, what are they for? Have they been approved?
- Prepare a cost-to-complete estimate to determine that the loan remains in balance.
- If tenant improvement funds have been requested, establish that there is a signed lease on file. Is the request appropriate for the terms and conditions of the lease? Has the lease been approved?
- If homeowner option funds have been requested, establish that there is a signed purchase contract on file. Is the request appropriate for the terms and conditions of the contract? Has the contract/purchaser been approved?
- Examine payment requests and determine if there are new or previously undisclosed subcontractors. If so, determine why.
- Ensure that the title update has been received.

RETAINAGE

The final area of major concern in construction lending is retainage (sometimes called the holdback). Retainage is the amount withheld from each draw request until such time as the construction is complete and the lien period has expired. There are at least two reasons why construction loans contain a retainage provision. The first reason is to keep the contractor's interest in the project until all the work has been completed and accepted by the owner. The amount of the retainage represents part, if not all, of the contractor's profit. Therefore, if the profit is not paid until the project has been completed, then presumably the contractor will complete the assignment on time and on budget.

The second reason for the retainage is to ensure that the work of subcontractors is completed and that the general contractor pays the subcontractor so that no liens are filed. If the general contractor fails to pay the subcontractor, then the subcontractor will probably file a lien on the project. If the retainage will not be released until such time as the lien period has expired, then there are at least some funds available to defray the cost of fighting the lien or making a duplicate payment because the general contractor might have embezzled the first payment without paying the subcontractor.

Loan Collateral Sold Out of Trust

Many loans are secured by the property purchased with the loan proceeds—houses, vehicles, business inventory, etc. Usually, the borrower is not authorized to sell the loan collateral without the lender's permission or without paying the lender the proceeds. However, the borrower might sell the property "out of trust," meaning he sells it without informing or obtaining authorization from the financial institution. Often, the financial institution does not discover the illicit sale until the borrower defaults, and there is no collateral to recover. These schemes are especially common with loans for rental equipment that is sold out of trust.

Red Flags of Loan Fraud

There are several red flags of loan fraud. Many times the schemes are perpetrated in tandem with other schemes, so what appears to be a red flag for one scheme might in fact lead the fraud examiner to one or more schemes.

Nonperforming Loans

A *nonperforming loan* is a loan that is in default or close to being in default. The interest and principal payments might be overdue, and the creditor has reason to believe the loan will not be collected in full. This is often indicative of a fraud scheme.

Fraud schemes resulting in a nonperforming loan include:

- *Fraudulent appraisals*—The cash flow cannot support an inflated loan and resulting debt amount.
- *False statements*—The loan was made on false or fraudulently presented assumptions.
- *Equity skimming*—The borrower never intended to make the underlying loan payments.
- *Construction over-budget items*—The over-budget amount might be a concealment method for other schemes such as embezzlement, misappropriation, or false statements.
- *Bribery*—The loan was made because the lender received a bribe or a kickback from the borrower.
- *Land flips*—The purpose of the loan was to finance the seller out of a property that has an artificially inflated value.
- *Disguised transactions*—The loans are sham transactions, without substance, made to conceal other ills.

High Turnover in Developer's Personnel

One of the first signs to look for, particularly in construction lending, is whether the real estate developer is experiencing a higher-than-normal employee turnover. Typically, when a developer experiences a high degree of turnover, something is wrong with the internal operation. This is often a preamble for other problems to come.

High Turnover in Tenant Mix

If the tenant mix in a commercial project (such as a retail center or an office building) is suddenly undergoing a major change, there might be some problem with the management of the project or with the method of allocating the pass-through expenses, such as utilities or maintenance. In addition, a decline in the tenant mix might be an indication that the deferred maintenance for the project is not being properly attended to.

Change Order Abuse

In the course of many projects, such as road repair or building construction, unanticipated changes in conditions can result in the parties agreeing to amend the contract terms after signing, perhaps to increase their scope or cost. This is known as a *change order*.

Change orders can have the same impact on a project as altering the original documents. As with anything that is contracted for on a bid basis, change orders could also be an indication of collusive bidding. A common change order abuse scenario involves collusion between the contractor and personnel from the procuring entity. The corrupt contractor submits an artificially low bid to ensure that he is awarded the contract (often with inside knowledge of competing bid amounts), but after the procuring entity awards the contract, the corrupt contractor increases the contract price with subsequent change orders. Furthermore, change orders might be an indication that the original project was not feasible and that shortcuts are shoring up other problem areas. Change orders should be approved by the architect and engineer on the project in addition to the lender's inspector.

Loan fraud schemes involving project management often involve the use of change orders, so it is important to be able to recognize red flags in this area. The necessity for change orders can vary widely, depending on the type of project. Ultimately, the key characteristic that the fraud examiner should look for in change orders is abnormality, which can come in many forms.

Change orders are often submitted along with draw requests. Although many times the change orders represent legitimate construction changes (for design, cost, or other things), they can also be indicators of fraud schemes. An increasing trend in the number of change orders or amounts on change orders might be an indication that construction changes have taken place that would alter the originally planned project to such an extent as to render the underwriting inappropriate.

Alternatively, some projects—especially large projects—tend to have many change orders. It might be more abnormal in situations like these to have few change orders or none at all than to have many. For instance, a lack of change orders for a large project might suggest that progress is not actually being made. Fraud examiners should discover what the normal trend for change orders is in terms of both quantity and content with the particular type of industry and project, and then they can look for deviations from those trends.

Change orders generally receive less scrutiny than the process used to acquire the underlying contract, making them a popular way to fraudulently access funds or generate funds for kickbacks. Even though change orders are often inevitable and can develop for legitimate reasons (e.g., change in scope, weather delays, building code changes), fraud examiners should view all contract change orders carefully.

Missing Documentation

Missing or altered documentation is a red flag for any type of fraud scheme. Because concealment is a key fraud element, missing documents are a definite giveaway. Missing documents are of particular concern in construction lending. Experience has shown that most complete draw requests have some missing document, which can complicate the detection of fraud.

LOAN FILE

Missing documents in the loan file are another cause for concern. It is important to determine if missing documents have been misplaced or were never received. A waiver of certain documents is one common way for lenders to conceal fraud schemes. Documentation for real estate loans is fairly standard. The following are some of the more important documents that should be present in the loan files:

- Appraisal
- Architect's or engineer's report
- Assignment of leases and rents
- Assignment of limited partnership notes
- Assignment of take-out commitment
- Availability of utilities (water, sewer, gas, and electric)
- Budget
- Completion schedule
- Copies of leases (existing or, if project is preleased, commitment letters)
- Disburser's notice, if required
- Easements
- Environmental impact study
- Ingress and egress
- Inspection report (lender's inspector)
- Insurance binder (lender should be loss payee)
- Legal opinion letter
- Letters of credit, if applicable
- List of general contractors and subcontractors
- Loan agreement
- Plans and specifications
- Promissory notes from limited partners to partnership, if applicable
- Road dedications
- Soils report

- Subscription agreements, similar to limited partnership notes, if applicable
- Survey
- Take-out commitment, if applicable
- Title policy, including instruction letter from closing
- Zoning

DISBURSEMENT FILE

- Copies of all checks issued at closing
- Lien releases issued at closing (architect, engineers, etc.)
- Loan closing statement

DRAW REQUESTS

- Bank reconciliation (general contractor disbursement account)
- Canceled checks (if general contractor pays subcontractors, copies of the canceled checks should be included in the following draw)
- Inspection report (lender's inspector)
- Lien releases for each subcontractor for the previous draw
- Loan balancing form (The lender should prepare some form of reconciliation to ensure that the loan remains in balance with each draw. Items of particular concern are interest, tenant finish, and retainage.)
- Receipts (for all items submitted on the draw request form)
- Title updates from the title company
- Wire transfer instructions (from the lender to the general contractor's disbursement account)

In addition to the normal loan files, the lender should require a continuing report from the borrower. For example, the borrower could be required to report its annual financial condition coupled with a tax return. Missing documents in these follow-up files might indicate that the project or the borrower is having difficulty that might be the result of a fraud scheme.

Loan Increases or Extensions, Replacement Loans

Simultaneous loan extensions and loan increases might indicate that the real estate project cannot support the debt service. Typically, the loan increases are to pay for the interest and extension fee. This red flag might also indicate that the loan was made to a related party or

made as a loan to hasten a sale or other transaction. In other words, the loan was not properly underwritten.

If the loan is increased and extended several times, it might indicate that higher appraisals are being obtained on a "made-as-instructed" basis. Loan increases and extensions might be the method used by the lender to conceal a nonperforming loan.

However, according to William T. Thornhill, CFE, a consultant in the field of financial institution fraud, fraud perpetrators tend to write a new loan or credit facility to *replace* an existing or old loan because they are aware of the fact that a rewrite might attract loan review, loan administration, or internal audit attention. Accordingly, replacement loans are now increasingly used rather than a simple rewrite of a loan.

Cash Flow Deficiencies

The actual cash flow of a commercial project is a very telling red flag. If the project is experiencing an unexplained cash flow deficiency, then an internal fraud scheme might be the cause. The project cash flow might reflect any of the previously mentioned schemes.

Change in Ownership Makeup

A change in the ownership makeup, commonly referred to as business divorce, might indicate fraudulent activity. It is not uncommon to have a working partner and an equity (money) partner. When the two partners become disenchanted with their relationship and seek a "separation," it might suggest things have gone sour.

Disguised Transactions

Transactions disguised to conceal their true nature often involve the lender and either an existing customer or new customer. Banking personnel will sometimes engage in fraudulent schemes to forego the requirement to record additional loan loss reserves. One method employed is to "sell" OREO (Other Real Estate Owned) property to an existing customer or a new customer in exchange for making a new loan on another unrelated project. In other words, the bank is tying one transaction to another, quid pro quo.

Another method of concealing a transaction's true nature is to conduct the transaction through nominees. For example, the bank might be required to recognize an additional loan loss reserve due to the lack of performance on a particular loan. The borrower might or might not be a good customer of the bank. Regardless of the customer's status, the bank

might request that the project (underlying collateral) be sold to another party, with the financing to be arranged by the bank. The borrower can form a new entity (nominee or shell company) to purchase the property; a new (generally higher) appraisal is obtained and the property is sold. In this illustration, the avoidance of loss required the participation of the bank personnel, the borrower, and the appraiser.

Real Estate Fraud

Losses reported by financial institutions across the globe are in the billions of dollars. Most financial institutions invest heavily in real estate transactions; a substantial portion of these losses relate to real estate fraud. Generally defined, *real estate fraud* is any false representation, coupled with intent to deceive, made in connection with a real estate transaction**.** There are several real estate fraud schemes that will be examined below, including the real estate loan fraud schemes discussed previously. In addition, there has been a recent growth of mortgage fraud-related incidences due to the rise of subprime lending and the mortgage crisis.

Most real estate transactions require more money than any single individual or entity can provide themselves. Therefore, most of these transactions must be wholly or partially financed. Because these transactions require borrowed money, experts such as appraisers, lenders, and auditors are needed.

Loan Falsifications

It is illegal to provide false documents to verify income or assets, to make misrepresentations in a loan application, and to knowingly process a false loan application. Common types of loan falsifications include altered bank statements, altered or fraudulent earnings documentation, fraudulent letters of credit, fabricated letters of gift, misrepresentation of employment, misrepresentation of loan purpose, altered credit scores, false government identification numbers (e.g., Social Security number, national insurance number), failure to fully disclose borrower's debts or assets, and brokers using the identities of prior customers to obtain loans for customers unable to qualify.

The following red flags might identify mortgages containing false or misleading information:

- An item other than cash is used for the down payment (i.e., gift, rent credit, sale of personal property, repayment of loan)
- Borrower purchasing property from employer or landlord
- Borrower has a non-purchasing spouse

- Borrower purchasing investment property does not own current residence
- New home is too small for proposed occupants
- The only listing of employer's address is a post office box
- Borrower, who is purchasing private residence property, has an unreasonable commute from the subject property to his employment
- Borrower's level of education is inconsistent with employment
- Borrower's age is inconsistent with the stated employment or the number of years employed
- Borrower is self-employed or his office phone number is the same as his work number
- When compared, borrower's assets and liabilities are inconsistent
- Buyer is downgrading
- Loan application or appraisal is handwritten or incomplete

Forged Documents

Since tax documents, bank statements, title commitments, leases, and similar documents other than the loan application are used to verify income and asset information, such documents are routinely falsified, altered, or forged to perpetuate mortgage fraud schemes.

Appraisal Fraud

The Role of the Appraiser

The appraiser performs an independent property valuation for the new (or old) owner. The regulated real estate associations impose licensing requirements for appraisers. There are several professional associations for real estate appraisers. It is important, particularly in regard to complex commercial property, that the appraisers' experience and credentials be carefully scrutinized.

Fundamentals of Real Estate Appraisals

Real estate transactions assume a willing buyer and a willing seller. Fraud can occur when the transaction breaks down or the expert assistance is not at arm's length. Many fraud schemes have a false appraisal report as a condition precedent. Several different kinds of reports are used by appraisers. They are summarized here.

LETTER FORM REPORT

The letter form report is used when a client is familiar with the area, and supporting data, therefore, is not necessary. The report consists of a brief description of the property, the type of value sought, the purpose served by the appraisal, the date of value, the value

conclusion, and the signature of the appraiser. This form generally is not used by financial institutions for credit decisions.

SHORT FORM REPORT

The short form report is used by financial institutions, usually for residential real estate loans (sometimes referred to as consumer loans). The report varies from one to four pages and consists of check sheets or spaces to be filled in by the appraiser about pertinent property data.

NARRATIVE REPORT

The narrative form includes all pertinent information about the area and the subject property, as well as the rationale for the estimated value. It includes maps, photographs, charts, and plot plans. Financial institutions use narrative reports to support real estate lending and investment decisions on large commercial real estate transactions. Any other type of appraisal report (i.e., letter form or short form) on these complex transactions would likely be considered inadequate.

Determining "Value"

Value is composed of four elements: utility, scarcity, demand, and transferability. Real estate appraisals assign three types of values to property. They are as follows.

FAIR MARKET VALUE

This is the estimated price the property would bring if freely offered on the open market with both a willing seller and a willing buyer.

SALES PRICE

Sales price is the actual price paid for the property. It might be higher or lower than fair market value.

LOAN VALUE

Loan value is the percentage of a property's value (fair market value or sales price) a lender can or might loan a borrower.

Valuation Methods

SALES COMPARISON APPROACH

The sales comparison approach lends itself to the appraisal of land, residences, and other types of improvements that exhibit a high degree of similarity, and where a ready market exists. Compared to the other approaches, this method has great influence on residential portfolio valuations. This method is the least complicated to understand and apply.

Subject property is compared with similar property that is either offered for sale or has recently sold. Items evaluated include time of sale, location of sale (or offer for sale), physical characteristics, and improvements. Adjustments are made to the value of comparable properties (either plus or minus) on the basis of differences between them and the subject property. Relevant items might be an oversized lot, a view, a busy street, or access.

THE COST APPROACH

The cost approach generally does not exert much influence on the appraiser's final value estimate. It serves as a "benchmark" against which the sales comparison and income approaches are measured. The cost approach is more accurate for new properties. It views the value of a parcel as the combination of the land value if vacant and the cost to construct a new building on the given date, less the accrued depreciation the existing building would suffer in comparison with the new building.

The cost approach has five steps:

- Estimate the land value as though vacant and available for development to its highest and best use. (Use the sales comparison approach.)
- Estimate the replacement or reproduction cost of the existing improvements as of the appraisal date.
- Estimate the accrued depreciation amount suffered by the improvements from all causes (physical deterioration and/or functional or external obsolescence).
- Deduct the accrued depreciation from the replacement cost to find the estimate of value of the depreciated improvements.
- Add the improvements' depreciated value to the land value to arrive at the value of the property.

This is the most frequently used cost approach method. It involves the cost associated with rebuilding with modern methods, design, and materials that would most exactly replace the existing building. Reproduction cost is a cost approach used to estimate the cost to

reconstruct a replica of the building. It is generally used only when dealing with unique construction or for testimony in court.

THE INCOME CAPITALIZATION APPROACH

Under this approach, the property value is based on its capacity to continue producing income. This method is particularly valuable for the valuation of complex commercial properties. The net income the property produces is an important consideration. Net income is the amount of money over the remaining life of the property and its improvements that a fully informed person, using good management, is warranted in receiving.

Income capitalization is the mathematical process of estimating the present value of income property based on the anticipated annual net income it will produce. Key to the application of this approach is the capitalization rate that is used. There are three types of capitalization rates: *interest rate, recapture rate,* and *overall capitalization rate.* Interest rate is the rate of return earned on investment capital. Recapture rate is the rate of return originally invested funds provided the owner. Overall capitalization rate is a combination of the interest and recapture rates.

Fraudulent Appraisals

Fraudulent appraisals result from any number of situations, some of which are:

- Intentional use of an incompetent appraiser
- Giving the appraiser improper or false assumptions to use in arriving at the value, such as:
  - Assuming zoning will be changed for a higher and better use when in fact zoning will not be changed
  - Assuming unrealistically low vacancy and expense rates (or unrealistically high vacancy and expense rates for a short sale)
  - Assuming unrealistically high income, selling prices, or absorption—the rate at which vacant space will become rented
  - Otherwise influencing the appraiser—for example, paying above-market fee or promising future business
  - Direct collusion with the appraiser to commit fraud

Uses for Fraudulent Appraisals

There are several reasons that fraudsters might fabricate or falsify appraisals, including:

- To obtain approval on marginal or substandard loans to attain or exceed goals in order to be promoted or receive a commission, bonus, or raise
- To justify extending or renewing a "bad" loan to avoid recognition of a loss that might defer commission, promotion, bonus, or raises
- To avoid adverse publicity and regulatory, management, and shareholder disapproval because of excessive losses
- To avoid recognition of a loss on real estate owned and to permit additional capital infusions
- To criminally gain money

Red Flags of "Made-as-Instructed" Appraisals

Fraud examiners should look for common indicators that an appraisal was performed fraudulently or by parties who were not at arm's-length:

- The appraiser used has never been used before, is not on an approved list, has no professional credentials, or those offered are of questionable credibility.
- The appraisal fee is unusually high.
- Invalid comparables are used.
- Supporting information is missing, insufficient, or contradictory.
- Market data does not support the price and absorption figures used to arrive at value.

Detecting Fraudulent Appraisals

To detect unrealistic or bogus appraisals, the fraud examiner should address the following:

1. Read the appraisal. Does it match the documents in the file?
   - Leases
   - Comparables
   - Absorption rates
   - Residual values
   - Capitalization rate
   - Legal description
2. Is there sufficient demand for the project to ensure absorption of the property into the marketplace?
3. Are there unique characteristics of the project that will ensure a competitive advantage over other projects?
4. Is the project sensitive to changes in local economic conditions?

Mortgage Fraud

Fraud has always been present in the mortgage industry, as it readily adapts to economic changes and modifications in lending practices. The economic recession of 2008 and the related subprime mortgage crisis, which resulted in the collapse of several major financial institutions, the enactment of significant financial reform legislation, and the adoption of austerity programs in many European countries, has only exacerbated the problem. The housing market after the recession has been slow to recover in many parts of the world, leading many governments to adopt programs to make it easier for banks to create more mortgages. Of course, these programs also make various fraud schemes available to criminals.

Emerging Fraud Schemes

BUILDER BAILOUT

A builder bailout scheme flourishes in a downturned economy. It usually occurs when a builder is left with stagnant inventory. The builder might be suffering from financial difficulties with these lingering homes and might need to sell them quickly to pay off delinquent debts. To dispose of the remaining properties, the builder might undertake a variety of schemes that could include, but are not limited to, the use of hidden seller financing and inflated property values. This scheme is also unfolding in the condo-conversion market, in which developers converted apartment buildings into condos at the same time the market turned and fell behind in debts owed. This scheme might not produce any ill-gotten gains to the builder, but the builder is able to unload his inventory and pay off his debt.

Some builders include lavish incentives in the transaction to lure buyers. Such incentives usually involve a form of down-payment assistance so that a borrower can purchase a home without any equity contribution. Other concessions or incentives that might be offered to potential buyers include managing the properties as income-generating investment properties, absorbing any negative cash flow for the first 12–36 months, guaranteeing mortgage payments for the first 12–36 months, or providing other turnkey services and guarantees even though the properties might remain vacant. Builders might also agree to pay the buyer a substantial rebate that is not disclosed to the lender.

Getting concessions from the seller is common and is not necessarily fraudulent. The simple test to determine whether the transaction might be fraudulent is to ask: Are these concessions disclosed, and have they been approved by the lender?

Some builders engaging in builder bailout schemes find marginal, legitimate buyers whose intent is to occupy the property and make the payments. These schemes typically involve some form of undisclosed down-payment assistance. Other builders seek straw borrowers who are often induced with no-risk investment property ownership.

EXAMPLE OF A BUILDER BAILOUT SCHEME

A builder bailout scheme might unfold like this:

- The builder (or third party) recruits a straw borrower to purchase the property for no money down and cash back at closing.
- The builder obtains an inflated appraisal that is used as a basis for the loan amount. This inflated loan amount will allow the builder to recoup the expense of the incentives, pay a fee to the straw, and keep the loan current for two to four years.
- The builder (or third party) fails to disclose these monetary incentives to the lender.

CHARACTERISTICS OF A BUILDER BAILOUT

The following characteristics are common in builder bailout schemes:

- New construction or renovated condo conversions in an overbuilt market
- Slight decrease in sales and volume, followed by a spike in both volume and sales price
- Non-local borrowers with no knowledge of the local market are recruited to purchase the homes at the inflated sales prices
- Missing the purchase contract addendums disclosing the incentives
- Originated as second homes
- Mortgage payments are made by the builder to avoid detection and prosecution
- Loan remains current for a period of time, but then goes into delinquency
- Property might remain vacant and the neighborhood might be deteriorating

AIR LOANS

Some builders might have debt on vacant land for which they do not have sufficient capital to construct a home. To get out from under the debt, the builder, in collusion with other industry insiders, might undertake an air loan scheme.

An *air loan* is a loan for a nonexistent property—with *air* symbolizing the loan's fraudulent absence of collateral Most or all of the documentation is fabricated, including the borrower, the property ownership documents, and the appraisal. This type of scheme involves a high level of collusion, and perpetrators might have even set up a dummy office with people pretending to be participants in the transaction, such as the borrower's employer, the

appraiser, and the credit agency. Usually, air loans go into early payment default, and, since there are no actual properties on which to foreclose, the losses on these loans can be enormous. However, these schemes are typically short-lived because the detection rate is high.

IDENTITY FRAUD SCHEMES

Identity fraud is defined as the misrepresentation of data underpinning one's identity (such as using another person's government identification number). Mortgage fraud is not immune to schemes involving the improper use of identifying data.

The individuals in the best position to use a person's identifying information for purposes of committing mortgage fraud are industry insiders. Identity fraud schemes might be perpetrated by mortgage brokers in possession of personal identifying information provided by a legitimate borrower and, unbeknownst to him, used over and over again.

Identity fraud schemes are also perpetrated by "investment club" organizers who collect personal information from members and then use it without their knowledge to purchase properties.

In other cases, real estate agents, mortgage brokers, criminals, and other industry insiders provide the stolen identification information of an individual with good credit to an individual with bad credit who wishes to purchase a home. They help create a credit history under the bad credit borrower's name.

Finally, straw borrowers are often provided with stolen or falsified identification information to use in originating loans. This scenario involves a high level of collusion between all parties involved in defrauding the lender.

IDENTITY THEFT SCHEMES

An *identity theft* scheme is defined as the assumption of someone else's identity, which is then used to steal something that individual owns, like his home. Identity theft schemes can be far more troubling than identity fraud schemes.

Two examples of identity theft schemes involving mortgage fraud include the fraudulent acquisition of a person's home and the fraudulent origination of a loan on a property belonging to another person.

Fraudulent Sale

Fraudulent sale scams are particularly harmful because they involve the fraudulent acquisition of a homeowner's property by filing a fraudulent deed or respective real estate document that makes it appear that the property legally belongs to the criminal. This scam does not happen at the origination of the loan, but rather might occur without the homeowner's knowledge decades after the property was originally sold.

The perpetrator identifies a property—typically belonging to an estate or non-resident owner—that is owned free and clear. He then creates fictitious property transfer documents that purport to grant all rights and title on the property to the fraudster. The true owner's signature is forged on the documents, and the scammer files them in the jurisdiction's real property records. Once the ownership documents are filed, he applies for and executes a loan on the property (using a straw borrower). Often, the value is inflated. He absconds with 100 percent of the loan proceeds.

FRAUDULENT SECOND LIEN

In a variation of the fraudulent sale scheme, a person assumes a homeowner's identity and takes out an additional loan or a second mortgage in the homeowner's name. If there is not enough equity in the home to warrant a second loan, an inflated appraisal is obtained. This scheme involves a high level of collusion between a loan officer, an appraiser, and a title agent (or other real estate document service provider).

Foreclosure Rescue Scams

Homeowners who struggle with potential foreclosure might fall prey to foreclosure rescue scams. There are some legitimate foreclosure assistance programs in which the homeowner is offered short-term financing that pays off the delinquent debt. This allows homeowners to stay in their homes as tenants until they can repair their credit and obtain long-term financing. These legitimate programs are offered by government nonprofit counseling agencies, which provide their services for free. However, there are also many fraudulent programs.

Foreclosure rescue scams come in two primary variations: phantom-help scam and lease-back scheme.

PHANTOM-HELP SCAM

The scammer promises to save the homeowner's credit or get him low monthly payments. Instead, the homeowner pays thousands of dollars in fees, and the scammer either does nothing or files bankruptcy on behalf of the borrower and absconds with the fees.

LEASE-BACK SCHEME

The homeowner is tricked into conveying the deed to his house to the fraudster and ultimately loses both the house and any equity.

Property Flipping and Flopping

Property flipping is the process by which an investor purchases a home and then resells it at a higher price shortly thereafter. For example, an investor buys a house in need of work for $250,000 in July, renovates the kitchen and bathrooms, and landscapes the yard at a cost of $50,000. He then resells the house two months later (the time it takes to make the renovations) for a price that is reflective of the market for a house in that condition. This is a legitimate business transaction, and there are numerous individuals and groups in the real estate market who make an honest living flipping properties.

Property flipping is not intrinsically illegal or fraudulent, but it becomes so when a property is purchased and resold within a short period of time at an artificially or unjustly inflated value, often as the result of a fraudulent appraisal. In a flipping scheme, the property is sold twice in rapid succession at a significant increase in value (also known as an *ABC transaction*, where the property moves from party A to party B to party C very quickly).

In the traditional property flipping schemes, it was not unusual for a title agent to close the second transaction (the B/C transaction) first, thereby using the lender's funds to C to fund the acquisition of the property in the A/B transaction. Because this effectively allowed the scheme to be perpetrated without an outlay of capital, property flipping flourished. Today, many title insurers require their agents to close the A/B transaction first.

To circumvent the need for capital to close the first transaction (A/B transaction) before conducting the second transaction, a perpetrator might rely on a short-term loan company for funding. This allows the perpetrator to close the first transaction before the second (albeit only by minutes).

Property flopping is a variation on property flipping, but it generally involves a property subject to a short sale (meaning the owner sells the property at a lower value than the unpaid mortgage amount on the property). This variation typically is conducted by industry insiders or unscrupulous entrepreneurs rather than the homeowner. Property flopping involves a rapid transfer of property with an unjustified, significant change in value (like the ABC transaction in flipping schemes), but instead of inflating the value on the second transaction, the value on the first transaction is deflated. Short sales have provided fraudsters a plentiful supply of inventory to flop, and because lenders are motivated to move nonperforming loans off the books, they can be vulnerable to let property go for less than what it is really worth.

Examples of property flopping include:

- The perpetrator targets a distressed homeowner with an alternative to foreclosure by offering to purchase the property via a short sale.
- The perpetrator then receives third-party authorization to negotiate a short sale with the lender.
- A colluding real estate agent is used to satisfy the lender's requirement to list the property to find what price the market will bear; however, the real estate agent fails to list the property or holds back higher offers.
- The perpetrator influences the broker price opinion ordered by the lender in an attempt to deceive the lender into accepting less than market value for the property.
- At the same time, the perpetrator is recruiting an end buyer to purchase the property in a separate transaction.
- The marketing of the property occurs before the perpetrator takes legal title and purchases the property.
- Once the lender agrees to the short sale price, the perpetrator closes on the transaction at the lower amount and immediately flips the property to the straw at a higher price.
- Because lenders and title agents require that the first transaction close before a second can be conducted, a perpetrator might rely on a short-term lender (one which issues loans for as little as one day) for funding for the first transaction (which will often close just minutes before the second transaction).
- The title company might conceal the rapid transfer of title to evade seasoning requirements and anti-flip rules.
- The alleged misrepresentation is that the subsequent, immediate second transaction at the higher sales price is not disclosed to the original lender, who then loses out on a legitimate recovery of the property.

- Many facilitators and negotiators think there is nothing wrong with this process and claim they have no duty to disclose the second transaction to the lender or other parties.

Many lenders and title insurers have no *seasoning requirements*—meaning that a buyer can qualify for a mortgage on a property that the seller has owned without any seasoning of title.

To prevent problematic short sale flopping, some lenders are starting to require all interested parties to sign an affidavit requiring disclosure of an immediate subsequent sale. In addition, government mortgage assistance programs, such as the Making Home Affordable program in the United States, might prohibit short sales approved under their program from being re-conveyed within a short period of time (e.g., 90 days).

Equity Skimming

Equity skimming is a scheme whereby an individual, entity, or group of individuals purchase one or several single-family homes. Typically, the financing is for a percentage of the purchase price (e.g., 80–90 percent) and the owner invests the balance of the purchase price as equity. The home(s) is/are then rented.

The owners collect the rent from the tenants but fail to make the mortgage payment(s). When the owner has withheld mortgage payments that equal the amount of the invested equity, he can then either resume payments or allow the mortgage to be foreclosed.

Although the mortgage might eventually be foreclosed, the owners have recouped their original investment plus any rental payments not applied to the mortgage. This scheme is most successful with non-recourse mortgages.

An equity skimming scheme eventually collapses, putting the purchasers at risk being sued for deficiencies (if the loans were recourse). Regardless, fraudsters continue to practice the scheme. It has become an increasing problem as many residential homes are auctioned and bulk purchases are encouraged.

Mortgage Pulling

For the purpose of disguising loans exceeding a bank's legal limits, loans are made to a partnership's members who by prearrangement then invest in a single risky venture in a total amount exceeding the lending limit. In reality, the single borrower is the partnership, and the

collateral is the partnership's property. Mortgage pulling might involve fraudulent loan applications and payoffs to the individual partners for participating.

New Account Fraud Schemes

Fraud is much more likely to occur in new accounts than in established accounts. *New account fraud* is generally defined as fraud that occurs on an account within the first 90 days that it is open; often, perpetrators open these accounts with the sole intent of committing fraud. Special efforts must be taken to properly identify the potential new customer. Screening criteria should be established and enforced by everyone handling new accounts. Prompt, decisive action is necessary to manage and/or close apparent problem accounts.

False Identification

New account criminals are actors. They use false identification to open new accounts and steal money before funds are collected by the bank. False identification is easily purchased.

Business Accounts Using Stolen Checks

Some bank customers defraud business institutions by opening a new business account using checks stolen from another business. The fraudsters then withdraw the funds and close the account.

Personal Accounts Using Fraudulent Checks

A similar scheme is to open a new personal account with two checks drawn by other people. The checks are either forged or stolen. The fraudster then deposits one and takes cash for the other. Shortly thereafter, the fraudster writes checks to overdraw the deposited amount.

Mobile Deposit Fraud

Financial institutions are increasingly allowing mobile deposits, which typically involves a person sending a digital image of a check or similar payment order to the depository institution so that the paper document never has to be received or processed. There is a relatively high risk of new account fraud with mobile deposits for two main reasons. First, there is no face-to-face transaction required, which fraudsters prefer in order to maintain anonymity. Second, the digital image is often taken by a camera or a scanner, so it is easier to make forged or counterfeit deposits.

Security features in physical checks, such as water marks and magnetic ink, are not effective for detecting such schemes. However, financial institutions have had success in limiting fraud by setting relatively low daily deposit limits for consumer accounts. Additionally, imposing wait limits on new accounts can reduce the fraud risk. Some financial institutions share depository information with each other, which can help detect duplicate items.

ATM Deposits

Financial institutions should also consider the increased risk of new account fraud when offering ATMs that accept deposits. Like with mobile deposits, the fact that ATM deposits do not require face-to-face transactions with a teller is ideal for fraudsters. Many ATMs have cameras to help identify users.

Prevention

A relationship with a financial institution should never be established until a potential customer's identity is satisfactorily established. If the identity cannot be established, the relationship should not be established.

Personal Accounts

No account should be opened without satisfactory identification, such as:

- A locally issued driver's license with a photograph
- A passport or alien registration card, together with:
  - A college photo identification card
  - A major credit card (verify the current status)
  - An employer identification card
  - An out-of-area driver's license
  - A current utility bill from the customer's place of residence (e.g., gas, electricity, telephone)

In addition, the following identity verification measures should be taken:

- Consider the customer's residence or place of business. If it is not in the area served by the bank or branch, ask why the customer is opening an account at that location.
- Follow up with calls to the customer's residence or place of employment, thanking the customer for opening the account. Disconnected phone service or no record of employment warrant further investigation.

- Consider the source of funds used to open the account. Large cash deposits should be questioned.
- For large accounts, ask the customer for a prior bank reference and write a letter to the bank asking about the customer.
- Check with service bureaus for indications that the customer has been involved in questionable activities such as kiting incidents and non-sufficient-funds (NSF) situations.
- If applicable, establish the customer's identity through an existing relationship with the institution, such as some type of loan or other account relationship.
- Conduct an audit of third-party credit reporting agencies and customer identification services.

Business Accounts

Business principals should provide evidence of legal status (e.g., sole proprietorship, partnership, or incorporation or association) when opening a business account. The following verification measures should also be taken:

- Check the name of a commercial enterprise with a reporting agency and check prior bank references.
- Follow up with calls to the customer's business thanking the customer for opening the account. Disconnected phone service warrants further investigation.
- When circumstances allow, perform a visual check of the business to verify its actual existence and that the business has the capability of providing the services described.
- Consider the source of funds used to open the account. Large cash deposits should be questioned.

Since tellers are often the frontline defense in preventing check fraud, it is important that they receive training that will allow them to identify fraudulent checks. Tellers should:

- Be aware of magnetic and fractional routing numbers.
- Look for variations in font sizes in the payee, amount, and date sections.
- Recognize the increased likelihood of counterfeit items from foreign entities.
- Look for checks with numbers lower than 200.
- Be aware of the date that the account was opened.
- Have easy access to the signature card.
- Be aware of what is acceptable identification.
- Recognize forged/altered identification.
- Recognize forged negotiable instruments.

- Be familiar with patterns of behavior related to potential culprits:
  - Overly polite
  - Nervous
  - Aggressive and hurried

Detection

Some of the more common red flags of potential new account schemes are:

- Customer residence outside the bank's trade area
- Dress and/or actions inconsistent or inappropriate for the customer's stated age, occupation, or income level
- New account requesting immediate cash withdrawal upon deposit
- Request for large quantity of temporary checks
- Services included with the account that do not match the customer's purpose
- Missing or inaccurate customer application information
- Invalid phone numbers or addresses in customer account information
- Use of a mail drop address (a service where a non-affiliated party collects and distributes a person or entity's mail)
- Large check or ATM deposits followed by rapid withdrawal or transfer of funds (a flow-through account)
- Business accounts without standard business transactions, such as payroll or transactions that would be expected in that business
- Transactions without a clear purpose in jurisdictions known for high levels of corruption
- Opening deposit that is a nominal cash amount
- Rare customer ID type
- Applicants over the age of 25 with no credit history
- Customers who cannot remember basic application information (phone number, address, etc.)

Money Transfer (Wire) Fraud Schemes[1]

Wire transfers of funds are nothing new—they began in the 1940s. However, with today's growing emphasis on a cashless society, the number of wire transfers increases each year.

[1] The editors wish to thank James Incaprera, CFSSP, CPP, and Joyce C. Lambert, Ph.D., CIA, CPA, for their assistance in preparing this section. Mr. Incaprera is the Audit Manager for Crescent Bank in New Orleans, LA, and Dr. Lambert is a professor of accounting at the University of New Orleans.

Typically, fraudsters who commit this type of crime are knowledgeable about wire transfer activity, have at least one contact within the target company, and are aggressive in carrying out the theft.

Instantaneous Transfer

Wire transfer services electronically move funds worldwide from a financial institution to a beneficiary account at any banking point as per a customer's instructions. (A banking point is any institution or business capable of receiving electronic transactions, such as banks, savings and loans, credit unions, brokerage firms, and insurance companies.) On any day, $2 trillion to $3 trillion moves among financial institutions. The transactions are primarily for completing interbank purchases and sales of federal funds; purchasing, selling, and financing securities transactions; disbursing loan proceeds or repaying loans; and conducting real estate business.

Although these technologies enhance operations and increase the financial institutions' efficiency, they also provide a tremendous opportunity for criminals who learn to manipulate the electronic environment for their personal gain. Wire transfer fraud is a particularly dangerous risk to a business's solvency—one major wire fraud can destroy any firm.

Common Schemes

The following are some of the more common schemes involving wire transfers.

Dishonest Bank Employees

People who have access to correct account identification information can transfer money improperly—insiders wire funds to themselves and/or related parties.

Misrepresentation of Identity

People pose as customers, having used pretext calls to obtain correct account information from the bank. People posing as wire room employees in another bank or a branch office order transfers to dummy accounts in another bank.

System Password Security Compromised

People who have legitimate access to sensitive account and daily code information for a limited time (for example, computer consultants) affect improper transfers through unauthorized access.

Forged Authorizations

Bank officers' and customers' authorization, whether oral or written, is improperly obtained or forged. People forge orders to transfer money to their own accounts when the recipient account is actually in someone else's name.

Unauthorized Entry and Interception

Unauthorized personnel gain access to the wire room and its equipment, or the actual transmission is intercepted and altered.

Preventing and Detecting Wire Transfer Fraud

Fraud examiners and auditors need to advise management on ways to prevent and detect wire transfer fraud.

Business Audits and Other Controls

Every firm must have written policies and procedures for wire transactions. In addition, fraud examiners or auditors should conduct unannounced audits of those transactions. The following are other examples of wire transfer controls:

- Make sure the person authorizing the wire transfer isn't the individual who orders it.
- Require those ordering transfers to have secure passwords.
- Maintain and keep a current list of those ordering wire transfers, as well as a log of all transfers.
- Require employees who handle wire transfers to go on vacation.
- Require that reconciliations of accounts affected by wire transfers be performed by individuals not involved with the wire transfer process.
- Keep all confidential information about the firms' accounts and wire transfers in safe rooms secured with locks. Give computer key cards to these rooms to authorized personnel only. Shred discarded documents.

Businesses frequently perform vendor audits, but often neglect to audit their bank's wire transfer controls. To conduct such audits, a fraud examiner should:

- Pick a sample of transactions and review the log of the calls made back to the banking points to verify their authenticity. (You might listen to the recording of the actual authorization to ensure compliance with call-back rules.)
- Review documentation of past wire transfer activity from bank statements or bank online transaction history for a daily debit and credit match of each transaction.

- Obtain written confirmations of transactions from the wire transfer provider to determine the timeliness of their receipt by your firm.
- Promptly reconcile problems caused by the usual custom of ending all wire transfers for a day in the mid-afternoon. (Some customers believe they should receive credit and interest on funds received at the end of a day. However, wire transfers made after the afternoon closing time aren't credited until the next business day.)

Bank Audits

Financial institutions should ensure the following safeguards when transferring funds:

- Provide customers with unique codes that are required to authorize or order wire transfers.
- Maintain and update lists of employees authorized to perform wire transfer transactions.
- Compile audit trails of incoming and outgoing wire transactions, as well as the employee responsible for each portion of the transaction.
- Review all wire transfer transactions at the end of each day to ensure that the original transfer instructions were executed correctly.
- Make sure the businesses to which the funds are transferred are contacted to ensure authenticity of fund transfer requests. If the businesses are contacted by phone, the phone numbers used should be the original numbers given by the customers when the accounts were opened and not the phone numbers provided by the callers who requested the transfers.
- Don't execute wire transfers solely from faxed instructions. Again, verify authenticity by phoning the original numbers given by the customers when the accounts were opened and not the numbers provided by the callers who requested the transfers.
- Require that all accounts affected by wire transfers be reconciled by bank employees not involved with the wire process.
- Ensure that the in-house wire operations manual is available only to authorized personnel and secured when not in use—especially after hours. Cleaning crew employees could help themselves to client pass codes and other confidential information.
- Record all incoming and outgoing calls for wire transfer instructions.
- Carefully screen wire transfer personnel applicants.
- Reassign to other departments wire transfer employees who have given notice that they are resigning but still have some time left with the company.
- Require all employees involved in the transfer of funds to take at least five consecutive days of vacation each year; assign their duties only to other transfer department staff members during their absence.

- Make sure bank employees never disclose sensitive information over the telephone until the caller's identity and authorization have been verified against the customer information file.
- Separate duties among wire employees who transmit or receive requests for funds. These employees shouldn't also verify the transactions' accuracy.
- Train employees on proper internal controls, fraud awareness, and the importance of protecting information. Share alerts issued by government agencies and professional groups.

Automated Teller Machine (ATM) Fraud

An ATM is a dispensing facility from which a debit or credit card holder can withdraw cash. Some types of prepaid cards can also be used at ATMs. The facility can also perform other services, such as depositing funds and verifying account balances, but the most common use is to dispense funds. Fraud schemes have been perpetrated involving the unauthorized use of ATM facilities. Schemes include:

- Theft of card and/or unauthorized access to PINs and account codes for ATM transactions by unauthorized persons
- Employee manipulation
- Counterfeit ATM cards
- Counterfeit ATMs
- Magnetic strip skimming devices
- ATM deposit fraud

EXAMPLE

A former Citibank employee was sentenced to 41 months in prison for masterminding a scheme to steal $200,000 in cash from several of the bank's ATMs. The computer expert was the No. 2 official in Citibank's ATM security department and programmed the bank's money machines to issue money and not leave any record of the transactions. This was done by remotely accessing the company's mainframe computer and instructing it to put particular machines in "test mode."

Detection

When investigating ATM schemes, look for a lack of segregation of duties between the card issuing function and the personal identification (PIN) issuance.

Account Takeover

In an account takeover, the perpetrator gains unauthorized access to a customer's account, usually through online banking. The perpetrator often gains access through phishing techniques, in which he attempts to get victims to visit fraudulent websites or download malware that gathers personal information from the user's device. Once account access is gained, the fraudster poses as the customer and is able to perform various actions regarding the account, such as creating payments to be issued from the account without the true account holder's knowledge. Depending on when the victim reports the takeover, this type of crime can go undetected for several months.

Detection

These schemes are best detected through automated monitoring to identify red flags, with manual examination of transactions that appear suspicious. Automated monitoring systems use a variety of factors to determine whether a transaction appears abnormal for that particular customer, including:

- Daily or overall purchase patterns that substantially exceed the customer's normal range
- Purchase volume substantially exceeds customer's anticipated income or credit limit
- Geographic location of transactions (online and mobile banking applications can typically collect such data)
- Identification of electronic devices (e.g., smart phones, tablets, PCs) that the customer registers with the institution
- Abnormal IP addresses that the user logs in from
- Whether the transacting parties make sense for the particular customer
- Abnormal transaction timing (e.g., large volume of purchases late at night for the customer when there previously were none during this time)

Many financial institutions now use behavioral analytics software that can proactively identify account takeovers. These programs are designed to establish a baseline that describes the manner in which a particular user typically accesses and interacts with a Web application. After enough data has been collected to establish a user's profile, any activity that significantly deviates from the expected behavior is flagged for further review, and in some cases, halts the transaction in real time.

Fraud examiners should assess the organization's risk and determine what types of schemes are most likely to occur. The best automated monitoring system will be tailored for the financial institution and its various types of customers.

Advance-Fee Fraud

An *advance-fee fraud* is a scheme in which the fraudster persuades the target to advance sums of money by falsely promising the delivery of a product or a service. Banks find deals that seem "too good to be true" to gain access to large amounts of money (deposits) at below-market interest rates. The catch is that the bank must pay an upfront finder's fee to a person claiming to have access to the money. In some cases, desperate institutions are offered access to illegal money, and they typically do not report the loss of the advance fee when the deal falls through. More information on advance-fee swindles can be found in the "Consumer Fraud" chapter.

EXAMPLE

The bank is contacted by an agent (such as a broker, advisor, consultant, promoter, lawyer, or bank customer) offering to provide money at a below-market interest rate for a long period of time (e.g., 10–20 years). The agent asks for a large fee to close the deal. The agent takes the fee and disappears. The deposits might or might not exist, and if they do, they seldom equate to the agent's representations.

Red Flags

There are a few key indicators of advance-fee fraud, including:

- The agent requests documents on bank stationery or signatures of officers.
- The bank is asked to give nondisclosure agreements to protect agents or other parties.
- There are several complex layers of agents, brokers, and other middlemen.

Brokered Loans

A variation of the advance-fee scheme is the brokered loan. *Loan brokering* applies to either packages of individual residential (consumer) loans or single commercial loans. A variation of a brokered loan is *loan participation*, where multiple parties purchase and have interests in a loan or a package of loans. The fraud schemes associated with brokered loans or loan participation generally involve selling phony loans (packages) or selling participations in loans that have not been properly underwritten. Generally, a large fee is charged for these brokered loans.

With residential loan packages, the broker sells the package, takes the money, and disappears. Brokered loans are generally not sold with any recourse to the broker. Therefore, the purchaser must look to the borrower and the underlying collateral for debt satisfaction. With loan participations, the lead bank generally performs the underwriting. However, this does

not relieve the participating bank from its obligation to perform its own due diligence. If the participating bank does not independently examine the documentation and perform its own due diligence, then fraud schemes on the part of the selling institution are possible.

Letter-of-Credit Fraud

Most letter-of-credit fraud arises from foreign trade and contracting. Letter-of-credit fraud can be perpetrated by beneficiaries using forged or fraudulent documents presented to the issuing bank with a demand for payment. The documents, however, must conform to the terms of the letter-of-credit agreement.

EXAMPLE

An American exporter might offer to sell goods to an overseas importer. When terms are arranged, a letter of credit is obtained in the exporter's favor and confirmed by a bank near the exporter's location. (The actual export never occurs, and the request for payment is bogus.)

Inside/Outside Frauds

Inside/outside frauds are on the rise; in this type of fraud, the employee (an insider) might be co-opted through a bribe or a threat of violence against him or a family member. Sometimes the insider is a bank teller who agrees to cash certain items as long as the items look reasonable and are below a cashing limit. Other times, the insider is a proof operator or sorter operator who inserts documents directly into the computer system to affect fraudulent deposits. The insider might also be selling copies of documents to individuals who use computer techniques to make fraudulent items.

Account Information Frauds

Information is sold to organized rings or insiders who use the information themselves. As financial institutions make more services available to customers and strive to make them more usable, information about customer account relationships reside in many forms, such as 24-hour customer operators, online systems, printed documents that are innocently put in the trash only to be retrieved, or credit card information on high-line cards.

Trading Activities

Trading activities can be compromised to defraud banks. Usually perpetrated with the assistance of an internal employee or by an employee acting alone, trading can include foreign exchange, securities trading, loan sales, and securitization. Often, when this type of problem is suspected, the investigator must turn to traders themselves as the only source to gather information.

Prevention

Like other organizations, financial institutions should have standard internal control measures to assist in the detection and deterrence of fraud. In addition to normal procedures, such as segregation of duties and budget and actual comparisons, the following are some specific control measures that might enhance the detection and deterrence of financial institution fraud.

Loan Origination, Underwriting, Closing, Disbursement, and Servicing Segregation

By separating all of the functions relating to loans, a lending institution reduces the opportunity for an individual (an insider) to perpetrate loan fraud. Additionally, the segregation provides for at least one, if not several, levels of independent review to reduce its external loan fraud exposure.

Committee Approval of All Large or Unusual Transactions

If a loan committee or a board of directors committee is responsible for approving loans and other large or unusual transactions, then insiders will have a more difficult time perpetrating large fraud, and the transactions submitted by external fraudsters will be subject to another layer of independent review.

Transfer Journal Entries and Orders Review

Regularly review all transfer journal entries and orders. As with an expense review, if a routine-but-unscheduled review occurs from time to time, then the fraudster loses his vehicle for concealment.

Independent Review of Loans

An independent review of loans provides a nonpartisan approach to all loan transactions. Either the internal or external auditors (or other consultants) can perform this independent review that allows for a "second opinion" on loan transactions. The reviews should be

consistent and performed on a regular basis to help establish loan loss reserves. Typically, this loan review is established for loans over a certain dollar amount, such as $25,000 or $100,000.

Management Review of Write-Offs

Excessive write-offs are a form of concealment for phantom loans, conflicts of interest, and embezzlement. Therefore, if all write-offs are subject to management review *before they are written off*, then management reduces the potential environment for fraud.

Routine Examination of Officers' Accounts

Routine examination of officers' accounts might prevent fraud schemes such as wire transfer fraud, embezzlement, withdrawals from dormant accounts, conflicts of interest, and so on. This review can be performed when the officer is on mandatory vacation.

Proper Lending Policies

Employees should be trained in the institution's proper (and regulated) lending policies. Any deviations from the policies will be red flags and will help to prevent loan fraud from both internal and external perpetrators.

Document Requirements for Standard Transactions

Deviations from normal or proscribed documentation should be an automatic red flag. Who better to recognize a potential fraud than the employees routinely handling the documentation? Therefore, employees should be well-educated in proper documentation for the transactions they are handling.

Information Verification (For Example, Loan Applications)

Fraud potential can be eliminated—or at the very least detected—before companies suffer damages if the employee knows how to verify information. For example, if the loan officer advises a potential borrower that the information submitted on financial statements will be verified, the borrower will be less likely to submit false or fraudulent financial statements. Additionally, if a teller advises a depositor that the deposit will be verified before cash is paid out, then the incidence of split deposits can be reduced.

Employee Training

Fellow employees are generally the first people to recognize other employees' unusual transactions or behavior changes. These might be early indicators that a fraud has started or

will soon begin. Employees and managers should be properly trained to recognize these symptoms. For example, bank tellers should be adequately schooled in split deposit schemes, new account officers in new account schemes, and so on.

Standardized Procedures

An institution can provide a low-fraud environment by standardizing procedures in sensitive areas, such as the following:

- Loan application processing
- Information required for loan approval
- Credit report requests
- Appraisals accepted from a pre-approved list of vendors
- Inspection reports on construction draw loans
- Conflict of interest disclosure statements
- Routine confirmation calls for
  - Wire transfers
  - Construction vendors
- Confirmation of registered securities with registrar or transfer agent
- Periodic physical inventory of securities

Suspicious Transaction Reports

Under the Financial Action Task Force's (FATF) Recommendation 20, countries should require financial institutions to promptly report to the country's financial intelligence unit if they have "reasonable grounds to suspect that funds" from a transaction "are the proceeds of a criminal activity, or are related to terrorist financing." Many countries have implemented laws in compliance with Recommendation 20. The reports are typically called *suspicious transaction reports, suspicious activity reports,* or something similar. The financial intelligence unit should review the reports and work with law enforcement to investigate likely instances of financial crime. For more information about suspicious transaction reports, see the "Money Laundering" chapter in the Law section of the *Fraud Examiners Manual.*

The Basel Committee on Banking Supervision[2]

The Basel Committee, established by the central-bank Governors of the Group of Ten (G10) countries at the end of 1974, provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.

The committee is composed of 60 member countries. Countries are represented by their central bank and also by the authority with formal responsibility for the prudential supervision of banking business where this is not the central bank.

The committee does not possess any formal supranational supervisory authority, and its conclusions do not, and were never intended to, have legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements—statutory or otherwise—which are best suited to their own national systems. In this way, the committee encourages convergence toward common approaches and common standards without attempting detailed harmonization of member countries' supervisory techniques.

The committee reports to the central bank Governors and to the heads of supervisory authorities of these countries where the central bank does not have formal responsibility. It seeks their endorsement for its major initiatives. One important objective of the committee's work has been to close gaps in international supervisory coverage in pursuit of two basic principles: that no foreign banking establishment should escape supervision; and that supervision should be adequate.

In 1988, the committee introduced a capital measurement system commonly referred to as the Basel Capital Accord. This system provided for the implementation of a credit risk measurement framework with a minimum capital standard of 8 percent by the end of 1992. Since 1988, this framework has been progressively introduced not only in member countries, but also in virtually all other countries with internationally active banks. In June 1999, the committee issued a proposal for a revised Capital Adequacy Framework. The proposed capital framework consists of three pillars: (1) minimum capital requirements, which seek to

[2] The material in this section is compiled from materials and resources issued by the Bank for International Settlements. For more information on this subject, please refer to their website at www.bis.org.

refine the standardized rules set forth in the 1988 Accord; (2) supervisory review of an institution's internal assessment process and capital adequacy; and (3) effective use of disclosure to strengthen market discipline as a complement to supervisory efforts. Following extensive interaction with banks, industry groups, and supervisory authorities that are not members of the committee, the revised framework was issued in June 2004. This text serves as a basis for national rule-making and for banks to complete their preparations for the new framework's implementation.

Over the past several years, the committee has moved more aggressively to promote sound supervisory standards worldwide. In close collaboration with many non-G10 supervisory authorities, the committee developed a set of Core Principles for Effective Banking Supervision, which provides a comprehensive blueprint for an effective supervisory system. To facilitate implementation and assessment, the committee developed the Core Principles Methodology.

The committee's secretariat is provided by the Bank for International Settlements in Basel. The fifteen-person secretariat is mainly staffed by professional supervisors on temporary secondment from member institutions. In addition to undertaking the secretarial work for the committee and its many expert sub-committees, it stands ready to give advice to supervisory authorities in all countries.

The Basel Core Principles for Effective Banking Supervision

The Core Principles for Effective Banking Supervision have been used by countries as a benchmark for assessing the quality of their supervisory systems and for identifying future work to be done to achieve a baseline level of sound supervisory practices. Experience has shown that self-assessments of countries' compliance with the Core Principles have proven helpful for the authorities, in particular in identifying regulatory and supervisory shortcomings and setting priorities for addressing them.

The Core Principles are a framework of minimum standards for sound supervisory practices and are considered universally applicable. The committee drew up the Core Principles and the Methodology as its contribution to strengthening the global financial system. Weaknesses in the banking system of a country, whether developing or developed, can threaten financial stability both within that country and internationally. The committee believes that implementation of the Core Principles by all countries would be a significant step toward

improving financial stability domestically and internationally and provide a good basis for further development of effective supervisory systems.

The Basel Core Principles define 29 principles that are needed for a supervisory system to be effective. Those principles are broadly categorized into two groups:

- Supervisory powers, responsibilities, and functions (principles 1 to 13)
- Prudential regulation and requirements (principles 14 to 29)

The Core Principles are neutral with regard to different approaches to supervision, so long as the overriding goals are achieved. The principles are not designed to cover all the needs and circumstances of every banking system. Instead, specific country circumstances should be more appropriately considered in the context of the assessments and in the dialogue between assessors and country authorities.

National authorities should apply the principles in the supervision of all banking organizations within their jurisdictions. Individual countries, in particular those with advanced markets and institutions, may expand upon the principles in order to achieve best supervisory practice.

A high degree of compliance with the principles should foster overall financial system stability; however, this will not guarantee it, nor will it prevent the failure of individual banks. Banking supervision cannot, and should not, provide an assurance that banks will not fail. In a market economy, failures are part of risk-taking.

The committee stands ready to encourage work at the national level to implement the principles in conjunction with other supervisory bodies and interested parties. The committee invites the international financial institutions and donor agencies to use the principles in assisting individual countries to strengthen their supervisory arrangements. The committee will continue to collaborate closely with the IMF and the World Bank in their monitoring of the implementation of the committee's prudential standards. The committee is also committed to further enhancing its interaction with supervisors from non-G10 countries.

The Core Principles can be found here: www.bis.org/publ/bcbs230.htm.

The Basel II Framework

The International Convergence of Capital Measurement and Capital Standards: A Revised Framework, or the "Basel II Framework," offered a new set of standards for establishing minimum capital requirements for banking organizations. It was prepared by the Basel Committee on Banking Supervision, a group of central banks and bank supervisory authorities in the G10 countries, which developed the first standard in 1988.

Capital Requirements

Nearly all jurisdictions with active banking markets require banking organizations to maintain at least a minimum level of capital. Capital serves as a foundation for a bank's future growth and as a cushion against its unexpected losses. Adequately capitalized banks that are well managed are better able to withstand losses and to provide credit to consumers and businesses alike throughout the business cycle, including during downturns. Adequate levels of capital thereby help to promote public confidence in the banking system.

The technical challenge for both banks and supervisors has been to determine how much capital is necessary to serve as a sufficient buffer against unexpected losses. If capital levels are too low, banks may be unable to absorb high levels of losses. Excessively low levels of capital increase the risk of bank failures which, in turn, may put depositors' funds at risk. If capital levels are too high, banks may not be able to make the most efficient use of their resources, which may constrain their ability to make credit available.

The 1988 Basel Capital Accord set out the first internationally accepted definition of, and a minimum measure for, bank capital. The Basel Committee designed the 1988 Accord as a simple standard so that it could be applied to many banks in many jurisdictions. It requires banks to divide their exposures up into broad "classes" reflecting similar types of borrowers. Exposures to the same kind of borrower—such as all exposures to corporate borrowers—are subject to the same capital requirement, regardless of potential differences in the creditworthiness and risk that each individual borrower might pose.

While the 1988 Accord was applied initially only to internationally active banks in the G10 countries, it quickly became acknowledged as a benchmark measure of a bank's solvency and is believed to have been adopted in some form by more than 100 countries. The committee supplemented the 1988 Accord's original focus on credit risk with requirements for exposures to market risk in 1996.

Advances in risk management practices, technology, and banking markets have made the 1988 Accord's simple approach to measuring capital less meaningful for many banking organizations. For example, the 1988 Accord sets capital requirements based on broad classes of exposures and does not distinguish between the relative degrees of creditworthiness among individual borrowers.

Likewise, improvements in internal processes, the adoption of more advanced risk measurement techniques, and the increasing use of sophisticated risk management practices such as securitization have changed leading organizations' monitoring and management of exposures and activities. Supervisors and sophisticated banking organizations have found that the static rules set out in the 1988 Accord have not kept pace with advances in sound risk management practices. This suggests that the existing capital regulations may not reflect banks' actual business practices.

The Basel II Framework's Effect on Capital Requirements

The Basel II Framework builds on the 1988 Accord's basic structure for setting capital requirements and improves the capital framework's sensitivity to the risks that banks actually face. The overarching goal for the Basel II Framework is to promote the adequate capitalization of banks and to encourage improvements in risk management, thereby strengthening the stability of the financial system. This goal is to be accomplished through "three pillars" that reinforce each other and that create incentives for banks to enhance the quality of their control processes. The first pillar represents a significant strengthening of the minimum requirements set out in the 1988 Accord, while the second and third pillars represent innovative additions to capital supervision.

Pillar 1 of the Basel II capital framework revises the 1988 Accord's guidelines by aligning the minimum capital requirements more closely to each bank's actual risk of economic loss. First, Basel II improves the capital framework's sensitivity to the risk of credit losses generally by requiring higher levels of capital for those borrowers thought to present higher levels of credit risk, and vice versa. Three options are available to allow banks and supervisors to choose an approach that seems most appropriate for the sophistication of a bank's activities and internal controls.

Under the "standardized approach" to credit risk, banks that engage in less complex forms of lending and credit underwriting and that have simpler control structures may use

external measures of credit risk to assess the credit quality of their borrowers for regulatory capital purposes.

Banks that engage in more sophisticated risk-taking and that have developed advanced risk measurement systems may, with the approval of their supervisors, select from one of two "internal ratings-based" ("IRB") approaches to credit risk. Under an IRB approach, banks rely partly on their own measures of a borrowers' credit risk to determine their capital requirements, subject to strict data, validation, and operational requirements.

Second, the Basel II Framework establishes an explicit capital charge for a bank's exposures to the risk of losses caused by failures in systems, processes, or staff or that are caused by external events, such as natural disasters. Similar to the range of options provided for assessing exposures to credit risk, banks will choose one of three approaches for measuring their exposures to operational risk that they and their supervisors agree reflects the quality and sophistication of their internal controls over this particular risk area.

By aligning capital charges more closely to a bank's own measures of its exposures to credit and operational risk, the Basel II Framework encourages banks to refine those measures. It also provides explicit incentives in the form of lower capital requirements for banks to adopt more comprehensive and accurate measures of risk as well as more effective processes for controlling their exposures to risk.

Pillar 2 of the Basel II capital framework recognizes the necessity of exercising effective supervisory review of banks' internal assessments of their overall risks to ensure that bank management is exercising sound judgment and has set aside adequate capital for these risks. Supervisors will evaluate the activities and risk profiles of individual banks to determine whether those organizations should hold higher levels of capital than the minimum requirements in Pillar 1 would specify and to see whether there is any need for remedial actions.

The committee expects that, when supervisors engage banks in a dialogue about their internal processes for measuring and managing their risks, they will help to create implicit incentives for organizations to develop sound control structures and to improve those processes.

Pillar 3 of the Basel II capital framework leverages the ability of market discipline to motivate prudent management by enhancing the degree of transparency in banks' public reporting. It sets out the public disclosures that banks must make that lend greater insight into the adequacy of their capitalization.

The committee believes that, when marketplace participants have a sufficient understanding of a bank's activities and the controls it has in place to manage its exposures, they are better able to distinguish between banking organizations so that they can reward those that manage their risks prudently and penalize those that do not.

The Basel III Framework

On December 16, 2010, the committee issued two publications containing the final text of an update to Basel II. These were followed, on January 13, 2011, by an Annex containing the reform to the redefinition of regulatory capital. These publications, collectively known as Basel III, are a comprehensive set of reform measures to strengthen the regulation, supervision, and risk management of the banking sector. The implementation deadline has been delayed several times as a result of amendments, and is currently scheduled for 2019.

Increased Capital Requirements

Under Basel III, the minimum requirement for common equity—the highest form of loss absorbing capital—will be raised, starting from the previous 2 percent level prior to Basel III, and eventually increasing to 4.5 percent by 2019. The Tier 1 capital requirement, which includes common equity and other qualifying financial instruments based on stricter criteria, will increase from 4 to 6 percent over the same period. Additionally, Basel III implemented adjustments regarding how the percentage is measured, making it more strict.

The capital conservation buffer above the regulatory minimum requirement will be calibrated at 2.5 percent and be met with common equity, after the application of deductions. The purpose of the conservation buffer is to ensure that banks maintain a buffer of capital that can be used to absorb losses during periods of financial and economic stress. The conservation buffer is set to be gradually phased in, starting in 2016 and ending in 2019. While banks are allowed to draw on the buffer during such periods of stress, the closer their regulatory capital ratios approach the minimum requirement, the greater the constraints on earnings distributions. This framework will reinforce the objective of sound supervision and bank governance and address the collective action problem that has prevented some banks

from curtailing distributions such as discretionary bonuses and high dividends, even in the face of deteriorating capital positions.

A countercyclical buffer within a range of 0–2.5 percent of common equity or other fully loss absorbing capital will be implemented according to national circumstances. The purpose of the countercyclical buffer is to achieve the broader macroprudential goal of protecting the banking sector from periods of excess aggregate credit growth. For any given country, this buffer will only be in effect when there is excess credit growth that is resulting in a system wide build-up of risk. The countercyclical buffer, when in effect, would be introduced as an extension of the conservation buffer range.

These capital requirements are supplemented by a non-risk-based leverage ratio that will serve as a backstop to the risk-based measures described previously.

In addition to meeting the Basel III requirements, global systemically important financial institutions (SIFIs) must have higher loss absorbency capacity to reflect the greater risks that they pose to the financial system. The Committee has developed a methodology that includes both quantitative indicators and qualitative elements to identify global systemically important banks (SIBs). The additional loss absorbency requirements are to be met with a progressive Common Equity Tier 1 (CET1) capital requirement ranging from 1 to 2.5 percent, depending on a bank's systemic importance. For banks facing the highest SIB surcharge, an additional loss absorbency of 1 percent could be applied as a disincentive to increase materially their global systemic importance in the future. A consultative document was published in cooperation with the Financial Stability Board, which is coordinating the overall set of measures to reduce the moral hazard posed by global SIFIs.

Global Liquidity Standards

The Basel III global liquidity standards include a common set of monitoring metrics to assist supervisors in identifying and analyzing liquidity risk trends at both the bank and system-wide levels. Included in the standards are the liquidity coverage ratio and the net stable funding ratio.

LIQUIDITY COVERAGE RATIO

The liquidity coverage ratio (LCR) requires banks to have sufficient high-quality liquid assets to withstand a 30-day stressed funding scenario that is specified by supervisors. In January 2013, the Committee issued a final revised standard on the LCR.

- An increase in the range of eligible assets that can be held as part of the required liquidity buffer (subject to the discretion of each national supervisor)
- Changes in cash outflow and inflow rates
- A revised timetable, keeping the original January 1, 2015, date for full implementation, but with a transitional period where the minimum level of liquidity coverage will gradually rise from 60 percent of the minimum standard to the full 100 percent
- A clarification that it is expected that supervisors will permit the use of the liquidity buffer in times of stress (i.e. banks will be allowed to use the buffer, and thus fall below the minimum ratio, in a liquidity stress scenario)

NET STABLE FUNDING RATIO

The net stable funding ratio (NSFR) is a longer-term structural ratio designed to address liquidity mismatches. It covers the entire statement of financial position and provides incentives for banks to use stable sources of funding.

Sound Practices for the Management and Supervision of Operational Risk

In February 2003, the Committee issued a guideline entitled "Sound Practices for the Management and Supervision of Operational Risk." This paper outlined a set of principles that provide a framework for the effective management and supervision of operational risk, for use by banks and supervisory authorities when evaluating operational risk management policies and practices. The Basel Committee on Banking Supervision recognized that the exact approach for operational risk management chosen by an individual bank will depend on a range of factors, including its size and sophistication and the nature and complexity of its activities. However, despite these differences, clear strategies and oversight by the board of directors and senior management, a strong operational risk culture and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework for banks of any size and scope. However, the principles outlined in the guideline establish sound practices relevant to all banks.

Background

Deregulation and globalization of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their risk profiles (i.e., the level of risk across a firm's activities and/or risk categories) more complex.

Developing banking practices suggest that risks other than credit, interest rate, and market risk can be substantial. Examples of these new and growing risks faced by banks include:

- If not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;
- Growth of e-commerce brings with it potential risks (e.g., internal and external fraud and system security issues) that are not yet fully understood;
- Large-scale acquisitions, mergers, de-mergers, and consolidations test the viability of new or newly integrated systems;
- The emergence of banks acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems;
- Banks may engage in risk mitigation techniques (e.g., collateral, credit derivatives, netting arrangements, and asset securitizations) to optimize their exposure to market risk and credit risk, but which, in turn, may produce other forms of risk (e.g., legal risk); and
- Growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risks but can also present significant other risks to banks.

This diverse set of risks can be grouped under the heading of "operational risk," which the committee has defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events." The definition includes legal risk, but excludes strategic and reputational risk.

Operational risk event types that the Committee—in cooperation with the industry—identified as having the potential to result in substantial losses include:

- Internal fraud (e.g., intentional misreporting of positions, employee theft, and insider trading on an employee's own account)
- External fraud (e.g., robbery, forgery, check kiting, and damage from computer hacking)
- Employment practices and workplace safety (e.g., workers' compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability)
- Clients, products, and business practices (e.g., fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products)
- Damage to physical assets (e.g., terrorism, vandalism, earthquakes, fires, and floods)

- Business disruption and system failures (e.g., hardware and software failures, telecommunication problems, and utility outages)
- Execution, delivery, and process management (e.g., data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes)

Industry Trends and Practices

The Committee also recognized that management of specific operational risks is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk in principle, if not always in form. The current trends in the financial industry, combined with a growing number of high-profile operational loss events worldwide, have led banks and supervisors to increasingly view operational risk management as an inclusive discipline, as has already been the case in many other industries.

In the past, banks relied almost exclusively upon internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. While these remain important, recently there has been an emergence of specific structures and processes aimed at managing operational risk. In this regard, an increasing number of organizations have concluded that an operational risk management program provides for bank safety and soundness, and are, therefore, making progress in addressing operational risk as a distinct class of risk similar to their treatment of credit and market risk. The Committee believes that an active exchange of ideas between the supervisors and industry is key to ongoing development of appropriate guidance for managing exposures related to operational risk.

Sound Practices

In developing these sound practices, the Committee has drawn upon its existing work on the management of other significant banking risks, such as credit risk, interest rate risk, and liquidity risk, and the Committee believes that similar rigor should be applied to the management of operational risk. Nevertheless, it is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process. At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to

significant losses. Reflecting the different nature of operational risk, for the purposes of this paper, "management" of operational risk is taken to mean the "identification, assessment, monitoring, and control/mitigation" of risk. This definition contrasts with the one used by the Committee in previous risk management papers of the "identification, measurement, monitoring, and control" of risk. In common with its work on other banking risks, the Committee has structured this sound practice paper around a number of principles. These principles were grouped in four broad categories:

- Developing an appropriate risk management environment
- Risk management: identification, assessment, monitoring, and mitigation/control
- Role of supervisor
- Role of disclosure

DEVELOPING AN APPROPRIATE RISK MANAGEMENT ENVIRONMENT

Principle 1: The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained, and competent staff. The internal audit function should not be directly responsible for operational risk management.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organization, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes, and procedures for managing operational risk in all of the bank's material products, activities, processes, and systems.

RISK MANAGEMENT: IDENTIFICATION, ASSESSMENT, MONITORING, AND MITIGATION/CONTROL

Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes, and systems. Banks should also ensure that before new

products, activities, processes, and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Principle 6: Banks should have policies, processes, and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

ROLE OF SUPERVISORS

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor, and control/mitigate material operational risks as part of an overall approach to risk management.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures, and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

ROLE OF DISCLOSURE

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

CHECK AND CREDIT CARD FRAUD

Check Fraud

Although reported instances of financial crime increase each year, one scam that has traditionally plagued banks and consumers for decades is on the decline: check fraud. The number of organizations reporting incidents of check fraud dropped from 88 percent to 77 percent from 2013 to 2014, according to AFP's 2014 Payments Fraud and Control Survey.[1] The drop in check fraud corresponds with the declining popularity of checks; however, payment by check continues to account for 50 percent of all business-to-business payments made in the United States.[2]

The decline in check usage is largely attributable to the efficiency and ease of alternative forms of payment, namely online payment services, credit cards, debit cards, and wire transfers. For example, in most European countries, it is customary for businesses to publish their bank details on invoices so that the customer can pay via giro. A *giro* is a method of transferring money by instructing a bank to directly transfer funds from one bank account to another without the use of checks. This method of payment is predominantly used in Europe, where giros are seen as an effective way for companies to receive payments from foreign customers. Despite the declining use of checks, financial institutions and merchants that still use and accept this form of payment must be aware of the red flags of a fraudulent check.

Due to demands on law enforcement, prosecutors often fail to pursue bank check fraud cases. Many merchants have tried to use the police and prosecutors as check collection agencies; therefore, law enforcement and prosecutors are often not eager to pursue these cases. Furthermore, many purveyors of check fraud are constantly migrating from one location to another, making prosecution even more difficult.

The best solution for financial institutions and merchants, then, is to educate employees to recognize forged and fraudulent checks and the schemes behind them. Merchants and financial institutions should have a strict check acceptance policy with which all employees are familiar. When accepting checks, employees should always ask for identification and make sure it is valid. Many check passers mollify store personnel by showing them a small

[1] The full text of the 2014 AFP Payments Fraud and Control Survey can be found at: www.chase.com/content/dam/chasecom/en/commercial-bank/documents/2014-payments-fraud-survey.pdf.
[2] www.afponline.org/epayments

laminated rectangular document with a picture. After looking at several hundred of these, most employees tend not to scrutinize them. Check passers count on this. It is important for employees to examine each piece of identification closely every time they are presented with one.

Counterfeiting Checks

An effective check counterfeiting operation can turn a small financial investment into a fortune within a short timeframe. This can be done without high levels of computer expertise or expensive software. Often, all that is required is a quality computer, color inkjet printer, check format and MICR font software, magnetic ink cartridges, and paper stock.

Check counterfeiters commonly recruit other individuals to cash the checks for them. This allows the suspects to distance themselves from the transaction and avoid being identified by law enforcement. In many cases, the persons presenting the checks have no identifying information about the actual counterfeiters.

Signs of Counterfeit and Forged Checks

A counterfeiter will go to great lengths to make his check appear to be genuine. However, there are a few clues that a check is counterfeit. If the printing on the check does not seem uniform in texture and color or slants up or down, the check is likely counterfeit. Also, in the United States, the financial institution's routing transit number must match the first nine numbers at the bottom left portion of the check. These numbers occasionally do not coincide on altered checks, often due to the fraudster's attempt to slow down the check clearing process. The check number itself should typically be found both in the check's upper-right corner and in the encoded serial number at the bottom.

Knowing that many merchants regard checks with low check numbers as suspect, forgers often attempt to add a digit. Here again, they might have difficulty matching the ink used to produce the check. A simple and effective method of detecting bad checks is to fan a group of checks. Counterfeit checks will sometimes stand out as a slightly different color.

Check Fraud Vulnerabilities

A particular institution might be targeted for check frauds because of its location, inadequate internal controls, or marketing strategies that present opportunities to savvy check fraud artists. Some mutual fund companies, for example, regularly allow customers to open accounts by mail, a form of communication with many security vulnerabilities. A significant

number of check fraud complaints from a particular geographic area might indicate the presence of an active, organized group, which warrants law enforcement attention.

Investigators assigned to a region or institution should keep regular contact with businesses and regulators. Specific inquiries aim to identify weaknesses, develop controls, and prevent future losses. Analyzing the complaints filed by other victims of check fraud—including retail operations, check-cashing establishments, and food stores—might reveal common elements of schemes that might not otherwise seem related.

Check Theft

Three types of check theft are: using stolen canceled checks to obtain new checks, check washing, and stealing blank check stock.

- *Stolen canceled checks and statements*—Although a stolen canceled check cannot be negotiated, it does have fraud implications. Using a stolen canceled check, a check thief can order checks from a mail-order check printer and have them sent to a mail drop address. Checks can then be written on the new stock and cashed once false identifications are acquired.
- *Check washing*—Check washing is a type of check fraud that involves using acid-based chemicals found in common household products to erase particular pieces of information, such as payee name or amount, while simultaneously being careful not to alter the check issuer's signature. The check is allowed to dry, after which a new payee and payment amount are inscribed. Fraudsters who perpetrate check washing schemes usually write the checks for relatively modest amounts to decrease scrutiny and reduce the chance of exceeding the check issuer's account balance. As checks issued using colored inks and ball-point pens tend to be most susceptible to the chemicals used in these schemes, experts recommend using black ink and gel pens when writing checks.
- *Stolen check stock*—Professional thieves using sophisticated methods steal blank check stock already encoded with customer account information, which makes passing the check even easier. Corporate checks are the most likely target since they are easily cashed and deposited.

Check Fraud Schemes

Paperhangers

Paperhangers are the experts of phony check passing. They frequently pick a particular establishment or store and observe its security methods. Any store that scrutinizes check writers' identification is not a good target for paperhangers. However, they will observe and

choose to pass the check to the least experienced or most lackadaisical of store employees. The paperhanger will then ask the clerk for cash back from the transaction and make the check out for an amount greater than the price of the purchase. In some cases, the checks being written are counterfeit; however, in other cases the checks are purposefully being written on a closed account. A variation of this scam is making a fraudulent deposit at a bank and asking for cash back.

Stop Payment Orders

This scheme is quite simple. A "customer" purchases an expensive item with a check and then notifies his bank to stop payment. Savvy check passers might even contact the merchant, saying the item was defective, and that they should expect to hear from the customer's legal representative. Meanwhile, the check passer sells the item for a tidy profit.

Another scenario is that, after purchasing the item and notifying the bank to stop payment, the fraudster goes back to the store, wishing to return the item and receive a full refund. The merchant refunds the amount in cash and the scheme is successful.

Check Kiting

Check kiting is one of the original white-collar crimes. It continues to survive even with a financial institution's ability to detect kiting. Check kiting is the practice of recording the deposit of an interbank transfer before recording the disbursement, thus briefly double-counting the amount of cash. In a kiting scheme, multiple bank accounts are opened and money is "deposited" from account to account; however, the money never exists.

Floating makes check kiting possible. Floating is the additional value of funds generated in the process of collection and arises because the current holder of funds has been given credit for the funds before the check clears the financial institution upon which it is drawn. Businesses are most susceptible to check kiting if they have employees who are authorized to write checks or make deposits in more than one bank account. Today, check kiting is more difficult because technology allows for a much shorter float period. In many cases, electronic debiting to an account occurs simultaneously with the transaction. Unless detected, this process can continue indefinitely, covering one check written against insufficient funds with another check.

Demand Drafts

A *demand draft* is a check created by a seller that has a buyer's checking account number but no signature. Demand drafts can also be used to commit check fraud. Demand draft fraud involves the misuse of account information to obtain funds from a person's bank account without that person's signature on a negotiable instrument. Other terms for demand drafts are "preauthorized drafts" and "telephone drafts." While there are many legitimate business uses for demand drafts, such as quick-turnaround telephone transactions initiated by airlines and car rental companies, demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts without them realizing that such withdrawals are occurring.

Check Fraud Rings

While organized crime syndicates are most commonly associated with drug trafficking and violent crimes, they are also significant purveyors of check and credit card fraud. Most major financial institutions attribute more than 50 percent of all check fraud to organized crime rings. Additionally, the 2014 AFP Payments Fraud and Control Survey revealed that organized crime rings were responsible for 17% of all reported check and credit card payment fraud.

In 2012, more than 40 members of an organized crime ring operating out of Houston, Texas, were arrested for participating in a massive check fraud scheme. Members stole rent checks and money orders from more than 100 apartment building lock-boxes. After washing and counterfeiting the checks, members of the gang recruited countless other individuals, including homeless people, to cash the fraudulent checks at various establishments.

Check fraud rings thrive because the items needed to commit check fraud are easily obtainable and the total cost is minimal. Often, the only necessary equipment for a check fraud ring is a scanner, printer, and a personal computer. Moreover, check fraud is considered a relatively low-risk crime; the chances of being arrested and prosecuted are low, and the penalties are relatively mild.

Many rings specialize in payroll or other institutional checks, written for relatively small amounts. But some groups infiltrate financial institutions, collecting corporate payroll checks, money orders, and master original bank checks, and then cashing the duplicates for several thousand dollars.

Some crime rings have infiltrated or obtained accomplices in financial institutions and use that position to gather personal information on customers, passing the information to counterfeiters who produce falsified identification (driver's licenses, credit cards, etc.), which is used to open accounts, establish lines of credit, and secure loans. Other crime rings obtain the information needed to commit large-scale check fraud from illicit sources on the *deep Web,* a notorious segment of the Internet that is not accessible by conventional means.

An organized group might include a counterfeiter or printer, a distributor, one or more providers of false identification, and several co-conspirators who open false bank accounts or visit check-cashing establishments to negotiate fraudulent checks.

Crime rings that practice check fraud tend to be ethnically homogenous and are usually not rigidly structured. It is common for only the leaders of these rings to know the extent of their subordinates' participation. The leaders of such groups are usually quite intelligent and educated. Often, they have an extensive criminal or business background and direct the group's activities. Gangs have been known to share members and cooperate with one another in the past.

Check Fraud Detection

Techniques

The cashier or teller is the frontline defense in preventing check fraud. It is important that these individuals receive the training necessary to identify fraudulent checks. They should:

- Be aware of magnetic routing numbers.
- Use extra care in examining a check drawn from a non-local bank and require positive identification.
- Examine the date on the check for accuracy of day, month, and year. Do not accept the check if it is not dated, if it is postdated, or if it is more than 30 days old.
- Be aware of fonts used to print the customer's name that are visibly different from the font used to print the address.
- Be aware that the magnetic ink (MICR) used for routing codes should appear non-reflective and dull.
- Look for MICR coding that does not match the bank district and the routing symbol in the upper right-hand corner of the check.
- Be aware of the date that the account was opened.
- Be aware of stains or discolorations on the check possibly caused by erasures or alterations.

- Have easy access to the signature card.
- Look for perforated edges on the checks.
- Be aware that a color copy might reflect odd colors at times due to a failure of the toner to mix satisfactorily.
- Notice the absence of any design in the background of the check paper.
- Notice the absence of a bank logo and the printing of the bank name in the regular lettering.
- Notice the absence of the bank's address on the check.
- Be cautious of information that is typed or stamped.
- Do not accept a check that is not legibly written. It should be written and signed in ink and must not have any erasures or written-over amounts.
- Be aware of what is acceptable identification.
- Recognize forged/altered information.
- Recognize forged negotiable instruments.
- Telephone the business or account officer for approval on suspicious requests.
- Be familiar with patterns of behavior related to potential culprits:
  - Overly polite
  - Nervous
  - Aggressive and hurried

Check Fraud Prevention and Investigation

Special security printing techniques have been developed to make counterfeiting blank checks more difficult. One of the features is the use of a pattern of colors that is difficult to separate even with special cameras, filters, and film. Another technique used is scrambled indicia printing, which is a seemingly random pattern of tiny colored dots printed on the paper. Using a colored filter to view the check will make a word or pattern develop.

An additional technique, which is also used by credit card issuers, is to print a "micro-line" on the check, which appears as a solid line when viewed normally. Using a magnifying glass will show that the line is actually very small words or letters, which are very difficult to recreate with the normal printing process. Other security measures include using a three-dimensional hologram that is easily identifiable by the human eye, but is impossible to reproduce via ordinary copying or printing. Some checks have a security seal on the back that is visible when held up to a light. Reproductions, even good ones, will not have a seal.

Check Fraud Investigations

During a check fraud investigation, look for the following:

- Frequent deposits and checks:
  - In the same amounts
  - In round numbers
  - With checks written on the same (other) bank
- Frequent ATM account balance inquiries
- Many large deposits made on Thursday or Friday to take advantage of the weekend
- Large periodic balances in individual accounts with no apparent business
- Low average balance compared to high level of deposits
- Many checks made payable to other banks
- Bank willingness to pay against uncollected funds
- Deposits not made daily or intact
- Entity uses receipts that do not indicate mode of payment
- One or more personal checks in the cash drawer by the fund custodian
- Deposit timing lags
- Irregular check endorsements
- Amount of deposit does not agree with daily activity report
- Inappropriate access to signature plate
- Check numbers, payee name, date, and amount do not agree with entries in the check register
- Voided checks are not retained
- Checks issued to individuals for large, even dollar amounts
- Supporting documentation for checks is not available or has been prematurely destroyed
- Cash withdrawal with deposit checks drawn on another bank

There are several tips for businesses to use when cashing business and payroll checks:

- Examine all checks.
- Insist that the check be signed in front of the clerk.
- Compare the signature written on the check with the signature on the driver's license or government-issued identification.
- Be particularly careful with large-dollar checks presented by noncustomers.
- Examine all checks for signs of counterfeiting, such as a glossy, wax-like appearance and any lack of detail and sharpness.
- Look for signs of alterations or erasures, especially in the signature or numerical and written amounts.

- Compare the bank identification and routing numbers for a match.
- Verify that the texture of the check appears smooth; a rough document might signal erasures.
- Be cautious of information that is typed or stamped.
- Know that all checks, except government issue, should have at least one perforated edge.
- Know that the magnetic ink used for routing codes should appear nonreflective and dull.
- Look for faded colored paper, which can indicate that the check has been chemically bleached.
- Know that a color copy might reflect odd colors at times due to a failure of the toner to mix satisfactorily.
- Know that black lettering might have a slightly greenish cast when examined under a magnifying glass.
- Know that a light colored or delicate background might fade out when copied.
- Look for the absence of any design in the background of the check paper.
- Look for the absence of a bank logo and the printing of the bank name in regular lettering.
- Look for the absence of the bank's address on the check.
- Examine checks for an overall appearance of poor-quality printing and paper.
- Know that a payroll check will usually be for an odd amount and will appear neat, clean, and usually unfolded.

Tellers should telephone the business or account officer for approval on suspicious requests.

Check Fraud Prevention Tools

FORENSIC DOCUMENT EXAMINATION

Through handwriting, an individual can be positively identified, as is the case with DNA or fingerprinting. When investigating check fraud, a forensic document examiner focuses on the signature and the handwriting itself.

SIGNATURE

If the fraud examiner is investigating a forged signature, he should compare the suspicious signature to a sample of the actual one, noting discrepancies between the two. While one's signature might change over time, it would be close to impossible for a forger to duplicate a signature with 100 percent accuracy; minute identifying characteristics mark people's writing and are not reproducible.

HANDWRITING

Like fingerprints, handwriting is unique to an individual. Consequently, if the narrative portion of the check is handwritten, it offers a document examiner a greater opportunity to identify a forgery.

ELECTROSTATIC DETECTION APPARATUS

An electrostatic detection apparatus allows fraud examiners to detect indented writing from the top page of a pad of paper up to five pages below the original. This tool uses photocopier toner to develop the areas of indentation after a document has been covered with an electrically charged plastic film. In the best of cases, when the document is processed with the electrostatic device and the toner image is developed, the writing impressions are clearly defined and highly contrasted. If the developed writing is to be used in an investigation or to demonstrate results for the courts, the fraud examiner must turn to electronic image processing technology for further enhancement.

Credit Card Fraud

Credit card fraud is the misuse of a credit card to make purchases without authorization, or counterfeiting a credit card. Credit card fraud is successful because the chances of being caught are small and prosecution is not ensured. Retail stores have identified credit card thieves and contacted law enforcement only to receive little or no response regarding the crime.

Credit Card Schemes

There are many different types of credit card schemes, including selling the cards to thieves, family members using the credit cards without authorization, and fraudulently obtaining a card.

Unauthorized Use of a Lost or Stolen Card

Fraudulent activity normally occurs within hours of the loss or theft, before most victims have called to report the loss. Victims are commonly unaware that their credit cards are being used fraudulently until they review their monthly statement. It is important that victims report the loss or theft of their card within 60 days of receiving the statement with the fraudulent charges, as they will not be held responsible for any charges (beyond $50) that occur during that timeframe. If the credit card company is not notified of the theft and the card is used, the customer will be liable.

Organized Crime Rings

Organized crime rings are especially notorious for stealing or purchasing credit card and bank information from various sources. These articles are used to generate false identification documents, such as driver's licenses and government identification cards. The credit cards themselves are duplicated and distributed to members of the rings. The false IDs are then displayed during purchases made with the stolen cards. Members of the ring go on spending sprees, ending only when the credit has been fully used or the legitimate owner reports his card as stolen. Often, counterfeit and stolen cards are express-mailed to members of the ring in other parts of the country.

Advance Payments

Consumer regulations require credit card issuers to credit customers' accounts immediately upon receipt of payment. This means deducting from the balance of the account before the check or other payment instrument has actually cleared the bank. A loophole such as this is easily exploited by experienced fraud rings.

Using a forged or counterfeit check, an advance or overpayment is made on a stolen credit card. Since the issuer must credit the payment at the time it is made, there is no time to verify the check's authenticity. Consequently, cash advances and purchases can be made immediately. This scheme can be extremely lucrative to the perpetrators.

Stolen Card Numbers

The Internet has become the primary venue for the trafficking of stolen credit card information. The thieves who steal this information find credit cards or lists of credit card holders and their corresponding account numbers. They then make the numbers available to a larger group, which uses the information to obtain goods and services in the cardholder's name. Credit card and personal information is commonly obtained through burglaries, skimming, and data breaches. The information is then sold to brokers, who are commonly based in Russia or Eastern European countries, and then sold through websites located on the deep Web, where countless underground websites specialize in the sale and trade of illicitly acquired information. Many sites wantonly trade in this information, with entire sections devoted to payment card fraud, account frauds, personal information, and generic services. These sites are often surprisingly sophisticated, offering customer reviews, multiple payment options, and guarantees. The international and dispersed nature of the fraud makes it arduous to deter or prosecute.

Counterfeit Cards

Another type of bankcard fraud involves the illegal counterfeiting of credit cards. Known as "blank plastic" cards, this scheme uses credit-card-sized plastic with embossed account numbers and names. This scheme works in conjunction with a corrupt and collusive merchant or a merchant's employee. Other counterfeit cards are wholly manufactured using high-speed printing facilities and are used in association with organized crime groups.

Counterfeiting operations are centered in Taiwan, China, and Hong Kong, since these countries manufacture the holograms and magnetic strips that appear on many cards. Forged holograms are smuggled into and distributed throughout other countries around the world by crime ring members.

The actual counterfeiting process has been immeasurably eased by technology that allows for more accurate duplication. Duplicating legitimate cards is still an intricate operation, however. Magnetic strips, numbers, holograms, and logos must all appear authentic. Desktop computers, embossers, tipping foil, and laminators are common tools in the reproduction process. Perhaps the most difficult of all to accurately reproduce, however, is the hologram. True holograms use a "lenticular refraction" process; counterfeits are generally only reflected materials, usually a foil with an image stamped on it. These decals are attached to the card's surface rather than fixed into the plastic, as is the case with legitimate cards. Some holograms do not change colors, as legitimate ones do, when viewed from various angles. Counterfeit credit cards are the most damaging scheme of those mentioned here. However, with the increasing use of chips inside the cards and the addition of a PIN (Personal Identification Number), counterfeiting cards has decreased significantly as a method of bank card fraud in countries using this technology.

Telephone/Mail Order Fraud

The fraudster might offer a free trip or other nice prize, with the only catch being that the winner must have a credit card. Once the thief has the number, he can order merchandise or have money wired to himself.

A great deal of credit card fraud is simple to complete. Many perpetrators have great success by simply calling a person at random and pretending to be a credit card representative. The victim is told that his card number might have been obtained and used illegally by criminals. Alternatively, a supposed travel agency representative might call, claiming the victim has won a discount travel package. In any case, the victim is asked to read the card number off for

verification or inclusion in the discount deal. A surprisingly large amount of people fall for this scheme and give out their credit card information. Purchases through catalogues and mail order are then made using the victim's card number. They might select an unoccupied address to which their merchandise can be delivered, perhaps leaving a note asking the delivery service to simply put the package by the back door.

False Applications

Perpetrators might apply for a new card using information stolen from a wallet, purse, or the garbage. Additionally, they might steal a preapproved credit card application out of the mail or trash, or they might use credit card applications that are prominently featured in store displays.

Credit "Doctors"

Credit doctor is the term used for fraudsters who sell stolen credit card account numbers to people unable to get credit cards.

True Name Fraud

New credit card accounts can be opened by individuals possessing a victim's true name identification such as a driver's license or government-issued identification number. The true identification was either obtained as a secondary objective in the commission of a more aggressive offense, such as robbery, or as the primary target of a lesser crime, such as pick pocketing.

Non-Receipt Fraud

Non-receipt fraud is a form of credit card fraud in which the perpetrator intercepts credit cards that are in transit between the credit issuer and the authorized account holder. Losses attributable to mail theft have declined significantly as a result of "card activation" programs, in which the cardholder must call his financial institution and confirm his identity before the card is activated.

Key-Enter Counterfeiting

Credit card security codes are designed to provide protection against credit card fraud. These codes are typically three or four digits long and are independent of the account number and PIN. They are primarily used to secure cards used in transactions occurring over the Internet, by mail, or over the phone.

When banks began using card security codes, fraudsters came up with a clever ruse in response. For instance, the card verification value (CVV) system, which is used by Visa, features a three-digit number embedded in the magnetic strip of a credit card, identifying it as a legitimately issued credit instrument. Credit card counterfeiters figured out a way to beat the system. By leaving the magnetic strip uncoded or making it unreadable, fraudsters force merchants handling the transaction to enter the credit card number manually. This means the transaction never falls under the scope of the CVV system.

Clever bank and credit card officials very quickly found a patch for this scheme, though. The CVV2 and CVC2 systems use a three-digit security code that is printed on the backs of cards. It is designed to validate that a genuine card is being used during a transaction. When a point-of-sale (POS) terminal reads a card's magnetic stripe, Visa's Card Verification Value (CVV), MasterCard's Card Validation Code (CVC), or Discover's Customer Identification (CID) number can be verified during the authorization. Merchants using CVV2/CVC2 can expect to reduce their chargebacks by as much as 26 percent. The number appears in reverse italic at the top of the signature panel at the end. The CVV2 and CVC2 programs can also be used to reduce fraud in card-not-present transactions.

Creditmaster

This software program, downloadable from the Internet, allows the user to produce valid credit card numbers. Counterfeiters can then put these numbers to use in phony cards.

Probing

The fraudster sets up a computer program that lets him run stolen numbers through various financial institutions in the hope that one of them will still honor the number. Numbers that clear are often sold en masse to counterfeiters.

Skimming

This scheme requires a device, often referred to as a *skimmer* or a *wedge*, that scans and stores a large amount of credit card numbers. Credit card skimming is more frequent in businesses where an employee is able to remove the card from the customer's view to process the transaction before returning it to the customer.

Credit cards known for having high credit limits tend to be favored targets. This scam might occur in a retail situation in which a credit card is processed behind a tall counter, or in a restaurant scenario wherein a waiter walks away with a customer's card to process the

transaction. A restaurant patron, for example, hands his credit card to a waiter who swipes the card through a wedge while conducting the legitimate transaction. Once the waiter has collected enough numbers, he can either sell them to a counterfeiter or produce his own fake cards using the stolen information. It might be months before the customer notices phony transactions on his statement, making the point of loss very difficult to determine. It follows that the guilty waiter is, therefore, unlikely to be caught.

Skimming can also be performed via the attachment of covert devices to ATMs, automated fuel dispensers, vending machines, or self-service checkout kiosks. These devices are occasionally paired with a tiny hidden camera meant to record the input of a user's PIN code. Consumers must be wary of any credit card readers that seem awkwardly installed, or appear to have been tampered with.

Pretext Calling

Some fraudulent actors will call unsuspecting customers and pose as bank or credit card agents. The actor will request account information or other identifying information from the victim and use the information to apply for additional credit cards or use the credit cards to purchase goods or services.

Account Takeover

The fake actor might take over a victim's account by requesting a change of address on the account and then calling to report the card lost or stolen. The issuing bank will then send the replacement card to the new address.

Institutional Identity Theft and "Spoof" Sites

Fraudulent actors might create false Internet sites, pretending to sell goods to buyers who must enter their credit card information and other personal information to make purchases. The "seller" then uses the information to make fraudulent purchases in the buyer's name. More recently, fraudulent actors have begun creating "affiliate" sites of actual sellers or other creditors, such as banks. The perpetrator of the fraud then sends emails to existing customers of the actual seller or creator. These emails inform the unsuspecting customer that there is a problem with his account and ask the customer to log on to the company's site that the wrongdoer has copied and to re-enter his personal and credit card information. The fraudulent actor then uses the information to make purchases.

Information on how to commit credit card fraud is readily available to anyone willing to make the effort to look. Postings on the Internet give step-by-step instructions on how to obtain carbon paper receipts and call credit-reporting agencies using merchant numbers. The latter is done to verify that the card is valid and to obtain the amount of credit available. The fraudster usually watches a store employee dial the number of the agency, noting the numbers as they are dialed. He then listens to the employee give the merchant number. This number can often be found next to registers and can be copied down if in plain sight. The fraudster now has an excellent avenue to test stolen cards.

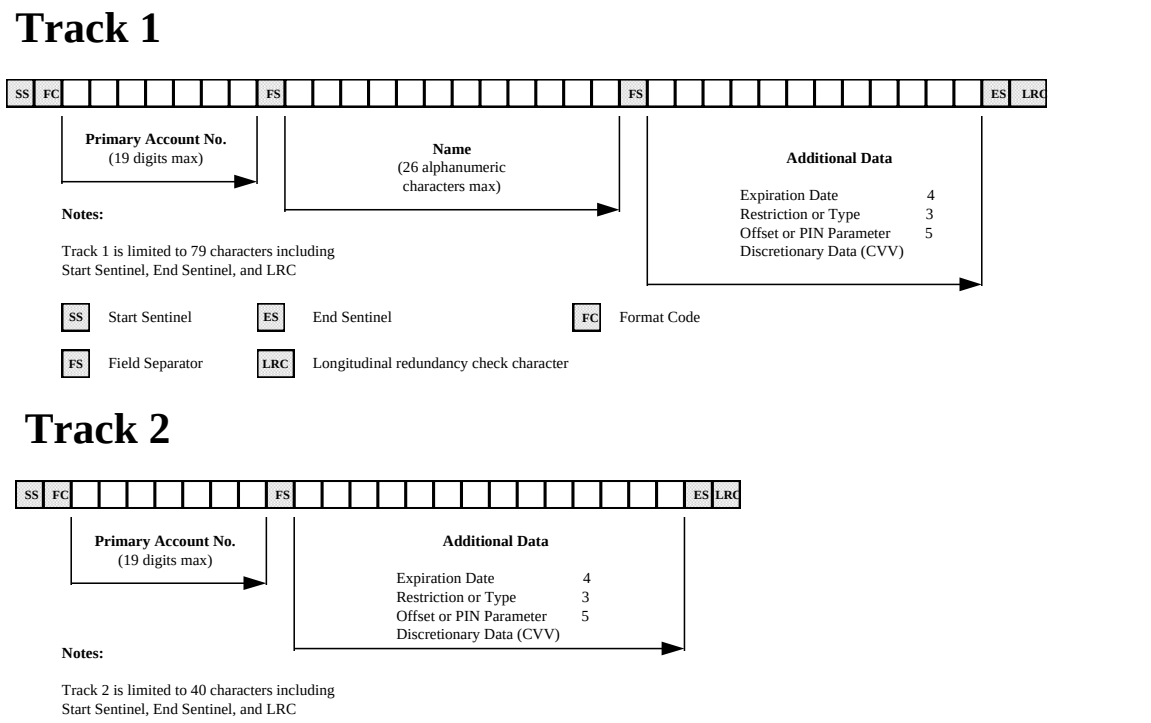
Merchant Scams

Collusion occurs between the sales people and the credit card fraudster to process valid credit card numbers on blank plastic cards. They might also make several imprints on sales tickets and fill them in at a later time.

Magnetic Stripe Compromise

Magnetic stripe compromise is a more sophisticated method of obtaining account information for fraudulent purposes. It requires the transfer, or encoding, of legitimate account information, along with a security code, from the legitimate magnetic stripe to a counterfeited card with a magnetic stripe. The full, unaltered, legitimate magnetic stripe must be obtained to accomplish fraud via this method.

Magnetic Stripe Diagram



As shown in the Magnetic Stripe Diagram, two tracks appear on the credit card's magnetic stripe. Track two is the most widely read. It is 40 characters in length; is strictly numeric; and contains the account number, expiration date, a security code, and discretionary bank data. Track one is 79 characters in length, is alphanumeric, and contains this information plus the cardholder's name.

Company Credit Cards

Company credit cards are provided to employees for convenience in conducting company business. No personal expenses may be charged on the company credit card except as specifically authorized by company procedures. The employee must pay any charged personal expenses promptly. Company credit cards should not be used to avoid preparing documentation for direct payment to vendors. Where allowed by local law, charges on company credit cards for which a properly approved expense report has not been received at the time of an employee's termination of employment may be deducted from the employee's last paycheck. The company will pursue repayment by the employee of any amounts it has to pay on the employee's behalf.

Guidance for Cardholders

It is in both the issuing bank and the cardholder's interest to minimize credit card fraud. Although liability for credit card fraud is limited in many countries (e.g., liability for lost or stolen credit cards is limited to $50 in the United States), cardholders might have to spend significant time and money (including possible legal expenses) to refute fraudulent credit card accounts or transactions. In addition, while cardholders might be aware of identity theft's pervasiveness, they might not be familiar with its consequences or know ways to prevent or minimize its effects. Since issuing banks will not often bear the losses related to identity theft that involves credit cards, banks should inform cardholders of ways to protect physical cards and combat the risk of identity theft.

Banks should send cardholders occasional reminders of steps that can be taken to safeguard their credit card identities, including the following:

- Always carry the least amount of credit cards with you as necessary.
- Do not supply credit card information to unauthorized people.
- Do not leave credit cards unattended with merchants.
- Routinely review credit card statements and immediately report any unrecognizable charges.
- Immediately report the loss or theft of any credit card to the card issuer.

- Obtain credit reports annually in order to detect any suspicious activity in which credit cards or other extensions of credit have been granted or applied for without your consent.
- Never reveal account numbers or other credit card account information to persons attempting to gain your information on the telephone after they represent themselves as agents of a bank.
- If you are aware of suspicious activity, immediately inform the relevant credit reporting agencies and have a "Fraud Alert" placed on your account. This will prevent any potential new creditor from granting new credit without first contacting you personally.
- Always keep credit card receipts in a safe place, and destroy them after you have received the billing statement that reflects the charges.
- If you receive a credit card you did not apply for, call the issuer and determine why it sent the card. Someone might have applied in your name and missed the opportunity to steal the card from your mailbox when it arrived.
- Void incorrect receipts and destroy carbon copies of credit card slips.
- Keep a record of account numbers, expiration dates, phone numbers, and addresses of each card issuer so that you can contact them in the event of the loss or theft of your credit card.
- Do not lend your card to another person.
- Do not write your account number on a postcard or the outside of an envelope.

Prevention and Detection of Credit Card Fraud

The essential part of any detection program is the education of the tellers and merchants who are responsible for handling the transactions. It is widely suspected that the vast majority of store clerks and cashiers do not check credit card signatures or request identification from a customer who presents them with a credit card.

While any of the following can occur in a perfectly legitimate transaction, these characteristics are frequently present during fraudulent transactions. Tellers and merchants should be advised to be alert for the customer who:

- Takes a card from a pocket instead of a wallet or purse
- Purchases an unusual number of expensive items
- Makes random purchases, selecting items with little regard to size, quality, or value
- Makes several small purchases to stay under the floor limit, or asks what the floor limit is

- Does not ask questions on major purchases
- Signs the sales draft slowly or awkwardly
- Charges expensive items on a newly valid credit card
- Cannot provide photo identification when asked
- Rushes the merchant or teller
- Purchases a large item, such as a television, and insists on taking it at the time, even when delivery is included in the price
- Makes purchases and leaves the store, but then returns to make more purchases
- Becomes argumentative with the teller or merchant while waiting for the transaction to be completed
- Makes large purchases just after the store's opening or as the store is closing

Tellers and merchants should be aware of the common signs of forged credit cards:

- Holograms crudely stamped or badly faked with tiny bits of aluminum foil
- Misspelled words on the card
- Altered signature panel
- Discolored
- Glued
- Painted
- Covered with white tape
- Cards that appear to have been flattened and restamped

At the consumer level, the credit card user should remember the following:

- Know where your card is at all times.
- Never leave your card unattended.
- Do not leave the store or ATM without all receipts.
- Do not leave your card in plain sight where others can get the number.
- Do not leave receipts in a public trash can, hotel, or shopping bag.
- Review monthly statements for accuracy and any items that you might not have charged.
- Review your statements via electronic means rather than waiting for paper statements. If possible, cancel paper statements altogether.
- Destroy expired cards.
- Never reveal your card number over the phone to anyone who has offered you a prize.
- Report missing cards immediately.
- Do not reveal personal information such as your address and telephone number.
- Do not allow a salesperson to record your credit card number on your check.

- Keep your card out of the view of others in a store or at a public telephone so they cannot read the name and account number.
- Use a tiered, see-through container in your wallet for credit cards, so it will be easier to notice missing cards.
- Always check your card when it is returned to you after a purchase. Make sure it is your card.

Prevention

Prevention is the key to reducing credit card losses. Several programs, such as those discussed below, can be implemented to prevent credit card fraud.

Education Programs

Tellers and merchants should be trained to be familiar with the credit card's security features. Although the majority of counterfeit cards contain some of the security features, they are usually not complete and offer indicators that the card is not legitimate. Credit card issuers should take measures to inform their customers about credit card fraud, what the financial institution is doing about fraud, and how the consumer can help.

Liaison with Law Enforcement

Companies should develop a strong liaison with law enforcement. When a company receives intelligence of hot frauds, law enforcement should be notified immediately.

Technological Deterrents

Banks can take advantage of technological developments to deter credit card fraud. These developments can make both the counterfeiting of cards and the fraudulent use of valid cards more difficult. Some of these developments require very little technology. For instance, most credit cards now include verification codes on the back to help merchants match cards used in purchase transactions with authorized cardholders. Card networks also maintain address and zip code verification services so that merchants, especially those involved in Internet or telephone transactions, can determine whether the supposed cardholder lives at the address given by the person placing the order.

Photographs

Photographs of the legitimate cardholder will deter counterfeiting to a degree, though they have become increasingly easy for counterfeiters to purchase. Photographs can be altered, but technological advancements permit digital encoding of the cardholder's image on the

magnetic strip of the credit card. Use of this technology requires specialized processing terminals that add to the cost of fraud detection.

Holograms

Holograms have been used by issuers as security devices since the early 1980s. Not long after their implementation, however, it was found that a very accurate counterfeiting industry was emerging. Even if one assesses the average credit limit of fraudulent cards conservatively, it only takes a few cards in circulation to add up to considerable losses for the issuer.

Signature Panel

Signature panels usually contain images of the issuer's logo. Blank or damaged signature panels are red flags of forged credit cards. Signatures on the panel and the sales receipt should always be compared for consistency. While most merchants might have a policy that employees should compare these signatures, it is often ignored.

Activation of Cards

In an effort to curb credit card fraud perpetrated using the mail, companies sending new cards in the mail do not activate them until the customer contacts the credit card company. Upon contact, the credit card issuer then asks the caller for personal information such as his mother's maiden name and birth date, or other information that the ordinary thief probably would not have. Once the information has been satisfactorily answered, the card is activated for use.

Advanced Authorization

Visa recently unveiled technology for analyzing card transactions both individually and collectively across its network in order to detect emerging fraud patterns. When a credit card is swiped, advanced authorization provides an instantaneous rating of the transaction's potential for fraud to the card-issuing financial institution, including whether the card number was among those lost or stolen in a data-security incident. The system is designed to spot situations where multiple accounts are associated with fraudulent testing or some other type of coordinated attack involving multiple accounts.

CyberSource Advanced Fraud Screen

CyberSource Advanced Fraud Screen enhanced by Visa is the first e-commerce fraud detection system enabled with current worldwide fraud trends and global payment-card usage patterns that provides a comprehensive transaction risk assessment of activity.

Combining this with CyberSource's hybrid system (neural network and rules-based technology) and merchant-activity data provides e-commerce merchants with targeted fraud detection ability. CyberSource Advanced Fraud Screen operates around the clock, 7 days a week, 24 hours a day. It effectively screens shoppers located anywhere in the world and works with all payment cards.

The CyberSource Advanced Fraud Screen's risk-management tool uses frequently updated intelligence about global payment-card usage patterns, including online and offline purchasing profiles, to provide an accurate fraud detection service. This advantage can help merchants lower fraud-related costs by identifying risky transactions and increase consumer goodwill by eliminating unintentional "insults" that might occur from incorrectly declined orders.

Computer Edits

Computer edits are built into some credit cards such that if the card is usually used five times per month, and it is used 25 times in one day, the system will prohibit authorization of further purchases.

Card Scrutiny at Point of Sale

How often do merchants scrutinize your card? In many stores, they never get the chance. Consumers use the credit/debit card machines at the sales counter and the cards never leave their possession. While this makes things more convenient for the consumer, it often means that the merchant is left holding the bag when a transaction is returned. If one of the key authorization components is missing (e.g., signature, expiration date, authorization number, card imprint), the merchant has to swallow the loss.

Internet/Telephone Orders

With these transactions, vendors never have the opportunity to see the customer's credit card. The only fail-safe, self-protective measure open to them is to postpone delivery until the transaction has cleared the customer's account. In our next-day-delivery society, however, this might be detrimental to some vendors' business. There are a couple of other options open to merchants:

- Check the billing address against the delivery address. Beware of orders with different "bill to" and "ship to" addresses unless the item is intended as a gift.
- Treat orders received from free email accounts with extra scrutiny. Setting up free email accounts is very simple and allows the user anonymity.

- Require all information printed on the back of the card to be produced. In particular, the card verification value—the three-digit number above the signature panel on the back of the card—should be requested.

Potential signs of card-not-present fraud:

- First-time shopper—Criminals are always looking for new victims.
- Larger-than-normal orders—Because stolen cards or account numbers have a limited life span, perpetrators need to maximize the size of their purchase.
- Orders that include several of the same item—Having multiples of the same item increases a criminal's profits.
- Multiple cards used from a single IP (Internet protocol) address—These transactions occur online.
- Orders consisting of expensive items—These items have maximum resale value and therefore maximum profit potential.
- "Rush" or "overnight" shipping—Fraudsters want these fraudulently obtained items as soon as possible to ensure they are received before the company identifies the fraudulent activity and cancels the order.
- Shipping to an international address—A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the country from which the order was placed.
- Transactions with similar account numbers—These transactions are particularly useful if the account numbers used have been generated using software available on the Internet.
- Shipping to a single address, but transactions placed on multiple cards—This could involve an account number generated using special software or the use of several stolen cards.
- Multiple transactions on one card over a very short period of time—This could be an attempt to "run a card" until the account is closed.

Financial Institution Measures

Banks and other financial institutions have great resources at their disposal to prevent fraudulent transactions. Many of them need merely to enforce their existing policies.

- New account screening—Educate personnel to thoroughly check applicants' information, comparing ID information, addresses, and credit reports for accuracy.
- PIN activation—Bank customers are often required to provide personal identification numbers in order to activate their cards over the phone. Callers who are not able to provide the PIN might have manufactured or stolen the card in question.

- Caller ID—Most people calling to activate their card will do so from home. If the number on Caller ID does not match any of the telephone numbers listed in the customer's account information, bank personnel should ask some identifying questions.
- CVV2/CVC2—Implement these systems as soon as possible. They are among the best defenses financial institutions have against credit card fraud.

Smart Cards

A *smart card* is a plastic card, the size of a credit card, embedded with a microchip. These cards are able to identify the user through encrypted information on the chip and must be inserted into a card reader connected to the credit provider's network. The technology is also known as *chip-and-pin* because the user typically must be present with the card and enter a pin code to complete the transaction, rather than provide a signature, as is typical of a magnetic stripe credit card. In some countries, including the United States, a less secure chip-and-signature system is being used instead of chip-and-pin. This system uses a microprocessor-embedded smart card, but maintains the magnetic stripe card's signature verification rather than a PIN.

The worldwide standard for smart card technology is known as *EMV,* which is an acronym for its developers: Europay Mastercard, and Visa. The EMV standard has already been adopted by more than 80 countries and has been proven to sharply reduce fraud related to counterfeit credit cards (magnetic stripe cards, in contrast, have proven far easier to duplicate). However, without a PIN requirement, EMV credit cards that are lost or stolen offer little more protection than the traditional magnetic stripe cards.

A key advantage of smart cards is that, unlike regular magnetic stripe credit cards, these cards cannot be easily replicated. Similarly, smart cards cannot be easily counterfeited, which greatly reduces the potential for fraud. And generally, smart cards are more secure than magnetic stripe cards. Smart cards include a wide variety of hardware and software features capable of detecting and reacting to tampering attempts and countering possible attacks. If someone tries to tamper with a chip on a smart card, the card will detect the intrusion and shut itself down, rendering the card useless.

Despite the advantages that smart cards have over magnetic stripe cards, and although smart cards are designed to withstand different kinds of potential attacks on security, smart cards are not immune from attacks. There are four main classes of attacks on smart cards: physical, side-channel, software, and environmental. *Physical attacks* are invasive attacks that seek to

reverse engineer the target card and determine the card's secret key(s). *Side-channel attacks* exploit information learned by observing smart cards' power consumption and electromagnetic emissions. *Software attacks* exploit implementation vulnerabilities in smart cards through their own communication interface. *Environmental attacks* seek to induce faults in smart cards by altering the physical environment around them (e.g., temperature, UV radiation, light).

Depending on the type of the embedded microchip, smart cards can be either memory cards or microprocessor cards.

- *Integrated circuit (IC) memory cards*: IC memory cards have a memory chip with storage space for data; they have no processing capabilities. Although IC cards can hold thousands of times more memory than magnetic stripe cards, their functions are limited to basic applications such as phone cards.
- *Microprocessor cards*: Microprocessor cards, or chip cards, have storage space for data and microprocessors with the ability to process data. In addition, these cards offer other functions such as encryption, advance security mechanisms, local data processing, complex calculation, and other interactive processes.

Electronic Bill Payment and Person-to-Person Payments

As previously mentioned with regard to check fraud, the use of checks is quickly declining in popularity. This is largely thanks to the corresponding increase in popularity of *electronic bill presentment and payment* (EBPP). More people than ever before are foregoing the traditional and inefficient method of mailing checks or using cash to pay their bills. Instead, automatic payments can be set up via the website of a bank or credit card to satisfy these payments. In addition, Forrester Research Inc. reports that 7 percent of retail sales occur online.

Individuals can pay each other for goods or services through this same electronic form, which is known as the person-to-person, or P2P, system. The most popular P2P system is PayPal, but many credit cards and banks have started offering the service to their existing customers as well. P2P payments are made using a computer, smartphone application, or email address.

Online payment services are successful because there are relatively low processing and customer service costs for billers, while customers can reduce time and costs in making payments. With some EBPP systems, customers might even be able to manage their funds

more effectively. Electronic bill payment has received faster acceptance than bill presentment, though acceptance appears to be dependent on the prices of these services. As the EBPP method of payment continues to increase, it is important to be prepared to combat fraud that might surface in this area.

Giro

A *giro* is a payment transfer from one bank account to another bank account instigated by the payer. Giro transfers are practiced primarily in European countries and are often used to receive payments from foreign banks. The use of checks and paper giros has declined in favor of electronic payments, which are faster, cheaper, and have a reduced risk of fraud.

Electronic Funds Transfer

An *electronic funds transfer* (EFT) is any transfer of funds, other than one originated by a check or similar paper instrument, that is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape that orders or purports to authorize a financial institution to debit or credit an account. Each of the following could be considered an electronic funds transfer:

- A customer's withdrawal of funds from his own account by an ATM
- A customer's transfer of funds from his checking account to his savings account at the same financial institution initiated by him through his personal computer
- A customer's transfer of funds from his checking account to his savings account at the same financial institution initiated by him through the bank's automated telephone service
- A customer's use of a debit card to purchase goods from a merchant who swipes the card through a point-of-sale (POS) device to authorize deduction of the amount of the sale from the customer's checking account
- A customer's transfer of funds from his bank account to a third party initiated by the customer through his personal computer
- An employer's instruction, initiated by computer or through a magnetic tape, to a financial institution to deposit funds representing an employee's pay into the employee's account
- A noncustomer's instruction, initiated by computer or through a magnetic tape, to a financial institution to withdraw funds from the checking account of a customer and transfer the funds to a noncustomer's bank account

Electronic Bill Presentment and Payment

Electronic bill presentment and payment (EBPP) involves the presentment of bills from one or more sellers of goods, or providers of services, to a consumer through electronic means and the payment of that bill by the consumer, also through electronic means. Some experts expect EBPP to become one of the fastest growing applications of electronic funds transfers.

At present, EBPP systems vary in organization and complexity. They might involve a transaction between a single merchant and a customer, the consolidation of multiple bills from different billers, or the consolidation of multiple payments from different customers. Initially, EBPP systems were offered by proprietary providers. More recently, however, banks have begun to enter the field, often by contracting out implementation of the system to proprietary providers. Banks might have an advantage in marketing these systems because consumers who are likely to use these systems often have existing relationships with their banks. Bank customers, therefore, might be more willing to trust those institutions to handle their accounts than to entrust funds to a new entity with which they have no previous or tangible relationship.

Biller Direct Systems

Existing EBPP systems usually fall within one of two categories: biller direct systems and consolidation/aggregations systems. In a biller direct system, merchants deal with each customer individually. In a typical transaction, the customer will enter an Internet site that the biller has created. There, the customer who wishes to pay his telephone bill online will simply log on to the telephone company's website, enter a username and password that allows the customer to pull up a copy of his bill, review it, and instruct the biller to obtain payment from the customer's bank account. Prior to this time, the customer will have entered into an agreement with the biller to receive and to pay his bills electronically. The customer will usually have created the username and password and will have provided the biller with information about the customer and the customer's account at the financial institution from which the biller might collect payment. Typically, this will include the customer's email address, the routing number of the customer's bank, and the customer's account number at the bank. In some systems, the biller will send an email to the customer indicating that a bill is outstanding and directing the customer to the biller's website.

After the customer views the information posted by the biller, the customer may approve the information and authorize payment. The biller will then initiate payment by contacting a

payment provider that has agreed to collect payments on the biller's behalf. The payment provider will contact the financial institution that holds the customer's account and request that the institution debit the customer's account and remit the proceeds to the payment provider. The payment provider will then credit the proceeds, minus any fees, to the biller. These payments may be transferred through an ACH transfer or through a paper transfer such as a cashier's check when the recipient is not able to receive payments in an electronic form.

Person-to-Person (P2P) Payment Systems

Personal online payment systems, often called P2P or person-to-person payment systems, are popular ways for making relatively small payments between individuals or between an individual and a business. These payments are used in the online auction market, where winning bids might be too small to justify the use of a credit card or the seller is an individual who does not accept credit card payments. In 2002, eBay, the online auction site, acquired PayPal, the dominant provider of P2P services. PayPal currently has more than 148 million accounts worldwide, and is available in 190 markets and 17 different currencies. The success of proprietary systems like PayPal has induced conventional banks to consider entering the P2P arena. Many banks now offer similar services.

One restriction of most current P2P systems is that they will only complete transfers to individuals who are also subscribers to the service. While this restriction might help a system to gain a customer base and reduce fraud by obtaining information about recipients, it also limits the scope of potential users.

A Model of P2P: PayPal

There is a significant opportunity for change and growth in implementation since P2P systems are still in their early stages. PayPal is dominant in the market at this point, so we will use it as a model of the P2P system for illustrative purposes. Potential users of the system must log in to the provider's website and submit registration information, including their name, mailing and email addresses, and phone number. An email is sent from PayPal to the user's provided email address with the user's password. Before initiating any transfers, the user must send that password from the email account that the user indicated at the time of registration. This permits the provider to verify information about the user and reduce the probability that the user is engaged in fraudulent activity or has established an account in the name of a fictitious person.

To make a payment, the user enters his username and password, along with the email address and payment information for the recipient. The user may authorize the provider to withdraw funds from any of three sources. First, the user may maintain an account directly with the provider. Second, the user may authorize the provider to withdraw funds from the user's account at another financial institution. If the user registers his bank account as a source of payment, the provider will verify the user's control of the account by making two small deposits to the account in an undisclosed amount and requiring the user to confirm the amount of the deposits. Third, the user may authorize the provider to charge his credit card with the amount of the payment.

Types of Fraud

There are several ways in which fraud can be perpetrated through EBPP and P2P systems since passwords that allow access into customer bank accounts must be made available to third parties. Also, bills that contain significant information about customers must be passed through multiple parties. Potential sources of fraud include the following:

- A biller might send a bill for services not rendered or for goods never sent.
- A person who has obtained information about another person's bank account might instruct a biller to obtain payment from the other person's account.
- A hacker might obtain passwords and usernames from an aggregator and use that information to direct transfers from a consumer's bank account.
- An employee at the site providing EBPP services who knows consumers' usernames and passwords for screen-scraping purposes might use that information to direct transfers from consumers' bank accounts.
- A bank employee might use customer information to direct transfers from a customer's account.

Unfortunately, the financial institution that offers electronic funds transfers to its customers will have difficulty determining the source of any leak of customer information necessary to initiate a transfer. Therefore, to maintain good relations with its customer and to avoid further liability, a bank might accept responsibility for them. Thus, the best strategy for the bank will be to take measures that reduce the probability that fraud will materialize in the first place.

Detection and Deterrence of Electronic Funds Transfer Fraud

Considering the limited capacity of banks to shift losses from unauthorized electronic funds transfers to their customers, banks should make efforts to minimize the incidence of fraud.

The justification for limiting consumer liability might be that banks are in a superior position to learn of and counteract fraudulent schemes that are employed to effect unauthorized transactions. Banks can take certain initiatives to secure access devices and computers from interference. Banks can also follow "know your customer" rules to prevent the issuance of access devices to individuals who are likely to use them fraudulently.

The following sections provide specific safeguards that banks can perform to reduce the risk that they or their customers become victimized by unauthorized electronic funds transfers.

Issuance and Use of Access Devices

Electronic funds transfer fraud often involves individuals who use information to obtain access to the accounts of others. As a result, bank personnel can prevent fraud by exercising care in the initial decision to allow an individual to access the bank's computerized services. Banks offering EBPP or P2P systems to customers should:

- Confirm phone and mailing addresses on the application to ensure that they are consistent with information about the applicant that is available from other sources and, with respect to existing customers, consistent with current records about these customers. This might involve obtaining credit reports about the applicant or obtaining copies of utility bills that show the applicant's address.
- Make sure that the area or city code on the applicant's telephone number matches the geographical area for the applicant's address.
- Send a "welcome" letter to the address on the application with the bank's return address so that the letter will be returned if the applicant does not live there.
- Verify by telephone or additional mailings any change of address requests in the same way that new account applications are verified.
- If a customer reports the loss or theft of an access device, cancel the existing card, PIN, or other form of access and issue a new one.
- If a customer reports that a person previously authorized to use an access device no longer has that authority, cancel all cards, PINs, or other access devices and issue new ones to the customer.
- Always mail PINs separately from other information, such as usernames, with which they are associated.
- Separate the responsibility of bank employees who have custody of information relating to access devices from those who have responsibility for issuance, verification, or reissuance of PINs.

- Ensure that any communication concerning usernames or passwords is sent in a secure, encrypted format.
- Require customers who register for EBPP or P2P systems to provide information indicating that they are authorized to use the bank account or credit card from which payments will be made.

Operation of Payment Systems

Banks that participate in EBPP or P2P systems can take steps to detect fraudulent transactions, either by providing information to customers or by analyzing transactions that have characteristics associated with fraud. These measures include the following:

- Send customers email alerts when a new bill arrives or a payment is sent. The email should advise the customer to contact the bank immediately if the bill was not expected or the payment was not authorized.
- Refuse or scrutinize any transactions from a payer or recipient who has been the subject of a notice from a credit card issuer indicating that the person was involved in an unauthorized credit card transaction or unauthorized transfer to or from a bank account.
- Ensure that the name on the bank account associated with the P2P account matches the name on the P2P account itself.
- Track and verify payments of similar amounts to the same recipient.
- Since P2P systems are frequently used to make payments for online activities, be aware of activities that are typically associated with fraud and scrutinize transactions with customers who engage in such activities. These activities include pyramid schemes, online auctions, and sale of items that have a delayed delivery date.

Protection of Internet Addresses

Banks or their customers can become victims of fraud, especially identity theft, if they do not carefully monitor the use of their name on the Internet. Fraudulent actors might create false domain names to attract the bank's customers and get them to provide information that will then be used for illicit purposes. This activity, known as *cybercloning*, involves the creation of a "spoof" site, complete with a domain name close to the domain name of a legitimate bank and containing the real bank's logo. An email might be sent asking customers and potential customers to log on to the false domain name. Those who respond might be asked for information such as account numbers and credit card numbers. Alternatively, individuals might register domain names close to the domain name of actual banks and use those sites to market goods or services with which the bank would not want to be associated. For

instance, Citigroup had a battle with an individual who registered the name citicard.com and directed users who logged in to this site to an online gambling site.

Prevention of EFT Fraud in Other Companies

The Information Systems Audit and Control Association (ISACA) recommends several steps for prevention of EFT fraud in companies. The following is a brief overview:

- Define the EFT process and controls points.
- Define EFT policies and procedures.
- Ensure physical security surrounding all EFT components.
- Implement effective EFT application security.
- Implement effective network operating system security.
- Implement effective security surrounding EFT data.
- Implement effective system logging that establishes a baseline that can be used to measure unusual activity.
- Conduct reconciliations to allow for the determination of whether data have been modified during any stage of the EFT process.

INSURANCE FRAUD

The insurance business, by its very nature, is susceptible to fraud. Insurance is a risk distribution system that requires the accumulation of liquid assets in the form of reserve funds, which are in turn available to pay loss claims. Insurance companies generate a large steady flow of cash through insurance premiums. Steady cash flow is an important economic resource that is very attractive and easily diverted. Large accumulations of liquid assets make insurance companies attractive for *takeover* and *loot* schemes. Insurance companies are under great pressure to maximize the return on investing the reserve funds, thus making them vulnerable to high-yielding investment schemes.

Types of Insurance Policies

Property insurance indemnifies against pecuniary loss to the insured's property (and, in some policies, to the property of others) for specific losses, such as those from fire, theft, or auto collision. *Casualty insurance* indemnifies against legal liability to others for injury or damage to people, property, or other defined legal interests because of specified risks or conduct. There are several types of casualty insurance, such as health, disability, life, fidelity, and bonds. *Health insurance* indemnifies against medical care costs under specified circumstances.

Disability insurance indemnifies against income loss under defined circumstances. *Life insurance* indemnifies for the death of the insured. *Fidelity insurance* indemnifies against economic loss to the insured caused by employee dishonesty. *Indemnity bonds* indemnify against loss to third-party beneficiaries when the insured fails to fulfill a specific undertaking for the third party's benefit.

Insurance policies can be marketed in combinations. Homeowners insurance and auto insurance policies usually include features of both property and casualty insurance. Some health insurance plans, for example, also might include disability benefit provisions. There are a multitude of insurance fraud schemes. Likewise, there are fraud schemes that are prevalent only in specific insurance areas. The largest amount of insurance fraud is in health care. Like all other industries, insurance is susceptible to both internal and external fraud schemes.

External health care fraud is perpetrated by outsiders against the company. The two main types of external fraud schemes are those committed by providers (such as doctors,

institutions, and home health agencies) and claim fraud by the insured. Health care frauds—a specific variation of insurance fraud—will be discussed in the "Health Care Fraud" chapter in this section of the *Fraud Examiners Manual.*

Agent/Broker Fraud

Cash, Loan, and Dividend Checks

A company employee requests cash, a loan, or a dividend check without the knowledge of an insured or contract holder and either deposits the check into his bank account or into a fictitious account. To minimize his chances of being detected committing a fraudulent act, the employee might change the company policyholder's address of record to either his address or a fictitious address. Once the check is issued, the address is then changed back to the previous address.

Settlement Checks

Company employees can misdirect settlement checks such as Matured Endowment, Paid Up, etc., to the branch office, to their homes, or to fictitious addresses. The employee can easily create a check defalcation by changing the address of record prior to the settlement check issue date, thus misdirecting the check in question. Also, an orphan contract holder might be transferred to his agency periodically, affording the opportunity to improperly request the issuance of a settlement check.

An *orphan contract holder* is a policyholder or contract holder who has not been assigned to a servicing agent or the whereabouts of whom are unknown. The servicing agent attempts to locate this family group and can possibly influence them to purchase additional insurance.

A clerical support employee might receive notification that the orphan contract holder does not reside at the given address. This will give the support staffer an opportunity to change the address to either his home or a fictitious address and possibly create a fraud.

Premium Theft

An agent collects the premium but does not remit the check to the insurance company. Thus, the insured unknowingly has no coverage available upon a qualifying event.

Fictitious Payees

An agent or a clerk can change the beneficiary on record to a fictitious person and subsequently submit the necessary papers to authorize the issuance of a check.

Fictitious Death Claims

An agent or employee obtains a fictitious death certificate and requests that a death claim check be issued. The agent receives the check and cashes it.

The sales representative can also write a fictitious application and, after the contestable period (two years), submit a phony death claim form and obtain the proceeds. The agent, by investing a small amount, could receive a much larger sum in misappropriated claims.

A company is particularly vulnerable to this scheme if the perpetrator has knowledge of the underwriting procedures, such as the limits under which insurance can be written without a medical exam and what should be submitted on a death claim.

Underwriting Irregularities

Equity Funding

Equity funding is the process of using existing premium/policy values to finance new businesses. As long as the insured is aware of what is being done by the agent and fully understands the long-range method of payment on the new contract, there is no apparent underwriting irregularity.

Equity funding techniques, also known as *piggybacking*, usually do not produce quality business. Furthermore, the company increases the amount of life insurance on the books but receives little or no new funds while incurring increased sales and administrative expenses associated with the issue of that new business.

Equity funding irregularities might involve improper financial benefits to field personnel as well as annual incentive compensation bonuses paid to management, if applicable. The fraud examiner should determine what financial benefit will occur from an improper equity transaction.

Misrepresentation

Misrepresentation might occur if a sales representative knowingly makes a false statement with the intent to deceive the prospective insureds in order to obtain an unlawful gain.

False Information

A company employee might submit the following false information to obtain unlawful financial gain:

- Improper medical information to obtain a better insurable rate for the prospective policyholder (for example, standard to preferred rate)
- Improper date of birth to obtain a cheaper premium on the new policy
- Improper home address to obtain a cheaper premium for home or automobile insurance
- Improper driving history prior to purchasing automobile insurance to reduce the annual premium or obtain insurance where the individual would normally have to apply through the risk pool

Fictitious Policies

To keep his position, a salesman submits fictitious policies to improve his writing record. Also, prior to an individual leaving the company, he writes fictitious policies called tombstone policies to improve his commission pool so that his compensation will be greater. The term *tombstone policy* came into being because agents would literally copy names from tombstones to write new, fictitious policies.

Surety and Performance Bond Schemes

Surety and performance bonds guarantee that certain events will or will not occur. An agent issues worthless bonds to the insured for high-risk coverage in the hope that a claim is never made. If a claim is made, the agent might pay it off from agency funds, delay the payment, or skip town.

Sliding

Sliding is the term used for including additional coverage in an insurance policy without the insured's knowledge. The extra charges are hidden in the total premium. Since the insured is unaware of the coverage, few claims are ever filed. For example, motor club memberships, accidental death, and travel accident coverage can usually be added to the policy without the insured's knowledge.

Twisting

Twisting is the replacement, usually by high-pressure sales techniques, of existing policies for new ones. The primary reason, of course, is for the agent to profit since first-year sales commissions are much higher than commissions for existing policies.

Churning

Churning occurs when agents falsely tell customers that they can buy additional insurance for no cost by using built-up value in their current policies. In reality, the cost of the new policies frequently exceeds the value of the old ones.

Vehicle Insurance Schemes

Ditching

Ditching, also known as owner give-ups, involves getting rid of a vehicle to collect on an insurance policy or to settle an outstanding loan. The vehicle is normally expensive and purchased with a small down payment. The owner falsely reports the vehicle as stolen while orchestrating its destruction or disappearance in some way, such as by having it stripped for parts, burned, or submerged in a large body of water. In some cases, the owner just abandons the vehicle, hoping that it actually will be stolen. The scheme sometimes involves a homeowner's insurance claim for the property that was supposedly in the vehicle when it was "stolen."

Past Posting

Past posting is a scheme in which a person becomes involved in an automobile accident, but does not have insurance. After the accident, the person gets insurance, waits a short time, and then reports the vehicle as having been in an accident, thus collecting for the damages.

Vehicle Repair

This scheme involves the billing of new parts on a vehicle when used parts were actually replaced. Sometimes this involves collusion between the adjuster and the body repair shop.

Vehicle Smuggling

This is a scheme that involves the purchase of a new vehicle with maximum financing. A counterfeit certificate of the vehicle's title is made showing that it is free and clear. The vehicle is insured to the maximum, with minimum deductible theft coverage. It is then

shipped to a foreign port and reported stolen. The car is sold at its new location and insurance is also collected for the "theft."

Phantom Vehicles

The certificate of title is a document that shows the legal ownership of a vehicle. Even though it is not absolute proof that a vehicle exists, it is the basis for the issuance of insurance policies. Collecting on a phantom vehicle has been shown to be easy to do. Note that the term *phantom vehicle* might also refer to vehicles involved in uninsured motorist claims wherein the vehicle and driver that purportedly caused the damage in question cannot be identified.

30-Day Special

In this scheme, the vehicle's owner reports the vehicle stolen and hides it just long enough for the insurance company to settle the claim—usually 30 days. Once the claim is paid, the vehicle is abandoned by the owner. These schemes are typically perpetrated by owners of vehicles that are in need of extensive repairs that would not be covered by their automobile insurance policies.

Paper Accident

This scheme involves the fabrication of an automobile accident that only exists on paper. When the repair costs are small (e.g., less than $1000), many insurance companies do not bother to send an investigator to examine the vehicle. Because this is a low-risk endeavor and the authorities are not involved, this scheme is very popular within organized crime rings.

Hit and Run

The hit and run is a variation of the paper accident. The owner of a previously damaged vehicle calls the police and claims to be the victim of a hit and run accident. The resulting police report is used to file an insurance claim. This scheme might also be perpetrated after a single-car accident with no witnesses.

Staged Accidents

Staged accidents are schemes in which an accident is predetermined to occur on a vehicle. The schemes are organized by crime rings and the culprits move from one area to another. They often use the same vehicle over and over, which sometimes causes their scheme to be uncovered.

Two Vehicle Accident

Perpetrators cause an accident and then lead the innocent driver to believe it's his fault.

Three or More Vehicle Accident

Perpetrators set up an accident in which all the drivers are involved.

Side Swipe

The side swipe is a scheme that relies on opportunity. In a busy intersection with multiple turn lanes, the perpetrator makes the same turn over and over again, waiting for another driver to cross into his lane. When a driver finally does, the perpetrator purposely drives into the other car. Witnesses and police involvement are helpful to the perpetrator in this case.

Drive Down

The scheme involves a perpetrator waving on a driver attempting to merge in front of him, and then intentionally colliding with the merging vehicle. After the accident, the perpetrator denies having waved on the merging driver.

Other Staged Accidents

Two drivers purposely collide where they will not be observed. Additional damage might be added to the vehicles after impact. The cars are driven to a road or highway and arranged so that the accident appears to have occurred there. The police are then notified.

SWOOP AND SQUAT

A victim of this scheme finds himself passed by two cars while driving. The car in the lead cuts in front of the second, forcing it to stop abruptly. The victim rear-ends the second car while the other driver speeds away. Victims often accept responsibility for the accident, thinking it their fault for not paying attention. The rear-ended vehicle usually contains the maximum amount of passengers, all of whom claim injuries.

Inflated Damages

The business environment and the competition for work in the automobile repair industry have motivated a scheme where some establishments inflate the estimated cost to cover the deductible. The insured is advised by the repair shop that the shop will accept whatever the company authorizes.

Vehicle Identification Number (VIN) Switch

VIN-switch fraud schemes are the work of professionals in which a wrecked vehicle is reported as repaired and subsequently sold. The vehicle is not repaired, but the VIN plate is switched with a stolen vehicle of the same make and model.

Rental Car Fraud

A person does not need to own a vehicle to commit automobile fraud. There are several schemes that can be perpetrated using rental cars. The most prevalent involve property damage, bodily injury, and export fraud.

Property Schemes

Property schemes usually involve the filing of insurance claims for property that never existed or for inflated loss amounts.

Inflated Inventory

Property that is lost through fire is claimed on an insurance form. However, property that does not exist also finds its way onto an inventory of the property claimed. Property claimed might have been previously sold or never owned by the claimant.

Phony or Inflated Thefts

A home or car that has been burglarized is the basis for filing a claim for recoveries of monies lost. However, as with items "destroyed" by fire, the items never existed or were previously sold.

Paper Boats

A claim is filed for a boat that sank, but actually never existed. It is not difficult to register a boat that is based on a bill of sale. After a period of time, a loss is claimed for the sinking of the boat. It is difficult to prove that the boat did not exist or was not sunk intentionally.

Life Insurance Schemes

Fraudulent Death Claims

To obtain reimbursement for life insurance, a death certificate is required. However, phony death certificates are not that difficult to obtain. The person might be very much alive and

missing, or the person might be dead and the death is past posted. With small settlements, death claims are not closely scrutinized and are paid relatively easily.

Murder for Profit

A murder for profit scheme involves the killing (or arranging for the killing) of a person in order to collect the insurance. The death might be made to look like it was an accident or a random killing.

Vanishing Premium Scheme

This scheme involves insurance companies marketing deceptive "vanishing premium" life insurance policies. The idea of the "vanishing premium" policy is that, after a set number of years of paying the policy's premium, the policy would be paid off. At that point, the policy holder would not have to make any more payments toward the policy.

In reality, though, around the time the policy would be paid off, the insurance company explains that the policy had been revised, and that several more years of payments are necessary. The policy holder is then faced with a dilemma: either cease making payments and risk having the policy lapse due to non-payment or continue making the expensive payments for several more years.

Liability Schemes

In a liability scheme, the subject claims an injury that did not occur. The slip-and-fall scam is the most common, where a person claims to fall as the result of negligence on behalf of the insured.

Red Flags of Insurance Fraud

Red flags of insurance fraud might include any of the following:

- The claim is made a short time after the policy's inception, or after an increase or change in the coverage under which the claim is made. This could include the purchase of a scheduled property or jewelry floater policy, or more than one during the time before the loss.
- The insured has a history of many insurance claims and losses.
- The insured earlier asked his insurance agent hypothetical questions about coverage in the event of a loss similar to the actual claim.

- The insured is very assertive and insistent about a fast settlement, and exhibits more than the usual amount of knowledge about insurance coverage and claims procedures, particularly if the claim is not well documented.
- In a burglary loss, the claim includes large, bulky property, which is unusual for a burglary.
- In a theft or fire loss claim, the claim includes a lot of recently purchased, expensive property, or the insured insists that everything was the best or the most expensive model, especially if the insured cannot provide receipts, owner's manuals, or other documentary proof of purchase.
- In a fire loss claim, property that would be personal or sentimental to the insured and that you would expect to see among the lost property—photographs, family heirlooms, or pets—is conspicuous by its absence.
- A large amount of the property was purchased at garage and yard sales and flea markets, or otherwise for cash, and there are no receipts (the insured will usually be unable to recall exactly where these sales took place or by whom).
- The insured cannot remember or does not know where he acquired the claimed property, especially unusual items, and/or he cannot provide adequate descriptions.
- On the other hand, the insured already has receipts and other documentation, witnesses, and duplicate photographs for everything; the claim is too perfect.
- Documentation provided by the insured is irregular or questionable, such as:
  - Numbered receipts are from the same store and dated differently or sequentially.
  - Documents show signs of alteration, such as dates, descriptions, or amounts.
  - Photocopies of documents are provided and the insured cannot produce the originals.
  - Similar handwriting or signatures—or the insured's apparent handwriting—appears on different receipts, invoices, gift verifications, appraisals, etc.
  - The amount of tax is wrong, either for the price of the property or for the date appearing on the receipt.
  - Receipts, invoices, or shipping documents do not have "paid," "received," or other shipping stamps.
  - In a theft or loss away from home, the insured waits an unusually long time before reporting the theft to the police.
  - The insured is able to give the police a complete list of lost property on the day of the burglary or shortly after.
  - The amount of the claim differs from the value given by the insured to the police.

  - In a business inventory or income loss claim, the insured does not keep complete books, or the books do not follow accepted accounting principles.
  - The physical evidence is inconsistent with the loss claimed by the insured.
  - In a burglary loss, there is no physical evidence of breaking and entering, or a burglary could not have occurred unnoticed under the circumstances.
  - In a fire loss:
    * The apparent cause and origin of the fire is inconsistent with an accidental cause and origin, or there is evidence of the use of an accelerant.
    * The remains of the property do not match the claimed property.
  - The premises do not show signs of having contained the claimed property, or the amount of property will not fit into the space where the insured says it was.
  - Physical damage to the insured's car is inconsistent with it having been in a collision with an uninsured car.
  - The insured has discarded the claimed damaged property before the adjuster can examine it.
  - Over the period of time it was allegedly acquired, the cost of the claimed property seems to exceed the insured's financial ability to purchase it.
  - The insured refuses or is unable to answer routine questions.
  - The insured provides supporting evidence and documentation that cannot be corroborated.
- Information on a life insurance application is very vague or ambiguous as to the details of health history: dates, places of treatment, names of physicians or hospitals, or specific diagnosis.
- Applicant fails to sign and date the application.
- Pertinent questions on the application are not answered, such as income, other insurance carried, hazardous duties, or aviation or flying activity.
- The insured has excess insurance, either shown at the time of application or developed through an underwriting report of database information.
- Earned income does not warrant the amount of insurance being applied for.
- The applicant's date of birth as shown on the application is much earlier than shown with other carriers or in previous applications or policies.
- The agent is exerting a great deal of pressure to have the policy issued because of the large amount applied for, but does so without the underwriter's knowledge.
- The physician's report is very vague on details of past medical history and does not coincide with the information shown on the application.
- A death claim is presented in which the death has taken place outside of the country.

- The signature on the application for insurance does not appear to be the same signature as shown on an authorization at the time of the claim.
- A claimant or claimant's attorney attempts to limit the type of information to be related by a signed authorization, which is a standard authorization used by the company.
- An attorney is immediately brought into a contestable death claim, attempting to interfere with the investigation and to withhold information required by the company.
- A contestable death claim that is reported as an accidental death could possibly be a suicide (fatal accident involving only one vehicle, a hunting accident, an accidental shooting while cleaning a weapon or repairing the same, etc.).
- An autopsy report discloses a different height and weight than what is shown on the recent application (auto or house fire death). Dental records do not coincide with those dental findings as shown by an autopsy report.
- Records are missing on a patient who was confined to a hospital, or records are missing on a patient from a physician's office.
- The death claim package sent to the insurance company is too well packaged and complete in every detail with supportive documents. Documentation that was not initially requested or required by the insurance company was voluntarily sent, such as newspaper reports, burial certificates, or reports on the shipment of the body from one country to the home country.
- The routine audit of a designated insured group shows a significant increase of added employees whose names do not show up on the payroll.
- Gunshot wounds or stabbings were inflicted by the insured as the aggressor or were self-inflicted.
- Police accident reports were submitted by the claimant.
- Pressure for speed of handling—claimant wants to stop by the office to pick up his check "as we're leaving for a trip in the morning."
- A series of prescription numbers from the same drug store do not coincide chronologically with the dates of the prescriptions.
- An automobile fire occurs in a very remote rural area with no witness, but the driver claims that an electrical shortage in the engine compartment caused the entire car to catch fire.
- Preliminary information for a business fire loss or home fire loss indicates considerable financial difficulties and financial pressures being brought upon the owner, and the fire is suspicious in nature and/or origin.

- An employee within the claims operations of an insurance company is known to have a drinking problem, drug problem, financial pressures, serious marital difficulties, or an extramarital affair, and irregularities start to appear.
- When dealing with burglary losses from a business or home, the investigator observes any of the following:
  - The remaining contents at the scene are of a much inferior quality than those items reported stolen.
  - There is no indication of indentation in the piling of the carpet where heavy items of furniture or equipment were to have been placed.
  - There are no hooks or nails on the walls where valuable pictures might have been hung.
- Entrances or exits are too small to take a large item through without laboriously disassembling it.
- Any information on a claim that has been filed if it is determined that there is deliberate cover-up or false statements contained therein.
- A disability income protection claim is filed and it is determined that the claimant had recently purchased numerous expensive items on credit and had them all covered by credit accident and health (A&H) insurance coverage.
- Public transportation accidents in which there are more passenger claims filed than there were passengers at the time of the accident.
- A witness to an accident or incident deliberately tries to hide from investigators rather than come forth and tell the truth.
- An official document of findings is in complete conflict with the facts in the case and there is no explanation for this conflict of facts. Photographs or other documents do not substantiate the reported findings.

Computer-Generated Detection Reports

Data analysis is an effective tool used to detect insurance fraud schemes. Using data analytics, fraud examiners can run reports that provide good leads to possible fraud. The following is a list of commonly generated reports.

Address Similarity Report

Address similarity reports electronically compare multiple checks going to the same address. They are extremely useful because they might show a check defalcation or funds going to another insurance company, broker, or fictitious payee.

Downloading of Files

A comparison of issue files to disbursement files can determine if funds are being used to place new policies by using the equity of old policies. For example, computer-assisted auditing tools and techniques (CAATTs) are used to download and compare electronic files.

Electronic Confirmations

Confirmations for mailed disbursements in force or lapsed premiums, change of address, etc., can be used to verify that company records agree with policyholder records.

Exception or Manual Override Reports

Computerized reports can be produced that list all exceptions to normal electronic processing. All human intervention can appear on a periodic management information report and can be test-checked by management. It is imperative that management review all exception reports for possible frauds on an ongoing basis.

Workers' Compensation Fraud

Some countries, such as the United States, have workers' compensation laws that require employers or their insurance plan to reimburse an employee (or act on his behalf) for injuries that occurred on the job regardless of who is at fault and without delay of legal proceedings to determine fault. The injury may be physical, such as a broken limb, or mental, such as stress.

Common Schemes

Schemes are generally broken into four categories: premium fraud, agent fraud, claimant fraud, and organized fraud schemes.

Premium Fraud

Premium fraud involves the misrepresentation of information to the insurer by employers to lower the cost of workers' compensation premiums.

EMPLOYEE CLASSIFICATION

Workers' compensation rates vary depending on an employee's job classification. Employees that have a higher risk for injury on the job will have a higher premium rate. For example, clerical employees have a lower probability for an injury than truck drivers or construction

workers, and thus their premiums should be lower. Therefore, to lower their premium rate, an employer might intentionally misclassify employees.

UNDERSTATEMENT OF PAYROLL

The premium for a specific job classification is based on the total payroll for that classification. The employer might understate the amount of the payroll for higher-risk classifications.

EXAMPLE

Two men pleaded guilty to charges of conspiracy and mail fraud in connection with a fraudulent scheme to reduce workers' compensation claims for a construction company. The men falsely reported that workers in high-risk trades were engaged in less dangerous occupations to lower premiums. They also concealed millions of dollars on the company payroll from the insurance company, thereby avoiding workers' compensation payments on those dollars.

EXAMPLE

A married couple found themselves responsible for a $71,049 judgment after being accused of misreporting payroll in their drywall business. Two former employees tipped off investigators that they were being paid with checks bearing different company names.

Half of their payroll money was paid by an insured drywall company, and the other half came from one that was not insured. Workers' compensation claims came from the company that was paying premiums.

GEOGRAPHIC LOCATION OF THE INSURED'S OPERATION

Premium rates can differ significantly based on geographic location from jurisdiction to jurisdiction. An employer might have a storefront location or a PO Box in an area that has lower rates. An employer with employees in multiple countries might list all of its employees as operating in the country that has the lowest rates.

HISTORY OF PAST LOSSES

The modification or "mod" factor is a multiplier that is used to determine premium rates. The multiplier is derived by comparing the employer's claims history with other employers' claims histories in the same industry. The higher the claims loss, the higher the mod, and thus the higher the premium. A new business starts with a neutral mod for that type of

business. Employers that have a high mod factor might become a "new" business that does not have a mod established and thus have lower premiums than they should.

CORPORATE GERRYMANDERING

The risk pool assigned to an employer accepts any business regardless of its claim experience. However, it does not have to accept any employer that owes premiums. Some employers create a new corporate entity to obtain coverage or avoid higher premiums due to past heavy losses.

FORGED DOCUMENTS

Some employers forge or alter prior certificates showing coverage to collect payment for work done or as proof of coverage to authorities.

Agent Fraud

PREMIUM THEFT

Agents issue certificates of coverage indicating the customer is insured, but never forward the premium to the insurance company.

CONSPIRING TO REDUCE PREMIUMS

An agent might alter the application for coverage completed by the employer to be able to offer a lower premium to his client. The agent might also improperly advise the employer as to how to complete the application or advise the employer to transfer a group of employees into a lower risk classification to avoid the experience modifier.

Even though the employer might not be aware that the schemes are a violation of law, since the employer signs the application, he can be charged for his part in the scheme.

Claimant Fraud

Claimant fraud involves misrepresenting the circumstances of any injury or fabricating that an injury occurred.

INJURY FRAUD

In this type of fraud, false information about the injured worker is submitted to the workers' compensation carrier. The report describes the injury and states that the employee is either totally or partially disabled and either unable to work or only able to work part-time. In many

of these schemes, the fraud is helped along by a doctor who, for a fee, will provide a false diagnosis and false medical records for phony treatments.

The employee might stage an accident and fabricate an injury, or actually have an accident and then exaggerate the injury.

EXAMPLE

A firefighter was arrested for insurance fraud related to workers' compensation payments he had received. The man claimed he fell off a ladder and injured his knee while working as a meat cutter in a grocery store. He collected temporary disability benefits and received medical treatment for six months, complaining of pain and telling doctors that he could barely walk. At the same time, the man was training with his city fire department as a reserve firefighter. The training consisted of strenuous exercise, such as heavy lifting and an hour of physical training each day.

SECONDARY EMPLOYMENT

Employees who are collecting workers' compensation benefits might also secure a job with another employer—either part-time or full-time. The employee might fake his identity or assume someone else's identity to receive compensation.

Organized Fraud

Organized fraud schemes are composed of the united efforts of a lawyer, a capper, a doctor, and the claimant. This scheme is used not only in workers' compensation cases, but also in other medical frauds, such as automobile injuries.

THE LAWYER

Lawyers are usually the organizers of the schemes and the ones who will profit the most. The majority of workers' compensation cases are accepted on a contingency fee basis. If no settlement is awarded, then the lawyers will not be paid. This is a high-volume business, and the lawyers do not want the cases to be litigated. They are relying on the insurance company's desire to settle as quickly as possible.

The lawyers will entice the claimant into securing their services by promising a large settlement from the insurance company. The claimants might or might not have to undergo the medical tests, since the only requirement of the claimants is that they be insured. The lawyer will then refer the injured party to a doctor for "treatment."

THE CAPPER

Cappers, also known as runners or steerers, are used to recruit patients for the scheme. They might be employed by either the attorney or doctor and are paid—either on a percentage of the total take or on a per person basis—for bringing in patients. Cappers might approach patients at unemployment compensation lines, work sites, scenes of accidents, or at any other type of organized gathering. Patients are brought into the scheme with promises of enrichment.

EXAMPLE

In August of 2010, the last member of a group of 51 suspects was arrested for insurance fraud and other crimes. The insurance fraud included clinic workers and owners who hired runners to recruit automobile accident victims, as well as staged automobile accident participants when they ran out of "legitimate" accident victims. Runners received $500 to $700 per patient, and the estimated fraudulent claims from this scheme exceeded $4 million.

THE DOCTOR

Doctors might be organizers or players in the scheme, but must be a part of it for it to work properly. Doctors are used to lend authenticity to the scheme, and they are well compensated for their efforts. The doctors bill for services that they might or might not render, as well as for unnecessary services. In addition, if patients have regular health insurance, doctors might double bill for the services. If an injury is the result of an automobile accident that occurred while the patient was on the job, the doctor might bill all three insurance companies: the workers' compensation carrier, the employee's health insurance, and the automobile carrier.

Because of coordination of benefit clauses in most insurance contracts, the insurance companies will coordinate the benefits to the extent that the maximum amount paid will be 100 percent of the injuries. However, the doctors will not let the patient's health insurance company know that the injury is work-related or accident-related, and thus the claim might be overpaid, since both claims are paid at their full liability.

Most of the treatments rendered are office visits, x-rays, vascular studies, physical therapy, and spinal manipulations. In some cases, hospital employees are part of the scheme and allow the use of the facility fraudulently.

Red Flags

- Documents have obviously been altered; correction fluid or erasure is evident.
- Documents are improperly filled out with entries in the wrong place or information that does not make sense.
- Claims are filed where the carrier indicated no record of coverage.
- Poor-quality photocopies of documents are submitted instead of original documents.
- Small payrolls are reported for large contractors or employee leasing operations.
- Payroll figures reported to insurers disagree with payroll reported for other purposes.
- Claims for employee injuries are inconsistent with that employee's classification.
- Industrial or construction enterprises with a work force are reported to be in low-rate categories.
- "New" corporations participate in ongoing jobs.
- Most of the employees from an employer with a high experience suddenly become employees in a new business.
- The agency employs large numbers of support staff and only has one licensed agent.
- The agent only accepts cash or money orders for premiums.
- No policy is received after an extended time.
- No bill is received for premiums.
- An employer review of the application indicates that it is inaccurate.
- Individual employees are reclassified into a lower classification.
- The employer begins to declare a smaller payroll.
- Claimants:
  - Are disgruntled, soon-to-retire, or facing disciplinary action or layoffs.
  - Are involved in seasonal work that is about to end.
  - Take unexplained or excessive time off prior to claimed injury.
  - Take more time off than the claimed injury seems to warrant.
  - Have no witnesses to the accident.
  - Have accidents that occurred in an area where the employee normally would not be working (especially if it's a high-risk area).
  - Delay the reporting of an accident.
  - Are new on the job or have a history of short-term employment.
  - Have a history of injuries.
  - Have inappropriate or a lack of medical treatment for injuries.
  - Are experiencing financial difficulties.
  - Change physicians when a work release has been issued.
  - Frequently change medical providers.

  - Make demands for quick or early settlement.
  - Are never at home after a "serious" injury or can only be reached by return telephone calls.
  - Are unusually familiar with workers' compensation procedures.
  - Are consistently uncooperative.
  - Receive mail at a post office box or at an address different from that on employment or driver and vehicle licensing records.
  - Have soft tissue injuries that are hard to prove.
  - Are incapacitated, but seen in activities that require full mobility.
  - Have independent medical exams that reveal conflicting medical information.
  - Have a history of self or family employment; have a trade or work in a cash business.
  - Have injuries that occur in an area where the employee would normally not be working.
  - Have injuries that would not normally be the type the employee should have.
  - Have injuries that occur on a late Friday afternoon or are reported on a Monday morning (if injuries are reported Monday morning, the injury could have resulted over the weekend).
  - Are actively involved in contact sports or physically demanding hobbies.
  - Have dates of disability or absences from work that do not coincide with the physician's date of disability or dates of treatment.
  - Have unprofessional diagnostic terminology.
  - Have misspelled medical terminology throughout the medical report or hospital record.
  - Have a pattern of accident claims by an individual or family members.
- Claimant repeatedly does not show up for his requested independent physical examinations or is not home when the regularly scheduled nurse stops by for therapy.
- The claimant's attorney is known for handling suspicious claims.
- Attorney reports his representation began on the day of the reported incident.
- Same doctor and attorney are known to handle these types of cases.
- Claimant complains to the insurance company's CEO in order to press for payment.
- The attorney threatens further legal action unless a quick settlement can be made.
- The attorney inquires about a settlement early into the life of the claim.
- Wholesale claim is handled by law firms and multiple class action suits.
- Dates of the accident are vague or contradictory.
- Treatment for the injury follows previous first-time visits to a provider.
- Same provider always bills for extra time or extra consideration on a claim.

- Provider is working through an attorney.
- Provider is reluctant to communicate with the insurance company.
- Provider shares the same patients with the same colleagues.
- Provider refers patients to specific other providers.
- Provider prescribes unnecessary supplies and/or care by a specific provider.
- Medical records are "canned."
- Medical records are out of sequence and missing dates of service.
- Different handwriting appears on documentation with same dates of service.
- Records are reported as lost, burned, or stolen when requested.
- Progress notes consistently reflect that the patient has a high degree of pain, yet his condition is improving or progressing as planned.
- Diagnosis is inconsistent with the treatment rendered.
- Provider bills on a holiday or Sundays.
- The medical reports are conflicting.
- Claims are photocopied.
- Claims for other patients are identical.
- The claimant bills or harasses the insurance company for payment.
- The claimant's address is different on the claim form than it is on the enrollment file.

Investigation Tips

Premium Fraud

- Review the application for coverage for completeness and accuracy.
- If the business is claiming to be new, verify that it is indeed new and no mod factors have been established.
- Review the underwriting of the application for suspicious activity. If the company is a large company and has a small payroll, verify the number of employees, as well as their classification.
- Review claims to determine if they are consistent with the type of employment reported and the number of employees claimed.
- Conduct an on-site audit of their payroll and related records for the policy period and determine where their principal place of employment is located.
- Observe if there are too many clerical employees or other low-risk occupations that make up the calculation leading you to believe that the records are misstated.
- Analyze the financial statements, when available, to determine what payroll expenses actually are compared to what is reported.
- Review accident and injury reports for suspicious activities.

- Conduct surveillance as needed to observe and document various activities.
- Document findings and report the results of the activity as required.

Claimant Fraud

In spite of the possible indicators of fraud, medical treatment must be secured immediately, but an investigation should be opened immediately if there is a suspicion of fraud. The following should be kept in mind when beginning such an investigation:

- The manager who is responsible for the area where the injury occurred should initiate an investigation on each reportable accident.
- The accident should be discussed with the employee as soon as possible.
- A signed statement from the employee should be obtained as soon as the employee is able to do so.
- In obtaining a signed statement, the following questions should be answered, as applicable:
  - What was the employee doing just prior to the accident and after the accident?
  - Was the employee carrying out his regular duties in the manner they should normally be conducted?
  - Had the employee been properly instructed as to how to safely perform the duties? When, and by whom?
  - Did he work in accordance with these instructions?
  - Did another employee cause the injury?
  - Was the equipment or machinery properly guarded and in good condition?
  - Was the equipment suited for the purpose it was being used?
  - Was the workplace properly lighted?
  - What were the housekeeping conditions in the area?
  - Did the work being done by the injured employee differ in any way from that being performed by other employees?
  - Is there a safer way that this operation can be performed?
  - Was the injured employee in good health when he reported to work on the date of the accident?

Have an independent medical examination performed to document the illness. The person performing the exam should photograph the patient, obtain a copy of the patient's photo identification such as a driver's license, and obtain the patient's signature.

The following questions should also be asked:

- Are you disabled from working?
- Are you now working part-time, full-time, or not at all?
- What are your daily activities?
- What is your activity level with regard to your ability to walk, jog, run, drive, swim, or participate in sports activities or hobbies?

HEALTH CARE FRAUD

Introduction

Health care fraud may be defined as an intentional act to defraud a health care benefit program or to obtain through false representations money or other property owned by a health care benefit program. This type of fraud involves a deception or misrepresentation that an individual or entity makes, knowing that the misrepresentation could result in some unauthorized benefit to the individual, entity, or some other party. The most common fraud involves a false statement or a misrepresentation or deliberate omission that is critical to the determination of benefits. Due to the highly technical nature of the health care industry and the broad diversity in payment systems throughout the world, health care fraud schemes can be among the most complex.

Types of Health Care Systems

To understand and investigate a health care fraud scheme, it is necessary to understand the type of health care system in which the fraud examiner is operating. For instance, some fraud schemes will be possible under some systems, but inapplicable or functionally different in others. There are many ways that health care systems can be classified, but for the purposes of this manual, the major factors will be:

- The extent to which the jurisdiction's health care system is privately operated and government operated
- The payment system(s) used
- The method for calculating compensation for health care services

Public and Private Systems

Each country has its own way of addressing health care, ranging from completely private systems to systems that are completely owned and operated by the government. Most countries, however, have mixed systems in which some services are provided by the government, while others must be paid by individuals or private insurance companies.

The differences in each system primarily affect who is defrauded and the method by which resources are stolen or misused. Government programs in nations with universal health care are the main target of health care fraud, while countries that rely on private parties to pay for health care see more schemes against insurance companies and individuals. Additionally,

whether health care providers are private parties or employed by the government can make a significant difference in the types of schemes observed.

Payment Systems

The issue of payments systems involves how payment flows from the parties paying for services to the parties who provided the services. There are three common systems: direct payment, single payer, and third-party payer, and each can be present in the same country.

Direct Systems

The first system is straightforward. In a direct system, patients pay directly from their own funds for health care services. Due to the largely unpredictable nature and high costs of health care, this payment system usually is accompanied by the other systems.

Single Payer

In a single-payer system, a government health care program pays providers on behalf of the patients who receive services. In other words, the "single payer" is the government. However, there might be copayments from patients in these systems (generally small payments in addition to what the government pays) and services that are not covered by the government program. Also, in single-payer systems, the government might directly own and operate health care facilities (such as in the United Kingdom) or delegate those duties to private parties (such as in Canada).

Regardless of whether health care providers are employed by the government or privatised, there are similar ways in which they can submit fraudulent bills or cost information. However, fraud examiners should consider the relationship to identify likely fraud schemes. For example, a government-employed physician who receives a set salary probably has less incentive to charge for fictitious services than a private physician who receives compensation based on each service provided.

Most governments that provide relatively robust health care programs use single-payer systems.

Third-Party Payer

A handful of countries use the third-party payer system, including the United States. The following list shows the parties in a third-party payer system.

- The first party is the patient or the person, such as a parent, responsible for the patient's health bill.
- The second party is the provider—the physician, clinic, hospital, nursing home, or other health care entity rendering the care.
- The third party is the insurance company or health care program that pays the physician, clinic, or other second-party provider for the care or services to the first party (patient). Generally, individuals are responsible for obtaining their own health insurance, but government programs might subsidise programs for those with low incomes, the elderly, people with special needs, and so on.

Again, a mix of these systems is possible. For instance, a country might have a single-payer system, but it might also be common for its residents to purchase additional medical coverage from a private insurer.

In countries with private health insurance, fraud accounts for 5–10 percent of all funds paid out, according to some estimates. Health care fraud in countries with government-provided health care is perpetrated primarily by providers.

Methods for Calculating Compensation

There are several types of reimbursements for providers: fee for service, capitation, episode of care, and salary. Each has advantages and disadvantages from an anti-fraud perspective.

Fee for Service

Fee-for-service reimbursement occurs when providers receive payment for each service rendered. The disadvantage of fee-for-service payment is that it creates an incentive for providers to increase their compensation by performing excess and unnecessary services. However, providers tend to like this payment system because it gives them wide discretion in selecting the services that meet the patient's needs.

Capitation

Capitation is a reimbursement method in which providers receive one lump sum for each patient that they treat, regardless of how many services the provider renders to each patient. While this method avoids some of the incentives for providers to perform unnecessary services, it might give providers a reason to focus on the quantity of patients they see rather than the quality of service. Additionally, capitation does little to stop schemes involving fictitious patients.

Episode of Care

Episode-of-care reimbursement is a health care payment method in which providers receive one lump sum for all the services they provide related to a condition or disease (as opposed to capitation, which is a lump sum per patient). This method captures some of the benefits of capitation by removing incentives to provide unnecessary services, but is also (in theory) more fair to providers than capitation because it compensates them more when multiple health issues are treated.

Salary

When governments directly operate health care facilities, it is common to pay providers a basic salary rather than offer service-based compensation. Even so, some medical services might be provided through contractors instead of government employees. On one hand, salary employees are not compensated for each service, so there seems like less incentive for performing unnecessary services or claiming fictitious services occurred. However, there are various institutional fraud schemes that still involve similar tactics.

Copayments, Deductibles, and Self-Insurance

Other important concepts for fraud examiners to understand when reviewing a health insurance fraud case include copayments, deductibles, and self-insurance.

Government and insurance health programs often require patients to pay a *copayment*, or a small portion of the total payment, when receiving drugs or services from a health care provider. There might be a small fee for a routine doctor's office visit or copayment for a prescription, for instance. Health care providers in private health care systems can commit kickback fraud violations under certain circumstances if they do not attempt to collect the copayments.

Patients are also often required to pay a *deductible*—an amount that individuals must pay before the insurance company pays reimbursements in a set timeframe—most commonly for a calendar year. Once again, a health care provider who fails to collect deductibles might be charging patients kickbacks instead.

Another concept is the *self-insured plan*, in which an employer accepts the financial risk of the health care costs of its employees. The employer administers its own health insurance benefits. Rather than shift the risk to a health insurance entity, the organization assumes the costs of health care for its employees or members and their dependents.

Provider Fraud

Provider fraud consists of practices by health care providers (including practitioners, medical suppliers, and medical institutions) that cause unnecessary costs to health care programs or patients through reimbursement for unnecessary or excessive services, or services that do not meet the recognized standards for health care.

Provider fraud is a particularly pervasive risk in the health care industry for several reasons. Providers possess the knowledge of medical techniques, procedures, and terminology needed to avoid being questioned by claim-handling personnel. Additionally, most insurance companies and government health care programs contract directly with providers for billing arrangements, leaving patients out of the loop. In addition, patients are usually reluctant to accuse physicians of wrongdoing because they rely on the provider's continued services and because, when providers engage in fraudulent practices, they often forgive any out-of-pocket expenses that the patient incurs.

Fictitious Providers

In a fictitious provider scheme, corrupt providers or other criminals fraudulently obtain and use another provider's identification information and steal or purchase lists of patient identifying information. Thereafter, the perpetrator submits bills using the fictitious provider's information to the insurance provider or government health care program for medical services, although no services are performed.

In perpetrating this type of scheme, fraudsters might set up fictitious entities using their legitimate home addresses or PO Box numbers and their own government identification numbers. Alternatively, they might use the addresses and identification numbers of their family members, business partners, or neighbors. Often, fictitious companies are opened and then quickly dissolved, with the money depleted as quickly as possible.

Phantom Services

In a phantom services scheme, legitimate health care providers charge or bill a health care program for services that were not rendered at all. Often, the providers submit bills for patients they have never seen, but whose private patient information they purchased from someone involved in identity theft or someone who otherwise improperly obtained it. These scams frequently are committed by medical equipment providers and service providers (such as infusion drug therapy), but they can involve normal physician offices, ambulance services, and others. Some phantom services schemes involve patients who are legitimate patients of a

doctor or provider. These individuals are charged or their health care programs are billed for patient visits or encounters that never occurred.

Rolling Labs

A *rolling lab* is a mobile laboratory that solicits individuals to participate in health screening tests at no cost to the patient. After conducting the tests, however, the lab bills the individual's insurance provider or health care program. Also, the lab might bill additional claims for later service dates even though no more tests are conducted.

Patients might be contacted by telephone for a free physical exam, or the provider might rent office space in a doctor's office for one day and then test all of that doctor's patients. Alternatively, the lab might be set up as a temporary operation in a shopping center, health club, spa, or on vacant property; passers-by are then invited in for a "free" health screening. The testing equipment itself often arrives in a truck or van and moves from one office to another.

Subsequent to the exam, the insurance company or health care program is billed for numerous claims for a single date of testing performed by multiple providers. Additional claims are billed for later service dates even though no more testing is performed. The lab typically moves to another location prior to the patient receiving the test results to avoid detection.

Over-utilization

Over-utilization occurs when a physician prescribes unnecessary or excessive patient services. There are two possible explanations for this. The first is monetary gain to the provider. Second, the physician may have believed additional visits were necessary for proper treatment or to reduce potential malpractice liability.

Clinical Lab Schemes

Clinical lab schemes occur when a provider advises a patient that additional medical testing is needed to diagnose the problem, when in fact, the testing is not required or advisable. The fee for the unnecessary work often is split with physicians. In some cases, physicians own the medical testing service.

Additional medical testing, which is later viewed as excessive, is not always fraud. Many doctors have a genuine fear of retaliation from their patients; they are afraid of malpractice lawsuits that might result from a delayed or erroneous diagnosis.

Uncredentialed Providers

Most jurisdictions require that medical providers possess specific credentials to perform and charge for certain services. For example, a physician assistant might be authorized to provide and bill for some medical procedures, but not those that only a physician is authorized to perform. Health care fraud is committed when someone without the necessary credentials performs a service but bills as though an appropriately credentialed provider actually rendered the service. This is a common form of fraud and is often difficult to detect.

Red flags of uncredentialed providers include:

- A credentialed provider submitted bills for procedures that add up to suspicious or impossible hours. For instance, a provider submitted 20 claims for a specific four-hour procedure all within one week, for a total of 80 hours, on top of other services performed that week.
- The practice group has a relatively low proportion of licensed staff per patients treated.

Disparate Price to Government Programs

Many government health care programs require that they receive the best available price that providers offer. In a disparate price scheme, providers charge some patients (e.g., those in direct-payment situations) a lower rate than they charge the government. This disparate bill rate causes the government to pay a higher rate in violation of regulations mandating that the government receive the lowest rate. In addition, some government health programs, such as Medicaid in the United States, require that wholesale pharmacies provide the program at the average wholesale price. However, providers might manipulate their data and provide false information to the government program.

Equipment and Supplies Schemes

While it is typical to think of provider fraud as schemes committed by physicians, nurses, and other direct service providers, fraud schemes by organizations and individuals providing medical equipment and supplies are also common. Medical services generally require many types of supplies and equipment, ranging from simple gauze to high-cost MRI machines. The following are several types of schemes committed by equipment manufacturers and sellers, suppliers, and similar providers.

Ambulance Transportation

Fraudulent billing for ambulance transportation can include bills for more mileage than incurred, for trips never taken, or for trips not covered by the insurance policy or health care program.

Infusion Care

Fraud schemes involving infusion care treatment include:

- Services billed at abnormally high rates in comparison to cost
- Bills for patients who are not covered by insurance or beneficiaries of the health care program
- Bills in excess of the physician's prescription
- Bills for unnecessary treatment
- Kickbacks given to the prescribing physician

Reusable Medical Equipment

Reusable medical equipment, often called *durable medical equipment* (DME), includes items such as crutches, wheelchairs, and specialized patient beds. Fraud schemes perpetrated by reusable medical equipment suppliers frequently involve:

- Falsified prescriptions for equipment or supplies
- Intentionally providing excessive supplies
- Equipment not delivered or billed before delivery
- Billing for equipment rental beyond when the equipment was checked out
- Billing for supplies not covered by the insurance policy or health care program
- Scooter scams (i.e., billing for electric-powered wheelchairs that are either unnecessary or are of poorer quality than the model billed for)

Home Health Care Companies

Under some health care programs, patients who are confined to their home are eligible to receive home health care services. Fraud schemes involving home health care providers include:

- Forging physicians' signatures on plans of care to make it appear that patients qualify for home health visits
- Altering the approved number of home health care visits on a legitimate plan of care
- Billing for home health care visits that were never made
- Billing for costs incurred during home health care visits that are not reimbursable

Pharmaceuticals

Pharmaceutical fraud is the largest source of provider fraud in the health care industry, and can involve pharmaceutical manufacturers, pharmacies, and providers who prescribe such products. Fraud schemes stemming from pharmacy transactions include:

- Merchandising—substituting something of value for a prescription drug
- Billing for brand name drugs but dispensing generic drugs
- Billing beyond amount prescribed
- Billing for drugs not prescribed
- Billing for a high-priced generic drug but dispensing a lower-priced generic drug
- Inflating the price of drugs sold to government-backed health care programs above those sold to private parties
- Package size differential—billing third-party payers for the price of drugs purchased in small package sizes when they were purchased at less cost in larger quantities
- Black-market purchasing—purchasing drugs at significantly reduced rates and then dispensing at regular prices
- Off-label marketing—illegally inducing medical providers to order a drug for off-label purposes (i.e., a purpose not approved by the appropriate drug-regulating agency)
- Providing kickbacks or bribes to providers to induce them to prescribe pharmaceutical products

Impostor Provider

An *impostor provider* is a provider who does not exist but bills fraudulent claims. A variation on this scam involves assuming the identity of a deceased provider and practice—or putting together a group of licensed providers—and fraudulently billing under the group's provider identification code.

To help determine whether a provider is an imposter:

- Call the telephone number on the bill to determine if the provider exists; however, keep in mind that a fictitious provider might actually have rented a location and established a telephone number.
- Contact the applicable licensing board to determine if the alleged provider was licensed to practice in the area at the time the service was allegedly provided.
- Visit the provider's physical address to determine if it is valid; if it is, speak to the superintendent to determine the tenant for that address.
- Contact the jurisdiction's postal service to verify what mail is being dropped at that address.

False Diagnoses

When a provider knows that a service is not covered by a health care program, he might use false diagnoses or procedure code manipulation. Examples of common services not covered are investigational or experimental procedures and elective cosmetic surgery (although reconstructive surgery after an injury or illness is often covered).

In addition, physicians might justify ordering expensive x-rays or other diagnostic services by falsely purporting that a need exists to make such diagnostic inquiries. The services are rendered, but because the claim for the services is based on false information and is used to deceive the insurance company or health care program, it is considered a false claim.

Double Billing

Double billing occurs when the health care beneficiary or the provider seeks to be paid twice for the same service. The fraud might be perpetrated by the beneficiary, with the complicity of the provider, or it might be conducted by the provider alone. The bill might be submitted to two (or more) different insurance providers or health care programs, or it might be submitted twice to the same insurance provider or health care program with documentation intended to show that two separate expenses have been incurred.

EXAMPLE

A doctor has his own practice and is also affiliated with a clinic. The clinic submits bills under its letterhead and tax identification number, and the doctor also submits a charge on his own stationery for the same service.

Red Flags of Provider Fraud

Warning signs that a provider is engaging in fraudulent practices include:

- Pressure for rapid processing of bills or claims
- Threats of legal action for delay in making payments
- Frequent telephone inquiries on claim status
- Assertive providers who demand same-day claim payment and special handling
- Charges submitted for payment with no supporting documentation available (such as x-rays or lab results)
- Patient's address on claim form is the same as the provider's
- Routine (not specialized) treatment for patients living several hours away from the provider
- Referring physician and provider of service in the same professional corporation

- Medical records that have been altered
- Medical records that have additional information attached that would make an apparent noncovered service now covered
- Missing pages of medical records that would cover the period of time under review

Additionally, fraud examiners should be wary of the red flags of someone submitting claims as an impostor provider:

- Misspelled medical/dental terminology
- Unusual charges for a given service
- Similar handwriting by the claimant and the provider of service
- Typed, not printed, bill heads
- Bills with irregular columns
- Unassigned bills that are normally assigned, such as large hospital or surgical bills
- Typed or handwritten hospital bills
- Drug receipts from the same pharmacy but on different color paper
- Erasures or alterations
- Lack of any provider's signature on a claim form
- Absence of the provider's medical degree or required license
- An illegible provider signature on the bill submitted or the signature does not match the one on file
- Surgeries that don't have other related services such as hospital charges
- Physician's specialty does not agree with diagnosis
- Services billed do not agree with diagnosis
- Impossible or unlikely services
- Photocopied bills

Fraud by the Medical Staff

Employees of providers also have an opportunity to steal and cover up theft of cash. They can submit fraudulent claims for patients and divert the payments to themselves. If they are covered under insurance, they can also use their own contract to submit fraudulent claims. For many employees of medical providers, care rendered by their employer to them or their family is free, but claims may be filed and assignment not accepted.

Another scheme involves the provider's office calling in orders for unnecessary prescription drugs to pharmacies. Once the drugs are picked up, they can be sold. For example, in a case

involving collusion between a medical office employee and an elderly lady in a retirement community, the elderly lady had developed a business selling the drugs purchased from the employee to her friends and neighbors in her community.

Inflated Billings

Health care billings can be inflated by providers as well as beneficiaries. The following are some of the most common fraud schemes encountered by investigators and claims approvers:

- Altered claims
- Added services
- Code manipulation

Altered Claims

Altering valid claims can be accomplished using a pen; photocopier; or scanner, computer, and printer. Common alterations are:

- Amounts changed
- Date of service changed
- Name of patient changed

For example, a medical bill can be altered by placing an additional number in front of the amount charged, and the date of service can be altered so that it becomes a covered expense rather than one that was incurred prior to the patient being eligible for coverage. The individual claiming services were provided can also change the name on the bill from a noncovered family member or acquaintance to one who is covered under the insurance policy or health care program.

Detection

Procedures that can help identify altered claims include:

- Analyzing charges and identifying any excessive claims for prescription or medical services above an acceptable level
- Looking for any alterations, erasures, changes of ink, or correction fluid marks on the original bill prior to paying the claim; this is important in today's environment in which original bills, checks, and other documents are destroyed as soon as they are scanned and digitally stored to minimize storage space for recordkeeping
- Training adjusters to look for obvious alterations when processing claims

Added Services

Some fraudsters add on services never rendered to dates of actual services. In these cases, the verification process is the same as the procedures listed under the alteration process.

Code Manipulation

Medical coding is an integral part of pricing and billing for services in the health care system. It is a process of assigning codes to diagnoses and procedures to determine costs and facilitate payments to providers from government and insurance health care programs. Payment amounts are based largely on what codes are submitted to the insurer or health care program.

Types of Medical Codes

Because mistakes or intentional manipulation can occur in the coding process, fraud examiners should be able to identify the applicable code systems in a fraud examination involving health care programs. There are different code sets for different functions (e.g., diagnostic codes, medical procedure codes, etc.). Each country tends to adopt its own method of classifying procedures and diagnoses, but the increasing globalization of the health care industry has resulted in increased consistency.

INTERNATIONAL CLASSIFICATION OF DISEASES CODES

The International Classification of Diseases (ICD) is a coding system used to classify diseases and related health problems. It is published by the World Health Organization (WHO). A code is assigned to every diagnosis recognized by the WHO, and more than one hundred countries use ICD codes to report mortality data. Additionally, many countries also use ICD codes for their method of allocating resources or for determining provider reimbursement.

There are various versions of the ICD codes. The number after ICD- refers to the edition, which is periodically updated to reflect new diagnoses and other changes in the medical community. The latest version is ICD-10, which has been implemented by almost all health care systems that use ICD coding.

The formats for ICD codes changed from a five-digit code in version 9 to up to seven digits in version 10, as follows:

- ICD-9-CM Format (XXX.XX): The first three digits in the ICD-9 version represent the category of disease. The two digits after the decimal represent etiology, anatomic site, and manifestation of the disease.
- ICD-10-CM Format (XXX.XXX X): As with the ICD-9 version, the first three digits in the ICD-10 format represent the category. The next three digits (as opposed to two in ICD-9) also represent etiology, anatomic site, and manifestation. The final digit is an extension, which allows for even more specificity in classification.

The implications of the switch from ICD-9 to ICD-10 are likely going to be mixed from the anti-fraud perspective. ICD-10 contains many more possible codes than ICD-9, which will give health care administrators more specific information into the types of conditions being treated. In the short term, it is likely that the newness and lack of training will lead to mistakes by both providers and payers, making fraud harder to detect. However, the increased information available from the codes will make it easier to find red flags in the long term.

PROCEDURAL CODES

Beyond classifying diagnoses, many countries also classify inpatient and outpatient procedures through coding techniques. While ICD codes are commonly used in many countries for diagnoses, procedural codes tend to be less consistent by country.

Code Manipulation Schemes

Fraudulent code manipulation takes place if the physician or other primary provider knowingly enters an incorrect diagnostic or procedural code to obtain some benefit.

Because the coding system can be complicated, providers, insurers, and health care program employees often have difficulty identifying the codes that most accurately describe the services provided. The process can be difficult because some coding systems attempt to identify codes for all accepted medical procedures, including codes to describe minor procedures that are components of more comprehensive procedures. Payment policies add to the difficulty. For example, the fee for surgery often includes the cost of related services for the global service period (i.e., for a set number of days before and after the surgery). To prevent overpayment in these cases, health care programs and insurers need to identify when claims for surgery include codes that represent related services and reduce the payment accordingly.

It is difficult for providers, insurers, and health care programs to maintain proficiency in proper coding practices because a substantial number of the codes are changed periodically. These complexities can inadvertently lead providers to submit improperly coded claims. They also make health care programs vulnerable to abuse from providers or billing services that attempt to maximize reimbursements by intentionally submitting claims containing inappropriate combinations of codes.

UNBUNDLING CHARGES AND FRAGMENTATION

Because health care procedures often have special reimbursement rates for a group of procedures typically performed together (e.g., blood test panels by clinical laboratories), some providers attempt to increase profits by billing separately for procedures that are actually part of a single procedure. This process is called *unbundling* or *coding fragmentation*.

Simple unbundling occurs when a provider charges a comprehensive code, as well as one or more component codes. For instance, in the following examples, the provider would be overpaid because the fee for the total procedure already includes the value of its component parts.

EXAMPLE

Procedure Code	Service Billed	If Correctly Billed
58150 58720 49000 44955 58740	Total Hysterectomy ($1,300) Removal of ovaries & tubes ($950) Exploration of abdomen ($671) Appendectomy ($250) Lysis of Adhesions ($550) **Total Charge $3,721**	Total Hysterectomy ($1,300) **Total Payment $1,300**
29877 29870	Knee arthroscopy with debridement ($1,650) Diagnostic knee arthroscopy ($1,625) **Total Charge $3,275**	Knee arthroscopy with debridement ($1,650) **Total Payment $1,650**
47610 47600	Cholecystectomy with common bile duct exploration ($1,997) Cholecystectomy ($705) **Total Charge $2,702**	Cholecystectomy with common bile duct exploration $1,997) **Total Payment $1,997**

Unbundling can be detected through the use of a computer program that determines whether each code submitted is a component of one or more comprehensive codes.

MUTUALLY EXCLUSIVE PROCEDURES

A variation of unbundling, this scam involves billing for procedures that are either impossible to perform together or, by accepted standards, should not be performed together.

GLOBAL SERVICE PERIOD VIOLATIONS

Some dishonest providers will bill for a major procedure—such as a surgery—as well as related procedures when the fee for the major procedure already includes the fee for related procedures during the predefined time period (the global service period). Detecting these abuses can be difficult because the fraud examiner must determine which services are related to the surgery and which are not. This difficulty is compounded by the fact that such services might be rendered by more than one provider.

UPCODING

Upcoding occurs when a provider bills for a higher level of service than actually rendered. One common form of upcoding involves generic substitution—filling a prescription with a less expensive drug, while billing for the more expensive form of the drug.

MISUSE OF NEW PATIENT CODES

Some coding systems, such as the CPT system in the United States, include special codes for new patient visits, which enable the physicians to be reimbursed for the additional work that new patient visits typically require. Consequently, physicians who want to pad their claims might bill for visits with established patients using new patient codes.

Kickbacks in the Health Care Industry

Kickbacks in the health care industry can come from several sources. The medical community is facing competition that it has not faced in the past, and monetary offers to prospective patients have been difficult to refuse.

Examples of kickbacks include:

- Payment for referral of patients
- Waiver of deductibles and copayments
- Payment for additional medical coverage
- Payment for vendor contracts
- Payments to adjusters

Payment for Referral of Patients

Providers in an area of high competition will pay runners to recruit new patients. In addition, patients may receive a monetary reward if they refer another patient to a provider. The provider makes up for the kickback in the unnecessary billing of medical expenses or false claims. In addition, providers will pay kickbacks to other physicians for patient referrals.

Waiver of Deductibles and Copayments

Many insurance policies and health care programs require patients to pay a deductible and copayment, or a small portion of the total payment, for services rendered. One of the reasons for having copayments is to make patients take an active part in the financial responsibility for their care. To attract patients, however, providers might improperly pay for or waive the patient's out-of-pocket expense, hoping to make up for that cost in additional business.

Payment for Additional Medical Coverage

Physicians with patients who are facing long-term care or lifetime treatment, such as dialysis for kidney failure, might improperly obtain additional medical coverage (e.g., by purchasing additional insurance contracts) for their patients. This ensures that the provider will be paid, and the patient has no out-of-pocket expense.

Payment for Vendor Contracts

Companies doing business with medical practitioners will pay a "consulting" fee for referring business to them or using their supplies.

Payments to Adjusters

In order to get a claim settled quickly, a patient, or someone operating on his behalf, might bribe adjusters or other claims-handling personnel to approve or speed up the payment of a claim.

Fraud by Medical Institutions

Fraud schemes perpetrated by institutions and their employees include those commonly used by doctors and other providers. However, the more common schemes in which hospitals are primarily involved include:

- Filing of false cost reports
- DRG creep

- Billing for experimental procedures
- Improper contractual and other relationships with physician
- Revenue recovery firms to (knowingly or unknowingly) bill extra charges

False Cost Reports

To obtain reimbursement for procedures and treatments, health care institutions submit cost reports, and these cost reports are used to calculate how much the insurer or health care program will reimburse the institution for its expenses.

Because cost reports can represent extremely large payments, some institutions file false cost reports to obtain higher reimbursements or funding than permitted. The false reports might inflate the costs incurred, give the wrong percentage of their services dedicated to patients, mischaracterize the nature of those costs, or include unallowable items.

Inclusion of Unallowable Items

The following are examples of noncovered or unallowable items that might be included in cost reports:

- Expenses for tax penalties, late charges, and promotional advertising
- Costs incurred from a related-party transaction with a mark-up over the costs incurred by the related party
- Expenses that are reimbursed under other programs (e.g., billable medical supplies and therapies)
- Excessive expenses such as hotel, food, and travel expenses for recreational events
- Luxury items (e.g., lavish furnishings, corporate planes, swimming pools, or spas)

DRG Creep

Diagnostic-related groupings (DRG) is a reimbursement methodology for the payment of institutional services. Originated in the U.S. health care system, this method or similar models have become more popular in other countries for the purposes of determining costs and reimbursing institutional providers. DRG categorizes patients who are medically related with respect to various types of information, such as primary and secondary diagnosis, age, gender, weight, length of stay, and complications. Reimbursements are determined by the DRG. For example, a heart bypass operation is worth a certain amount of reimbursement and a hernia repair is worth a different amount.

DRG creep occurs when medical staff members manipulate diagnostic and procedural codes to increase reimbursement amounts or other forms of funding. When it becomes a pattern and intent is established, it becomes fraud. For example, a hospital might repeatedly and incorrectly code angina (pain or discomfort in the chest due to some obstruction of the arteries) as a myocardial infarction (a more serious event, commonly known as a *heart attack*), and thus be reimbursed at a higher level.

Another type of fraud using DRG codes involves billing for the DRG code and then billing again for services that were included in the DRG payment.

Upcoding, discussed earlier in this chapter, is essentially a narrow definition of DRG creep that applies in specific instances of code manipulation. DRG creep refers to a more systematic pattern of manipulated diagnostic and procedural coding. One way to distinguish between DRG creep and upcoding is to determine whether there should be revisions to the DRG after an examination of the medical records by coding experts.

Billing for Experimental Procedures

One form of medical fraud is the billing for experimental use of new medical devices that have not yet been approved by the jurisdiction's health care authority. Some hospitals are deliberately misleading third-party payers by getting them to pay for the manufacturer's research. Many of the doctors involved are alleged to have stock in the manufacturing companies.

Improper Relationships with Physicians

Certain relationships between hospitals and physicians result in fraud to insurers and health care programs. Note that whether the relationship is improper often depends on whether the physician is employed by the institution. The following transactions are generally regarded as suspect:

- Payment of any sort of incentive by the hospital each time a physician refers a patient to the hospital
- Provision of free or significantly discounted billing, nursing, or other staff services
- Free training for a physician's office staff in areas such as management techniques, coding, and laboratory techniques
- Guarantees that provide that, if the physician's income fails to reach a predetermined level, the hospital will supplement the remainder up to a certain amount

- Low-interest or interest-free loans, or loans that may be forgiven if a physician refers patients to the hospital
- Payment of the cost of a physician's travel and expenses for conferences
- Payment for a physician's continuing education courses
- Coverage on the hospital's group health insurance plan at an inappropriate or very low cost
- Payment for services, such as consultation at the hospital, that require few, if any, substantive duties by the physician, or payment for services in excess of the fair market value of services rendered

Revenue Recovery Firms

Another form of health care fraud involves so-called revenue recovery firms padding medical bills. These billing consultants review patients' bills (months or even years after treatment) looking for charges that were missed. Critics have charged that too often these firms pad medical bills by adding on fictitious charges. The more charges that are added onto the bill, the more the revenue recovery firm gets paid. In addition, their employees might be paid bonuses for excess charges and might be pressured to meet monthly quotas.

Changing Codes

One of the most common methods used by revenue recovery firms is to change every hospital's or nursing home's billing codes. An example would be changing each code for an ordinary bandage so that the provider is charged for a more expensive surgical dressing.

Adding Items

Extra charges are added onto hospital bills by assuming that hospitals used certain items, even though there was no evidence of the procedure or service. For instance, if the hospital had certain procedures for which it sometimes uses a piece of x-ray equipment, the auditor reviewing the bill would always assume that the hospital had used the equipment, and would put it on the bill.

Kickbacks

Often, hospitals are unaware (sometimes intentionally) of the extent of the fraud committed by revenue recovery firms. In other cases, however, revenue firms report that they will contact a hospital or nursing home directly and tell them that if the institution will give them their bills, they will split the profit produced by the added charges.

Billing for Expensive Treatments

Numerous charges for the use of expensive treatments such as laser are added to patients' bills. Charges might be added after the patient had already been billed for the use of the laser.

Altering Records

In some instances, firms might actually alter medical records. For example, in one case, a firm added more than $1,300 to a patient's bill for video equipment that was supposedly used during surgery. To justify the fraudulent billing, the firm checked a box on the surgical record to indicate that the equipment had been used. After the original document was obtained, it showed that the box was not checked on the original form completed by the surgical staff.

Donating Organs

One hospital, which has ceased using a particular firm, reported that the firm regularly double billed for services and treatments, and in another instance, outside auditors found that the firm had tried to charge for dead patients donating their organs.

Additional Anesthesia Time

Another common scheme is the charging of additional hours of anesthesia. Patients should be billed from when they enter the surgery room to when they leave the surgery room. The revenue firm pads the bill by increasing the time billed to include time spent in a recovery room, or before the patient went into the operating room.

Rent-a-Patient Schemes

So-called *rent-a-patient schemes* involve paying individuals to undergo unnecessary medical procedures that are then billed to the patient's insurer or health care program. These schemes occur in countries using a third-party-payer system or single-payer system that allows private providers to bill health care programs.

Rent-a-patient schemes typically begin with the leasing of a sham medical clinic. Past investigations show that these clinics tend to be nondescript, often within shopping centers, and in destitute sections of town. The lessee of the clinic is almost always involved in the criminal organization of the scheme. Once a sham clinic is in place, recruiters (a.k.a., "runners" or "cappers") are hired to solicit low-income individuals, often those who do not

speak the local language, and offer them money in exchange for submitting to "minor" surgical procedures.

EXAMPLE

A surgery center paid hundreds of dollars to patients who endured largely unnecessary operations and then falsely charged the government. One of the operations involved collapsing the patient's lung to snip a nerve that would supposedly control "sweaty palms." The surgery did stop the patient's not-so-sweaty palms from perspiring; it also caused the patient to lose strength in his hands and sweat profusely on other parts of his body.

Once recruiters have convinced an individual to become a willing participant, they will request a copy of the individual's beneficiary information to confirm benefits prior to subjecting the patient to an unnecessary treatment.

Recruiters will drive the patients to small clinics. Along the way, the recruiter will advise each patient to describe particular false and embellished symptoms to the health professional at the clinic, such as: "I sweat too much"; "My stomach is bothering me"; "My nose hurts." Such descriptions will later be used by the scam clinic to create medical charts, justifying a particular surgical procedure. The patients then wait in line, sign an informed consent form, and promise to give the clinic all the checks thereafter received. Following administrative procedures, the patients briefly meet with a doctor and undergo the procedures that have been predetermined for them. The recruiter will then give the patients a modest amount of cash and drive them home.

After rendering services, the provider will bill the patients' insurer or health care program for the unnecessary procedures beyond the usual and customary cost (past investigations evidence up to 5,000 percent above average market price). The claims will likely include fees for surgical supplies and medical equipment that were never used or distributed. Some insurers reimburse patients directly for out-of-network claims, thereby requiring the patient to pay the facility. However, because the patients targeted in rent-a-patient scams are often indigent and believe they deserve the money for enduring the unnecessary procedures, it is common for them to deposit or cash the checks. It is a cycle whereby the victims are not only used to perpetrate the fraud, but in the end become fraudsters themselves.

Health care programs have difficulty determining when rent-a-patient schemes are being committed because their claims systems can only compare codes and cannot determine the

usual and customary cost for a particular procedure. To make matters worse, rapid claims turnover inevitably leads to poor oversight regarding fraud-related claims.

What to Do?

Consumer education is the front line to battling rent-a-patient schemes. Health care programs must educate their beneficiaries on the prevalence of this type of fraud and provide these individuals with means of communication when they believe fraud is afoot. Disadvantaged populations must also be informed about the negative impacts of participating in such schemes, such as health risks and criminal liability.

Health care programs must educate from within. Investigation units should be established to include skilled fraud examiners. Fraud detection software programs should be purchased to detect irregular claims patterns. They should pool resources, insight, and intellect from around the country to circumvent and prosecute rent-a-patient schemes.

Red Flags of Rent-a-Patient Schemes

The following might indicate that a rent-a-patient scheme is occurring:

- Large influx of non-local patients to a particular clinic; including clusters of patients from a particular location
- Several non-related procedures on a patient in a short period of time (e.g., a colonoscopy and circumcision on one patient within a few days or even weeks)
- Numerous claims by a particular clinic for the following procedures: colonoscopies, endoscopies, septoplasties, circumcisions, and thoracoscopies with sympathectomy (a.k.a., "sweaty palms surgery")
- Parallel procedures on families (husbands, wives, and children) on the same day
- Extremely high staff salaries
- Charging beyond the average market price for procedures, medical equipment, and devices

Other Frauds in the Institutional Setting

The following are additional schemes that have a high risk of being perpetrated against medical institutions.

Write-Off of Patient Accounts

When a patient account or other type of receivable has been determined to be uncollectible, the account is written off to bad debts. It becomes a fraudulent transaction when the account has been written-off prematurely and the balance is subsequently collected, with the proceeds going to the employee. In this scheme, the employee has the opportunity to collect the receivable and divert the funds to himself because companies typically do not keep track of old written-off accounts receivable.

Often, old accounts receivable are assigned to a collection agency. These agencies typically are paid on a percentage of the collected amounts. Fraud schemes can be perpetrated by these agencies if the company does not monitor the method by which the agency receives old accounts and the collection process itself.

The assignor organization needs to assure itself that the collection agency is being assigned only old accounts and not good accounts that can reasonably be expected to be paid within the normal course of business.

Additionally, the organization needs to be sure that the collection agency cannot compromise the indebtedness so that collections are not reported. This would allow the collection agency to compromise indebtedness for its own collection and not remit amounts owed to the organization.

Credit Balances Fraud

When patients have more than one party responsible for payment for services provided, institutions have been known to collect more than the original amount billed. This might occur when the patient has coverage under multiple insurance policies, is a beneficiary of more than one health care program, is in a vehicle accident where multiple automobile insurance carriers are involved, or is in a situation where workers' compensation is applicable. In addition, the facility might also collect the deductible and copayment from the patient. If the hospital has a credit balance, the amount paid above the charges should be refunded to the applicable parties. However, this does not always occur. Generally, the refund will only be made upon request.

Theft of Pharmaceuticals and Supplies

Because of the ready market for selling pharmaceuticals and supplies, they have a propensity for being stolen. Narcotic drugs, although they are usually tightly controlled, still might be

stolen and sold on the street. Supplies such as canes, sunglasses after cataract surgery, and admission kits are popular items for theft or employee abuse.

Fraud in Special Care Facilities

Medical facilities that offer special care services, such as nursing homes and psychiatric hospitals, and the patients in them are at a greater risk of fraud than most other medical institutions. Many health care fraud schemes come to light after a patient reports strange charges or other red flags. Unfortunately, criminals take advantage of the fact that patients in special care facilities are more vulnerable to fraud.

There are several features unique to special care facilities that make them particularly vulnerable to fraud:

- Unscrupulous providers can operate their schemes in volume because the patients are all under one roof.
- Many patients in special care facilities do not have the legal capacity or ability to be responsible for their own financial affairs and, consequently, are not as likely to report fraud involving their care.
- In some instances, special care facilities make patient records available to outside providers who are not responsible for the direct care of the patient (sometimes in violation of regulations).
- In automated claims environments, scrutiny of the claims at the processor level is inadequate because the automated systems used do not accumulate data that would flag indications of improbably high charges or levels of service in a timely manner.
- Even when abusive practices are detected and prosecuted, repayment is rarely received from wrongdoers because they usually go out of business or deplete their resources so that they lack any resources to repay the funds.
- Patient personal funds are often controlled by the facility's administration and are an inviting target for embezzlement. Individually, patients generally maintain a relatively small balance in their personal funds accounts. Collectively, however, these funds generate a considerable source of income for an unscrupulous special care facility operator or employee.

Additionally, many special care facilities do not have the in-house capability to provide all the services and supplies their patients need. Accordingly, outside providers market their services and supplies to special care facilities to meet the needs of their patients. Some

special care facilities allow outside providers or their representatives to review patient medical records; these providers can obtain all the information necessary to order and bill for services and supplies that are not necessary or even provided.

Nursing Homes

Nursing homes are a growing sector of the health care industry. As such, they have become a common target of fraud. A wide array of providers—including medical equipment suppliers, laboratories, physicians, optometrists, and psychiatrists—have been involved in fraudulent or abusive billing for services and supplies furnished to nursing facility patients. Most fraudulent activity involves billing for unnecessary or undelivered services, or misrepresenting a service to obtain reimbursement.

Psychiatric Hospital Fraud

Psychiatric hospitals are susceptible to fraud because of the very nature of mental health problems and the manner in which they are diagnosed and treated. Unlike the acute care field, it is often difficult to determine whether a person is in need of hospitalization for psychiatric treatment.

Abuse in the Admissions Process

Some psychiatric treatment facilities have developed programs for patients who exhibit symptoms of both psychiatric illness and substance abuse problems. Fraud occurs when a patient is admitted on the basis of a diagnosis that reflects the patient's health care coverage rather than the patient's illness. Psychiatric hospitals have been accused of finding something wrong with patients when it is known that they have health care coverage. Such patients might often be admitted without examination by a physician.

Fraud in the Treatment Process

The following types of abuses can occur with regard to psychiatric treatment:

- Extending the length of treatment programs or delaying discharges because patients have additional health care benefits remaining
- The use of illegitimate, questionable, non-approved, or dangerous treatment programs and forms of therapy, such as brain wave synchronization, magnet therapy, memory retrieval/enhancement therapy, and deep sleep therapy
- Engaging in excessive treatment of psychiatric patients such as thyroid testing, drug tests, or psychiatric evaluation tests

Abusive Marketing Practices

Many medical institutions rely on marketing as a means of encouraging treatment and generating referrals. Overly aggressive marketing methods include:

- Paying bonuses to employees to persuade or pressure prospective patients to undergo a psychiatric evaluation and to admit themselves for treatment
- Encouraging patients to admit themselves by offering financial incentives, such as payment of plane fare, child care, and waivers of patient copayments or deductibles

Financial Rewards for Referrals

Many facilities are dependent on outside sources of patient referrals, such as physicians or other clinicians. This dependence has led some hospitals to develop economic relationships in order to obtain referrals:

- Rewarding clinicians who refer patients by referring patients who need outpatient treatment to those clinicians
- Allowing allied health professionals who refer patients to provide therapy for their own patients at the hospital, while nonreferring allied professionals are not allowed to use the hospital
- Paying medical directors or other physicians an incentive bonus linked to the overall profitability of the hospital
- Paying a physician who is under contract to the hospital but who provides no services

Red Flags for Psychiatric and Substance Abuse Claims

Fraud examiners should look for the following red flags of fraud from psychiatric institutions:

- Treatment takes place far from the patient's home.
- Patient is on disability.
- Provider's credentials are questionable.
- Documentation of treatment is lacking.
- Ancillary services are not treatment oriented.

Insured and Beneficiary Fraud

There are various schemes that insured parties and beneficiaries can commit against health care programs.

Fictitious Claims

If a health care program allows an insured or beneficiary to submit reimbursement claims, then such parties might make fraudulent claims. Medical bills can be photocopied over and over again–all the perpetrator has to do is change the dates and amounts and resubmit the bills for payment. This can continue until the perpetrator is caught, which generally occurs through computer edits, routine audits, or an informant. For example, beneficiaries or insureds might attempt to perpetrate a fraud by submitting fictitious claims forms for the following:

- Multiple surgeries
- Multiple office visits
- Foreign claims—patient supposedly goes out of the country and falls ill
- Noncovered dependents

Multiple Claims

A beneficiary with medical coverage under multiple programs or insurance policies might have the right to submit claims to more than one insurer and under more than one policy. However, all programs should be advised of multiple policies. If more than one insurance policy is in place, one insurance carrier is generally designated as the primary insurer and the other companies will be secondary or tertiary insurers. When the beneficiary is covered by both government programs and private insurance, some countries require the private insurer to pay its claims first, and the government only covers the remaining amount.

The patient commits a fraud when he makes a claim for a covered expense without revealing that he has already been paid for that expense. Such a scheme might involve both fraudulent concealment of the prior claim(s) and payment(s), and misrepresentation that the expense has been uncompensated.

Doctor Shopping

Patients might "shop" around for multiple doctors who will provide controlled substances. One physician often does not know that the other has prescribed the drug. In addition, the patient might shop for drugs in emergency rooms by complaining of soft tissue injuries, sprains, and strains.

Misrepresentation on Application

Certain health care programs, such as many health insurance policies, restrict the coverage provided for medical conditions that existed prior to the time the individual applied for or

was granted health care coverage (i.e., pre-existing conditions). When such restrictions exist, the individual is required to provide information about any pre-existing conditions during the health care program application process. However, individuals might intentionally fail to list all prior medical conditions in order to circumvent coverage restrictions on related health care costs.

Alteration

A dishonest claimant can inflate a prescription or medical bill by placing an additional number in front of the amount charged. The claimant can also alter the date of service so that it becomes a recoverable expense rather than one incurred prior to eligibility. The individual submitting a claim might change the name on the bill from a noncovered family member to one included in the health care plan.

Third-Party Fraud

This category involves an unauthorized use of an insured's identification card by another known person or unknown person. The insurance company is usually notified by the insured once he receives a benefit statement worksheet for services rendered.

Death of Insured

Secondary beneficiaries are in a position to commit fraud if the primary beneficiary passes away. The beneficiary might not notify the insurance carrier and continue to submit fictitious claims on medical expenses.

Divorce

Divorced parties might commit fraud against a health care program. For example, suppose that a primary beneficiary and a covered spouse file for divorce, but neither party notifies the health care program. The ex-spouse, who remains at the address of record, might continue to submit claims even though he is no longer covered.

Red Flags

A fraud examiner should be aware of the following indicators of fraud by insured individuals and beneficiaries under health care programs:

- Pressure by a claimant to pay a claim quickly
- Individuals who hand-deliver claims and insist on picking up their payment in-person
- Threats of legal action if a claim is not paid quickly
- Anonymous telephone or email inquiries regarding the status of a pending claim

- Identical claims for the same patient in different months or years
- Dates of service just prior to termination of coverage or just after coverage begins
- Services billed that do not appear to agree with the medical records
- Billing for services or equipment that are clearly unsuitable for the patient's needs

Detection

The following methods are helpful for detecting insured and beneficiary schemes:

- Conduct utilization reviews of outpatient services to ensure that requested services are necessary.
- Flag future claims of aberrant providers or insureds.
- Develop automated programs that identify excessive charges for prescriptions or medical services above an acceptable level.
- Perform built-in claims to identify and reject duplicate submissions.

Fraud by Insurance Companies

In countries where private insurance plays a role in the health care system, such as the United States, there are several fraud schemes that might be committed by such insurance companies. These schemes may include the following:

- Submission of false documents
- Mishandling claims
- Failure to pay legitimate claims
- Charging unapproved rates
- Requesting rate increases based on fraudulent data
- Deceptive or illegal sales practices
- Failure to give "fee breaks"
- Patient screening

Submission of False Documents

If the insurance company works in tandem with government health care programs (e.g., by acting as an intermediary for the payer, such as Medicare in the United States), then the insurance company commits fraud when it improperly bills the government or submits false cost reports or audits.

Mishandling Claims

Mishandling claims also arises primarily in the area of an insurance company acting as an intermediary administering the payer's insurance program. The insurance company is under a duty to try to detect false claims by providers and beneficiaries. Although it is impossible to detect every fraudulent claim, if a company bypasses its own claims verification procedures, it can be found guilty of fraud in some jurisdictions.

Failure to Pay Legitimate Claims

The insurance company or carrier is required to pay any claim that is properly submitted, contains all the required information—absent of fraud—and has benefits available. An insurance company might commit fraud when claims are consistently rejected even though the required information has been submitted. Some jurisdictions have regulations regarding the amount of time an insurance company has to pay a "clean" claim—one that has all the needed information. Even if an insured party has committed fraud in the past, and for some reason or another is still an insured, the insurance company must still adjudicate a valid claim.

Charging Unapproved Rates

Some jurisdictions require insurance companies to obtain approval on their premium rates (the price that insured parties pay to be covered by the insurance). An insurance company might improperly begin charging the unapproved rate before it is allowed to do so.

Requesting Rate Increases Based on Fraudulent Data

Insurance companies or carriers needing regulatory approval for rate increases use cost data to justify their increases. To get their rate hike, they might use fraudulent cost data.

Deceptive or Illegal Sales Practices

Insurance companies might promote or condone deceptive or illegal sales practices to increase sales. The most common example is to disguise an insurance policy as a savings plan or investment.

Failure to Give "Fee Breaks"

An insurance company might be guilty of fraud if it fails to pass on fee breaks it negotiates with its providers. The alleged overcharging occurs when an insurance company negotiates a discount on a medical bill. If the company does not pass along the discount, the consumer's copayment is made on the full price rather than the discounted price, and the consumer ends

up paying a higher percentage of his bill than he should. For example, if a bill is $1,000 and a 50 percent discount is negotiated, the consumer's 20 percent portion should equal $100. If the company does not pass along the discount, the consumer pays 20 percent of the full $1,000, or $200.

Patient Screening

Because so much emphasis is placed on preventive care, some insurance companies might reduce their risk by limiting their insured to only healthy patients, which is illegal in some jurisdictions.

Detection

Methods to detect fraud committed by an insurance company might include the following:

- Review complaints by insureds.
- Compare financial statement data to data used to request rates.
- Compare rates charged with rates approved.
- Compare discounts negotiated with providers with the amounts allowed on the claims and coinsurance charged.
- Review rejected members to determine if underwriting guidelines were abused.

Employee Claims Fraud

Employees of health care programs and insurers, especially claims examiners and customer service representatives, can present additional problems to the fraud examiner. Due to their ability to access claims and subscriber files, the frauds perpetrated by these employees against the health care program or insurance provider can be almost limitless. The employee might collude with program beneficiaries or might use a beneficiary's claim information without the beneficiary's knowledge. The following are some common employee claims fraud schemes.

- Claims fraud using the employee's contract
- Claims fraud using another beneficiary's (i.e., insured's) contract number
- Claims payment using a relative's contract
- Claims adjustment system
- Payment for canceled contracts or deceased insureds
- Improper payee schemes

Claims Fraud Using the Employee's Contract

Employees who process health care claims generally have access to claims data and claim forms. They might be able to fraudulently adjust claims or pull someone's claim, change the claimant's contract number, and have the claim processed.

Claims Fraud Using Another Beneficiary's Contract Number

In health care systems in which private insurance is used, employees who have access to individuals' enrollment files can locate an individual with a similar name as the employee. From there, the employee can easily complete a claim form and submit the claims through the regular processing system. The employee only has to put his own address in to receive the payment.

Claims Payment Using a Relative's Contract

Employees can fabricate claims and submit them under a relative's contract or government identification number.

Claims Adjustment System

Claims that are legitimately paid incorrectly need to be adjusted. However, an adjustment examiner might adjust a claim for fraudulent purposes.

Payment for Canceled Contracts or Deceased Insureds

If an adjuster has access to the enrollment files, he might search for a deceased individual. By submitting or processing a claim before the deceased's coverage is canceled, the adjuster can manipulate the claims system and divert payment to himself.

Improper Payee Schemes

A claim approver overrides a claim payment system and pays out claims to improper payees. For example, the claim approver might use the name and address of a family member or acquaintance for the payee information.

Detection

The following steps can be used to determine if a company is dealing with an employee who is defrauding the system:

- Pull high-value claim payments. Investigate all unusual patterns by verifying services.
- Review printouts for special payee codes to search for employees.
- Review printouts for a high number of adjusted claims per insured or beneficiary.

- Review printouts of recently canceled contracts for unusual claims activity just prior to cancellation.
- Review address change lists for employee names or unusual activity.

Once unusual activity has been identified, follow normal investigative procedures.

Prevention

The following are some measures that can be taken to help prevent employee claims fraud:

- Have a separate area to handle employee claims.
- Limit access to employee claims information.
- Set up automated monitoring controls within the claims system to generate exception reports for high-value claims payments and multiple adjusted claims.
- Inform employees that audits are conducted regularly.
- Require and enforce adjusters to sign off their terminals they are not in use.

Electronic Claims Fraud

Electronic data interchange (EDI) is the exchange of electronic data between computers, with no human interaction. While this technology has advanced the ability to conduct business quickly and easily, it has also provided would-be fraudsters with an increased opportunity to commit white-collar crimes.

EDI's origins are in the 1960s, when many industry groups started to develop EDI standards in areas such as purchasing, transportation, and financial transactions. The next major step forward came when EDI-focused associations developed the first standards of electronic data interchange. At this time, they have developed more than 300 different standards for individual industries concerning the transmission of EDI. These standards are published by the Data Interchange Standards Association.

Although these standards have been adopted and used worldwide by a multitude of different industries, the health care industry had been notoriously slow in adopting the new technology because the health care system is so complicated that a switch in operation procedure of this magnitude would be difficult and expensive to implement. However, a substantial number of health care providers have endorsed the industry conducting business electronically.

EDI can be used internally within a business as a way of communication and data transfer, and it can also be used for the same purposes between different businesses. In the case of the health care industry, EDI enables the different companies to send claims, invoices, and other vital data that once was shipped in a paper format via the postal service. The fact that EDI allows for an immediate exchange of data makes the process of submitting and approving health care claims much more efficient for the health care industry.

The health care transactions affected by EDI include:

- Claims payment
- Enrollments
- Claims submission
- Eligibility
- Claim status
- Crossover COB
- Health care service review
- Patient information record
- Capitated payment
- Interactive claim
- Provider information

EDI has the potential to save the health care industry vast amounts of resources. It is very simply a more efficient way for the health care industry to do business. However, fraud examiners fear that a more efficient system also paves the way for more efficient ways to defraud the health care industry.

Solid controls must be established to deal with the health care industry's conversion to EDI, or else the potential savings might be eroded by bigger fraud losses. The electronic conversion of information completely removes paper-based controls.

Auditors reviewing electronic claims often use the same techniques as when auditing any other type of health care claims, but they might examine electronically transmitted information rather than original documentation. If the electronic information is reliable, then there is no difference; however, history has proven that electronic claims provide ample opportunity for fraud.

EDI frustrates fraud examiners' ability to detect fraud in the health care industry in three ways:

- The automation of claims has erased claims professionals' ability to detect suspicious-looking claims. Because they are used to handling the paperwork of claims, EDI hampers the claims professionals from getting a good picture of the overall nature of an account, instead reducing each transaction to individual claims.
- Because of the impersonal nature of electronic transactions, EDI raises the temptation of would-be fraudsters to commit white-collar crime.
- EDI leaves no paper trail, making the process of fraud detection difficult for the fraud examiner.

The reasons the health care industry is concerned about EDI's potential to stimulate fraudulent activity include:

- The lack of tools to detect EDI fraud
- The variety of health care services increases the potential for dissimilar frauds
- The efficiency of EDI allows for more vendors and thus more claims to account for
- The swiftness in which transactions take place allows less time to uncover fraud

In the past, the health care industry has developed sophisticated methods of detecting fraud within the paper-based system. Now that the conversion to EDI is taking place, the health care industry must find a way to apply those methods to the electronic format. These methods will only be as sophisticated as the health care industry chooses to make them; the less concern that the industry shows for creating fraud indicators, the more opportunity it gives fraudsters to "beat the system."

Fraud examiners should not fear that the conversion to EDI will eliminate any fraud-related job opportunities. In fact, that conversion will actually open up many fraud examination jobs, as the safeguards and red flag system against fraud have not been effectively established at this time. Therefore, fraud examiners need to be aware that their jobs include not only investigating fraud, but also creating systems that can effectively deter fraud.

Many new and complicated legal issues are raised as a result of the health care industry's conversion to EDI, such as:

- How does the insurance company or health care program prove that all electronic claims are authentic?
- Who is responsible for errors in electronic health care claims?

- How does the fraud examiner prove that the contents of an electronic health care claim are false?
- How does the health care industry ensure that all electronic transmissions are received exactly as they are sent?
- What terms and conditions govern electronic claims?
- How will fraud examiners determine the actual origin of electronic submissions?

Because automated claims are easily altered, the health care industry must ensure that claims are authentic. Fraud examiners should document that claims have been received in the same condition in which they were processed to help ensure that they are admissible as evidence.

Some examples of ways to ensure claims' authenticity include:

- Data encryption
- Digital signatures
- Message authentication codes
- Prior claims' history checkups
- A variety of field checks

CONSUMER FRAUD

Complaints of consumer fraud can be found as far back as the first century when Pliny the Elder told of the adulterated honey being sold in Rome and the mixing of wine with gypsum, lime, pitch, rosin, wood ashes, salt, sulphur, and other artificial additives. Schemes against consumers range from home repair frauds to more sophisticated scams.

Fraud is notably common in the repair and service industries. Home repair fraud, frequently perpetrated against the elderly, ranges from the sale or use of substandard materials—such as roofing—to securing payment without doing any work at all. Automobile repairs often involve fraudulent acts. One study maintained that 53 cents of every "repair" dollar was wasted because of unnecessary work, overcharging, services never performed, or incompetence.

In Australia, John Braithwaite found that used car dealers rolled back odometers on a third of the cars they offer for sale. Interviews with the dealers in Australia illustrate the kind of reasoning that can buttress such illegal activity. One salesman said: "People pay too much attention to the mileage reading on a car. There might be a car with a low mileage reading but all sorts of faults, and another perfect car with a high mileage reading. It doesn't matter what the mileage reading is, but how good the car is. So if you turn the mileage reading back on a car in perfect order, you're encouraging people to buy a good car." There was no evidence, however, that it was only on "good" cars that the odometer was made to provide a lower reading.

Another Australian dealer said: "They think because you are a used car dealer you are a liar. So they treat you like one and lie to you. Can you blame the dealer for lying back?"[1]

Con Schemes

Confidence games involve a range of fraudulent conduct usually committed by professional "con artists" against unsuspecting victims. The victims can be organizations, but more commonly are individuals. Con men usually act alone, but they might group together for a particularly complex endeavor.

[1]John Braithwaite, "An Exploratory Study of Used Car Fraud," in Paul R. Wilson and John Braithwaite (Eds.), *Two Faces of Deviance*. Brisbane: University of Queensland Press, 1978, pp. 101–122.

The following are some of the many kinds of confidence schemes. Telemarketing schemes and pyramid schemes are discussed in more detail at the end of the chapter.

Advance-Fee Swindles and Debt Consolidation Schemes

Advance-fee swindles are structured to obtain an illegal gain by falsely promising the delivery of a product or service. In some schemes, the product is marketed to a large number of customers, and then the operation is shut down prior to the delivery stage.

People who find themselves in debt sometimes turn to consolidation agencies for help. These agencies do not advance loans, but rather act as an intermediary between debtor and creditor. Some agencies are legitimate, but many are not.

In a typical scenario, the debtor contacts the agency, which compiles a list of the creditors and the amount of monthly payments. The agency usually writes letters to the creditors requesting a workout plan at lower monthly payments spread over a longer period of time. The creditors will often offer such an arrangement if they feel that the debt will thereby be paid or if the workout plan will forestall bankruptcy or default by the creditor.

Unscrupulous debt consolidation schemes often involve the agency collecting the money from the debtor but not forwarding it to the creditors. In some instances, considerable time can pass before the debtor finds out that his money has been misappropriated.

Another variation of the debt consolidation scheme occurs when a customer is guaranteed that he will receive a loan or a credit card regardless of his credit rating. Typically, the victims have been rejected by legitimate financial institutions because their credit ratings are poor. The victim must pay a processing fee for the application to be accepted. After the victim pays the fee, the con artist disappears.

Directory Advertising Schemes

The essence of directory advertising schemes is the sale of advertising in a nonexistent magazine or directory. A fake (or, in some cases, a real) directory is shown to the potential victim. The victim contracts and pays for display or classified advertising that is to appear some months in the future. By that time, the fraudster has disappeared.

Personal Improvement Frauds

These frauds prey upon the desire of people to improve their education or job skills; in some instances, they appeal to a person's appearance.

Diploma Mills

For what is often a hefty fee, a diploma can be purchased by those who apply. The fraudster usually claims that the fee is for processing the application or for verifying the experience necessary for the degree to be awarded. The hallmark of the diploma mill is the ease with which the degree is obtained. Because the school is not accredited, the degree is essentially worthless.

Modeling Schools

Modeling schools appeal to the vanity of some people. In the typical scheme, the modeling school representative tells the prospective student that he will prepare a portfolio of portraits to be sent to potential customers who might employ the victim as a model. The victim is then charged an inflated price for the pictures. Con game modeling schools often claim—inaccurately—connections to famous people and maintain that they have been instrumental in starting the careers of successful models. The schools sometimes target parents and grandparents with lures of the money that can be earned by their "exceptionally pretty" infant children or grandchildren.

Direct Debit from Bank Accounts

When a customer decides to purchase an item (from a catalog, online, or over the phone), he is told he can purchase it rapidly and simply by giving his bank's name and account number for a direct debit from his account. This results in unauthorized withdrawals from the account.

Equity-Skimming Schemes

Falling for this scam can cost consumers their homes. Con men try to talk the mark out of the equity on their homes and might try to persuade them to borrow against their equity.

Fundraising, Nonprofits, and Religious Schemes

Some groups use "cancer" or "AIDS" in their title to convince the consumer they are legitimate charitable organizations. Others offer a prize or award for the consumer as a reward for his contribution. In recent years, a concept known as *crowdfunding* has become

a popular online method of raising money for myriad causes and has already led to reports of fraud.

Home-Based Businesses

Decades-old home-based business scams have in recent years migrated to and flourished on the Internet. These scams are especially effective during a downturn in the economy and typically prey on those who are desperate for work or supplemental income. Many companies marketing home-based businesses require a person to buy materials for assembly-at-home products, while other common ploys include stuffing envelopes or processing medical bills. The consumer is promised that the company will purchase the completed products, and when it does not, the consumer is left with a bad investment and a stock of low-quality, worthless goods.

Home Improvements

A common scam involves phony repair people selling their services door-to-door. After paying the fraudster in advance for the materials needed to fix a roof, window, or other item, the consumer is left with unfinished repair work and no workmen.

Money Manager or Financial Planner

These scams involve convincing marks to invest in low-risk, high-return opportunities. Of course, consumers who invest in these opportunities see no returns at all.

Scavenger or Revenge Scheme

This involves the company that initially conned the consumer. Using a different company's name, the outfit contacts the consumer again and asks if he would like to help put the unethical company out of business and get his money back. Naturally, an upfront fee is required to finance the investigation.

Sweepstakes, Giveaways, and Prizes

Many of these so-called "free gifts" require the consumer to pay a fee (usually labeled a "shipping" fee) before collecting. This fee actually covers the cost of the merchandise deemed "free."

College Scholarship Services

This bogus service usually charges an upfront fee or advance payment fee for finding a scholarship suitable for the applicant.

Credit Repair

Some of these firms might charge unnecessary fees to fix credit problems, knowing that the consumer could easily call the credit bureau and request a copy of his credit report himself.

Other Con Schemes

Block Hustle

These schemes get their name because purveyors of cheap stereo equipment, jewelry, and watches usually peddle their goods on street corners or at traffic lights. The items for sale are generally either stolen or imitations of brand names.

Pigeon Drop

This is often used on middle-aged or elderly women who are likely to have a savings account. Pretending to find a wallet full of money, the con men convince their mark that they should divide the "discovered" money. As a show of good faith, each should withdraw a sum of money from their bank and turn it over to a lawyer or another third party for safekeeping. They agree to place an ad in a newspaper for the lost wallet. If it is not claimed within a certain amount of time, they will split the money. Of course, when the designated time expires, the victim will find that the lawyer was part of the scam and that her money has vanished.

Bank Examiner Swindle

Bank examiner swindles are also perpetrated against older women, especially widows with access to their husbands' life insurance policies. The con man impersonates a bank examiner investigating the victim's bank. He asks her to withdraw a certain amount of cash from her account, place it in an envelope, and allow him to inspect the bills for counterfeits. Many con men use false IDs and dress to take on this role.

Jamaican Handkerchief or Envelope Switch

In this con, the criminal puts his money into an envelope with the mark's money and then unobtrusively trades this parcel for another that looks like the same thing but is instead bulked up with worthless paper.

The Obituary Hustle

Capitalizing on a bereaved person's grief, the con man, culling information from an obituary, poses as a delivery person collecting money for a package or other order the deceased supposedly made.

Three-Card Monte

Also known as "Find the Lady," this is an old card game that involves two people who fleece an unsuspecting onlooker into a rigged game.

Poker Bunco

This scam can involve poker, dice, pool, and other games. The con man is of course an expert and hustles the mark.

Missing-Heir Scheme

In the modern version of this scam, the con man poses as a probate investigator or other genealogist, charging fees to distribute an inheritance.

Gold Mine Swindle

Here, the con man claims to own a productive mine but requires money to start operation. The scheme involves selling shares to the mine.

Spanish Prisoner Game

This con can be traced back to the Spanish Armada of the sixteenth century. A businessman receives a letter purportedly from a hostage held prisoner in some foreign land. He needs money to bribe his captors or pay a ransom. As collateral, a treasure map or other "valuable papers" are often enclosed.

Murphy Game

Also known as "Miss Murphy," "paddy hustle," or "carpet game," the traditional con is played in places where prostitution occurs. The con artist plays a pimp but never delivers the prostitute.

Badger Game

A refined version of Miss Murphy, but in this con, the con woman or prostitute is in on the scam. The con artist robs the mark of his wallet through simple theft or pretense of blackmail.

Goat Pasture Scam

The mark receives a call from a person who says he's from an oil and gas service that is sponsoring a lottery on mineral rights. If the consumer invests a certain tax deductible sum, he can receive a percentage of the income in royalty payments.

Telemarketing Fraud

While the telephone, newspaper, and postal service used to be the key tools of telemarketers, the Internet has afforded fraudsters a more fast-paced and anonymous method of carrying out their schemes. Telemarketing offenses are classified as consumer fraud, yet many businesses are affected by office supply and marketing services scams. The hit-and-run nature of phone rooms, the geographical distances between the perpetrators and their victims, and the resources and priorities of law enforcement agencies all make enforcement efforts difficult.

Telemarketing Terminology

Terms in the scammer's vocabulary include *banging*, or *nailing*, the customer (i.e., closing the deal). A salesperson's most effective skill is *puffing*, the ability to sound convincing while exaggerating the value of a business opportunity or gift. To make the puffing more persuasive, marketers hire *singers* or *criers* to tell potential victims what a great deal they are getting. Calls from angry customers who realize they have been swindled are known as *heat calls*. These are handled by someone claiming to be the company's manager or vice president.

Boiler Room Staff

Work in a *boiler room* is shared by *fronters*, *closers*, and *verifiers*.

Fronters

The fronter calls victims and makes the initial pitch. This low-level worker is usually breaking into the business and reads from a script to the prospective customer. Fronters seldom see the merchandise or know the full extent of the operation, which potentially limits what they can tell investigators and protects them in the event of prosecution.

Closers

The closer is a veteran. Fronters pass an interested caller to their closer, identified as the firm's "manager," who convinces the person to buy.

Verifiers

Next, the caller is passed to a verifier, who reads some vague words about the deal and records the person's agreement. These recordings are intentionally vague, leaving out the pitch and key details—essentially recording only the customer's consent. Verifiers also stall customers who call back to complain (*heat calls*), finding reasons why a little more patience

will solve the problem, and in some cases, convincing the person to send a little more money to help the process along.

Staff Exploitation

The customers of fraudulent telemarketing operations are not the only victims. Fronters are often poorly educated and easily taken advantage of by the career criminals who run the operations. Salespeople might face hidden costs in a work agreement, similar to the ones involved in the items they push on unsuspecting customers. For example, boiler room operators hold back parts of their phone lists and sell them to crew members as "hot leads." Telescam veterans know how to operate a gift sting that bilks both the customer and the salesperson. Operators overstate the retail value of the gifts, so the customers get less than they paid for; then, by giving agents an inflated wholesale cost, the operators can pay these workers less commission, which is figured on the "profit margin" between wholesale and retail.

The salespeople in boiler rooms are sometimes as desperate as their victims. Most are unemployed, with little education or marketable skills. Telemarketing promises easy work and big pay without any experience. Many people who start out as fronters, however, are serving an apprenticeship in their criminal careers. They are wooed with cars, mobile phones, and other perks. Former workers have reported that supervisors sprinkled lines of cocaine along the phone bank table and threw handfuls of money into the air, promising the proceeds to whoever made the next sale.

Naturally, there are no payroll taxes deducted from paychecks, so employees can owe big tax bills at the end of the year. Fronters' commission payments are often shorted or withheld. Paychecks frequently fail to clear the bank. Owners promise big profit shares for a month or two, and then shut down the business. They tell the workers that their assets have been frozen by creditors or regulators. Workers lose their jobs and usually their last weeks' commissions.

Telemarketing Suppliers

The telemarketing industry relies on a number of sources to supply its phone scripts, mailing lists, merchandise, phone banks, and autodialers. Mailing lists and phone lists are sold for a few cents per name. Lists of people who have been stung before or who have bad credit records are more valuable to the scammer and therefore more expensive. By supplying

telemarketers with the tools of their trade, these companies make telescamming possible. Many of the suppliers are aware of telemarketers' criminal intentions and choose to ignore them.

Turnkeys

Turnkeys comprise an industry of their own by providing the collateral a telemarketing scam needs: turnkeys launder credit card receipts and checks, sell autodialers and phone lists, and provide the merchandise portrayed as valuable prizes.

Independent Service Organizations

Telemarketers often have difficulty securing credit card services from reputable institutions. Many banks will not open credit-processing accounts for businesses that do a substantial amount of their business in phone sales because these accounts typically incur a high rate of chargebacks. Consumers have 60 days to protest fraudulent charges to their credit cards, and if successful, the issuer has to absorb the loss.

Telemarketing operations have learned the difficulties they face when dealing directly with banks. To circumvent this obstacle, phone sales companies hire "independent service organizations," which approach banks on the telemarketer's behalf. The service company agrees with the bank to cover any chargebacks from the operation. The telemarketer is required to post a large bond to cover potential losses, so the service organization is also protected from loss. However, even with a high-value bond, the reserve funds can be quickly depleted when customers start to realize they have been swindled, leaving the service company and/or the bank with enormous losses.

Factoring Companies

Telemarketing operations also commonly engage factoring companies. These groups buy credit card receipts from telemarketing concerns at a discount, and then use their merchant bank accounts to convert the receipts into cash. Some factors charge as much as 30 percent of the receipts' gross value to launder the slips. Factoring is illegal in some jurisdictions, though perpetrators find ways to slip through loopholes or disguise their alliances.

INTERNATIONAL FACTORING COMPANIES

Factoring through Asian and European merchants is becoming increasingly common. Factoring companies in these countries tend to charge a lower price for their services than some other countries—between nine and ten percent of the gross. Regardless of their locale,

factors have the opportunity to make a great profit. They also, however, face the risk that banks will freeze their accounts or sue them for excessive chargebacks. In response to the losses suffered at the hands of dishonest telemarketers, banks and credit card companies have started reviewing their accounts to locate those businesses with inordinate numbers of chargebacks. The financial institution closes these accounts, and might file suit if the account holder can be located.

Check-Cashing Establishments

Another convenient tool at the telemarketer's disposal is the check-cashing store. If a boiler room operation wishes to avoid the risks of setting up a bank account that might be traced or seized, customers' personal checks are taken to a company that cashes them for a small fee. These establishments rarely require any identification to cash the checks. Customers might complain and try to stop payment on their checks, but they are ordinarily too late.

Common Telemarketing Scams

Senior Scams

Elderly people are the favorite prey of telescammers. Fred Schulte, author of *Fleeced!*, relates the pitch delivered by Tim O'Neil to an elderly woman in the U.S. city of Philadelphia, Pennsylvania. The woman told detectives about the more than $10,000 for which O'Neil and his lieutenants swindled her. O'Neil's call to mollify the woman's protests was recorded by the U.S. Federal Bureau of Investigation (FBI). On the line, he insists that the "collectibles" the woman bought, including "actual bullets excavated from the American Civil War," are genuine and valuable.

> *Do you wear pendants? This is a beautiful, is a diamond … I'm not gonna ask you to spend a penny …*
>
> *How old are you? God bless you … 89 …*
>
> *We're gonna get that out to you … Look for it in the middle of next week, and then give us a call and then let us know how you like it …*
>
> *Well I hope I put a little sunshine in your day. Okay, honey, and God bless you. Oh, don't cry now, we're here to take care of you … We'll be here and if you need to talk to anybody at any time you give us a call, okay? Bye, bye, and God bless you.*

Telemarketers usually call in the evening. Seniors might be more vulnerable to pitches promising them extra money and luxury goods because many live on fixed incomes. These lottery-style gambits can seem like an easy way for the elderly to improve their financial status.

Targeting the Unemployed

The unemployed are another favorite target for sweepstakes pitches and job search services. Whereas "the system" has left the jobless without hope, the telemarketer offers a way around official channels. People with bad credit pay telemarketers to "repair" their credit record or get a major credit card. Instead, they get a list of banks that offer credit cards, commonly published in newspapers, or an application for a card that requires a security deposit for activation, usually several hundred or a thousand dollars. These people are also targeted by advance-fee loan scams, which promise loans in exchange for a fee.

Affinity Fraud

Affinity fraud targets groups of people who have some social connection. Neighborhoods chiefly populated by racial minorities, especially immigrant groups, are often the site of affinity frauds. Religious and professional ties are often exploited. Marketing technology has made it possible for a company to buy targeted lists, not just by location, but according to buying habits, leisure activities, and club memberships. The most expensive lists carry the names of people who have already fallen for a telemarketing scam. This is called *reloading*.

Consolation

When irate customers call telemarketers back to complain, their calls are routed to professionals who placate the caller with more promises and obfuscations. Some boiler rooms have a prearranged communication route for leading complaints through four or five different "departments." This tactic causes many callers to eventually hang up without having spoken to anyone. In some instances, telemarketers confronted with furious callers threatening legal action do award something of value to the customer, though the item is usually worth far less than the person has paid.

If obfuscation and consolation prizes fail to appease the caller, the con turns to threats and intimidation. This is a favorite method for dealing with senior citizens, especially elderly women. Threats are used not just to keep customers from filing complaints, but to cajole more money out of them. Some telemarketers have actually threatened callers' personal safety if they refused to pay.

The odds of catching a boiler room operation in progress are usually poor. Operations can select a town, set up a room, make their haul, and leave again in a matter of weeks or months. When authorities raid a boiler room, the operation has typically already moved on.

If the company owners registered with the appropriate regulators, they probably did so under an alias. By the time police arrive, the perpetrators have moved on and the chances of finding them are slim.

Toll-Free Numbers

Toll-free numbers offered by phone service companies are used by some operations. The scam is a toll-free line, advertised in mailers, fliers, and newspaper ads, to lure victims into making the call themselves. The toll-free number usually carries a recording that directs customers to a different line that charges the caller a per-minute fee to hear recorded messages. A favorite device of sellers is to insist that the offer being made is good for less than 48 hours. To secure the opportunity, the customer hands over a cashier's check to an overnight-delivery service. Even if the victim does have second thoughts, he will be unable to stop payment on a cashier's check.

Automatic Debits

The personal bank account is a convenient tool for defrauding telemarketing customers by setting up an automatic debit to the buyer's account. Telemarketing operations use this method to obtain payment before victims can change their minds about their purchases. Worse, telemarketers can simply use the information to drain the victim's account. This information is usually obtained by telling the victim that the account numbers are needed to verify eligibility for a giveaway or business opportunity. Banks are not responsible for any losses customers suffer in this way, so there are no chargebacks and little recourse for the swindled customer besides filing a complaint. Even if an investigation of the complaint brings the scammer to court, the chances that the victim will receive restitution are poor.

Business Opportunities (Biz Ops)

Many telemarketing frauds are aimed at people starting their own businesses. Regulators put losses in fraudulent business opportunities at over $100 million a year, and most observers think the number is far higher.

Work-at-Home Schemes

Besides franchise offers and other miscellaneous business scams, the most prevalent frauds involve work-at-home schemes. Victims of these phony offerings do not see themselves as part of the telemarketer's prey. They believe they are making a legitimate business investment.

Telemarketers use business-related terms such as *exclusive territory*, *annual gross revenues*, and *emerging markets* in these calls. This helps convince the mark that the biz op is legitimate.

Some business-pitch operations are complete fabrications. They offer envelope stuffing or book-review enterprises that do not really exist. Scammers mail out postcards, buy cheap ads in magazines and newspapers, or send out spam emails. Some might not even take any phone calls. The ads convince the victims to send money to a mailbox or via an online payment method. Many private companies will rent mail-drops to anyone for a monthly fee.

Fly and Buy

Some scams involve ventures such as vending machines, Internet terminals, and merchandise display racks. They often gain credibility by setting up a front operation and inviting investors for tours. This part of the ruse is known as the "fly and buy." For example, the promoter usually schedules a meeting with the potential victim. The promoter will then offer to let him in on a deal for something such as video pool and video bowling games. Thrilled with the demonstration and the promoter's promises of quick profits, the victim will pay thousands of dollars for the machines. Unfortunately, they often break down within a few months. Complaints generally go unanswered, or by the time the machines break, the promoter has moved on to other victims.

Entrepreneurial Enterprises

Telemarketers do not only deal in machinery-oriented scams like those described previously. The raising of exotic animals like ostriches and emus for luxury items and for slaughter has been a popular scam for a while, including weekend retreats to a model farm for would-be ranchers.

Whatever the nature of the opportunity, there are signs that indicate that it is not legitimate. Among the most common are:

- Classified ads urging the prospect to call a toll-free number
- Wild, unsubstantiated claims about potential earnings

- Promises about exclusive territories, assurances about good locations, or the assistance of a professional locator
- References specified by the company
- The lack of a complete disclosure document containing information about the promoter's experience, lawsuit history, audited financial statements, and substantiation for earnings assertions

Employment Services

The phony employment service is similar in nature to the biz op. Preying on the unemployed, these scams promise good jobs, many of them overseas, with the added enticement of tax-free wages. Victims pay between $250 and $1,000 for the service. Some get lists of government jobs, which are usually available for free, or listings from classified ads. Most get nothing.

Credit Services

The simplest credit scam promises that the company will secure a loan for the applicant, regardless of credit history and references, if the person pays an upfront fee, usually between $35 and $75. Checking account debits are a favorite payment method, as are 900 numbers, which charge by the minute to hear information widely available that provides no help in swaying a loan for the listener. Usually, there are few or no loans made. Occasionally, loan information and applications might be mailed out to the victim, but usually the operators are not heard from again after the fee has been paid.

Credit Repair Scams

Similar to loan scams are those that promise to repair credit. Pitch men like to say they can "wipe away," "doctor," or "cosmeticize" blotches on credit, insinuating they have ways of changing or disguising a person's credit history. Despite the fact that there is really no way to erase bad credit, many people fall for this scam, paying large sums of money to expunge their records.

Prime-Rate Credit Cards

In this scam, telemarketing companies assure customers they can get major cards for a small fee even if their credit report is poor. Victims receive an application for a credit card, which they could obtain in any department store. Telemarketers also push secured cards, which require a cash deposit to the issuer's bank to activate the card.

Gold Cards

A relatively new credit card sting on the Internet touts "gold card" status for customers, regardless of credit history. The advertisement claims applicants will be processed for a major credit card. In actuality, applicants are merely assisted in filing an application for a major credit card, a worthless service since applications are quite simple to complete and submit. For a large upfront fee, participants receive a "catalog card," which is only redeemable if the holder buys the company's over-priced, low-quality merchandise listed in the catalog as discounted for cardholders. Even then, an actual purchase might require paying additional fees or cash deposits before the customer is allowed to charge the remainder. Since the issuers do not report payment activity to any of the credit reporting bureaus, using the card does not improve the customer's credit rating.

Lotteries/Lottery Clubs

Consumers receive a false claim that they have won, or can get help to win, a lottery, often in a different country. Most lottery scams are perpetrated by con artists in other countries, sometimes using local addresses to disguise their real locations. Sometimes the lottery actually exists, but invitations to play don't come from governments that operate legitimate lotteries or anyone connected to them. The consumer has no way of ensuring that they will receive the tickets that they pay for or, in the unlikely event that they do win, will ever be able to collect their money. In many countries, it is illegal to play lotteries across borders. Differences in legal systems, difficulties of conducting investigations in other countries, and expenses and other complications involved in pursuing cross-border fraud make the chances of a consumer getting his money back very slim.

Buyer's Clubs

This scheme involves membership in discount buying clubs that consumers never agreed to join or were signed up for through free-trial offers. Consumers should beware of advertisements for products at incredibly cheap prices or for free if the consumer pays for shipping, as these offers might be designed to lure the consumer into a buyer's club membership. Another way to avoid being a victim of a buyer's club scheme is to understand how a "trial-offer" works. In many cases, the consumer will automatically be charged for a membership when the free-trial expires unless he contacts the club to cancel. The consumer should ask for the details of all membership offers in writing before agreeing to join. If unauthorized charges or debits are noticed on monthly statements, the consumer should contact his credit card issuer or bank and ask for his account to be credited for these unauthorized charges.

Travel/Vacation Schemes

These schemes involve offers of free or discount travel that never materializes. Consumers need to be skeptical of offers for "free" trips. Airlines and other well-known companies sometimes operate contests for travel prizes; however, there are also companies that offer "free" trips to try to lure people into buying their products or services. Consumers also need to know what is included with the trip; a "free" or incredibly cheap trip might have hidden costs. For instance, the cruise might be free, but the consumer has to pay to fly to the departure point and stay in a hotel at his own expense. Or he might have to endure a long, high-pressure sales pitch for a timeshare or travel club membership as part of the trip. Often, the best travel deals are only available for off-peak times, not during holidays or other popular travel dates.

To avoid being victims of travel/vacation schemes, consumers should confirm all travel arrangements. If transportation and hotel are included in the travel package, ask how to contact those companies and confirm with them directly that the reservations have been made. Consumers should do their own travel research; it's easy to get information from a local travel agent or the Internet. When making travel arrangements, it is advisable to pay with a credit card. Fraudulent travel operators can take a consumer's money and run, and even legitimate companies can go out of business. Paying with a credit card allows the consumer to dispute the charges if the promises that are made are not kept.

Real Estate

Real estate scams are easily recognized. There is almost always an element of time pressure, with the victims being convinced they are participating in a "once-in-a-lifetime, now-or-never" deal. The investors are led to believe there is no time to investigate the venture, and that if they hesitate, they will miss the opportunity to make a fortune. Promises of big profits for little or no involvement are the norm in real estate scams. The investor is also misled into assuming he is being let in on a special offer or an exclusive deal by the promoter.

Companies tout the riches available in real estate through seminars and books that claim to offer secret ways to cash in. The customer pays for the secret info and gets worthless tips in return.

TIMESHARES

Another scam sells timeshares in condominiums for travelers. Telemarketers pass themselves off as brokers to condominium owners and purport to specialize in selling timeshares.

OPTIONS

Some real estate ads try to coax investors into buying "options" on property. Supposedly, the option locks in a present-day price on behalf of the purchaser, who can exercise the option later if he wishes to buy the land or to sell it at a profit. Sometimes the investor has bought nothing but a piece of paper—the "agent" has no authority to make deals on the property. Occasionally, the option is only valid for a few months, or is too vaguely worded to be enforceable. Usually, there is an actual plot of land, but in most instances, it is undevelopable due to location or zoning restrictions, and is therefore worthless.

DEVELOPED PROPERTY

Various developed property schemes have been identified around the globe. These scams often involve a large deposit toward a property in a paradisiacal location such as Belize or Costa Rica that might or—more likely—might not be refunded dependent upon contractual technicalities. Those who do buy property through these schemes often find that their property is not as advertised or is heavily restricted from further development. In one example, the General Development Corporation of Florida ran a legendary land fraud scam in which potential investors were shown lots and houses guaranteed to make them rich. In this rendering of the "buy-and-fly" scheme, victims were shepherded and their contracts restricted until they signed a deal. The scam continued for approximately six years and cost victims millions.

Art/Rare Items

Land deals prey on the public's reverence for real estate. The con who deals in art objects preys on a similar impulse—the reverence for the rare. Paintings worth little more than their canvas and oil are tagged as "masterpieces" sure to grow in value. The victims who fall for these scams tend to be art novices who seem to unquestioningly believe the "dealer's" appraisal of the piece.

Victims buy lithographic prints, mass-produced by the thousands, thinking they are purchasing "limited editions." Any anxieties the victims might develop are calmed by a promised 30-day, no-obligation trial and with "certificates of authenticity." Among the most popular artists to counterfeit are Salvador Dali, Pablo Picasso, Marc Chagall, and Joan Miro.

Cruise ships are among the most common venues for this type of scheme. Captive cruise participants are often subjected to art auctions that promise a seemingly classy event and free

champagne. Auction prices are commonly driven artificially high due to false bids by the scheme's co-conspirators.

Collectibles and Memorabilia

Collectibles and household decorative items such as vases, bric-a-brac, and figurines are also commonly hawked by telemarketers. Again, these supposedly valuable objects are nothing more than cheap, shoddy merchandise. War memorabilia is especially popular, particularly items related to the World War II. Documents and keepsakes from any bygone era are on the fraudulent telemarketer's best-seller list. Stamps are sold as rare when they are in fact worthless.

Coins are another prime money-maker for telemarketers. "Certificates of authenticity" and "appraisals" are included with the merchandise to reassure customers, but these documents are usually produced by the sales company or doctored from a legitimate original.

Precious Stones

Gems are generally regarded as items that will not lose their value. Telescammers exploit this mindset by offering "high-quality" gems for wholesale prices. Customers are told they are being offered a special deal due to fluctuations in the market or because their names are on an industry list.

Victims are told that the risk is minimal. By acquiring the stones wholesale, the individual minimizes the investment exposure. The company even offers its own "brokerage" services, which can liquidate the stones at a moment's notice should the investor need the cash back quickly. The stones not only have a grading certificate and appraisal documents, but are also sealed in a plastic wrapper to guarantee that their condition remains flawless. The real purpose of the seal—which victims are told must not be broken if the gems are ever to be offered for sale—is to keep buyers from making a genuine inspection of the article.

Once a victim makes a buy, a company spokesperson calls a second time, saying that if the person buys more stones, his "gemstone portfolio" will be more attractive to prospective buyers and at auctions advertised in company literature. If the victim buys additional items, a company broker will inevitably call with "good news." The brokerage will have found a buyer for the victim's holdings, but before the transaction can go through, the customer must pay some "minor fees." These might be passed off as finders' fees, brokers'

commissions, examination fees, international duties, or taxes. There may be a provision requiring the victim to buy more stones before making the sale.

A variation on the scheme targets those who have already bought gems from telemarketers and whose names are taken from insider lists. The caller claims to be a broker representing an "overseas buyer" ready to purchase the listener's portfolio. But, invariably, the buyer must have a few more stones in the portfolio—which the caller offers to supply—in order to make the sale, and there are fees and commissions to be paid.

Precious Metals

The precious metals market has traditionally been one of wide variances. Prices fluctuate constantly, and even experts have trouble deciding what the next trend will be. Telemarketing operations play on this instability with offerings of gold, silver, and platinum. Once again, victims are told prices will never be this good again and that if they hesitate, they will miss a singular opportunity to make a fortune.

Premium Rate Telephone Numbers

Beginning in the early 1990s, telephone numbers in the United States starting with 976 and 900 prefixes were widely employed for various uses, such as psychic hotlines, phone sex lines, and other dubious enterprises. While these services have fallen out of use in the United States after being supplanted by online- and mobile-phone-related billing mechanisms, they are still used extensively in many countries. By using premium rate telephone numbers, customers can participate in interactive television programming or listen to prerecorded messages from their favorite celebrities. Some callers insist they did not know they were being charged for the service. By using a toll-free number that then links the caller to the per-minute charges, promoters are able to surreptitiously begin charging customers for calls. Toll-free numbers are often used as a front in telemarketing operations to lead consumers to think that a call is free, when in fact they are masking hidden charges. A particularly vicious combination uses a toll-free number to make a presentation about communication services. Once the caller dials in, the interactive voice response service automatically puts a monthly charge, sometimes labeled "voice mail," on the caller's phone bill.

International Calls

Callers believe they are dialing an international number for free information, usually about travel contests, discount fares, or overseas jobs. But the phone numbers, in Guyana and the Caribbean, charge up to $2.30 per minute for a recorded message that runs for 15 minutes.

The promoters get a kickback from the phone company; in one case, 37 cents per minute went to the scammers.

Another international rate scheme finds the victim receiving a call that rings only once. When the victim returns the missed call, he unwittingly dials an international number that results in extraordinarily high charges. As most calling plans now include long distance, the phone numbers appear to be toll-free but are typically located in island nations, such as the 473 area code in Grenada, which are typically dialed in the same manner as a domestic call. These scams were at one time confined to only a few easily avoidable area codes in the Caribbean, such as 809 in the Dominican Republic. However, they have enjoyed more success recently due to the rapid proliferation of new area codes in the region, which has made the immediate recognition of international phone numbers more difficult.

Selling Free Information

Companies involved in this kind of scheme take out ads in newspapers and magazines, or buy spots on talk radio, promising they can locate government jobs, get deals on liquidated equipment, or find student loans. All this information is available cheaply or free to the public, through government offices, on the Internet, and from other sources. One need only know where to look.

Scholarship Services

Maybe the most widely broadcast offering in the information racket is the college scholarship locator service. Whatever information these scam scholarship services do provide is available for little or no cost from legitimate institutions. The perpetrators imply that they have insider connections, or that they actually administer the dispersal of monies, when in reality they merely provide lists of scholarships offered by foundations and universities.

Student Aid Inc., a New York City firm, provides an example. SAI guaranteed students and their parents that they would receive valuable scholarships or grants for a small fee. "In reality," government prosecutors showed, "the defendants almost never obtained scholarship money for consumers." SAI used a common clause in its contracts to keep from paying refunds "requiring students [to] produce letters of rejection from every scholarship on their search list even though the list included scholarships whose deadlines had passed or for which the students did not qualify."

In most cases, information scams sell freely available material. There is also a version that does offer the information for free but adds a charge anyway. The International Call scam promises "free information" on travel contests and discount fares. The information itself does not cost anything, but the call to get it is billed at a high per-minute rate for a 15-minute call.

Charity Fronts

An increasing number of groups calling themselves nonprofit, charitable concerns are not what they appear. Very little or no money goes to the advertised cause. Police and firemen's associations have in some cases lent their names to telemarketing fund drives that only give about 35 percent of their collections to the group. Some boiler room operators claim to call for these groups—or for drives against a disease or underprivileged children—when they are in no way affiliated with the charity.

A twist to this scam is the impersonation of disabled workers by boiler room operators. Fraudsters call victims, claiming to be disabled, and attempt to sell light bulbs and other household products. The merchandise is priced at three times its actual value. The money is, of course, pocketed by the operators.

Door-to-Door Promotions

Sweepstakes promoters using a charity front offer the possibility of new cars and cash prizes to contributors. The raffle approach—tying the number of "chances" to a set amount—helps drive up how much the victim is willing to give. A favored device of phony charities is to send school-age children door-to-door, saying they are raising money for antidrug programs or for a group that takes underprivileged kids on trips. Some of the children repeat what they are told in exchange for a few dollars. Others believe they will receive rewards and free trips when in fact they, too, are being scammed.

Prizes, Sweepstakes, Discount Services

The most common giveaway scam is known as the "1-in-5." A postcard arrives in the mail telling the receiver he has already won a prize. A new luxury vehicle tops the list, along with cash, jewelry, a living room set, and gift certificates. The odds of winning any of the prizes are astronomical. Victims are given items of minimal value or coupons redeemable only for the company's own substandard merchandise.

Winners who call back are often asked to stipulate how they intend to spend their winnings for the company's "records," or for "publicity materials." Then they will be asked to pay a processing fee or to prepay the taxes on their winnings.

Magazine Subscriptions

A productive front for prize hawkers is the magazine subscription service. Prepaid subscription offers extract money from customers through credit cards and bank debits, and then never deliver the publication. In other instances, the processing fees far exceed the actual value of the subscriptions.

Office and Household Supplies

A prevalent office supply scam involves copy machine toner. An invoice for toner is sent to a company. The cons have usually called beforehand, gotten the name of the employee in charge of supplies, and addressed the invoice to that person. Although the office never ordered or received any toner, the con men are relying on poor communication to cover their ruse. The invoice will most likely be sent to the accounting department and paid. If the proper controls are in place at every level of business operations, this scheme should be detected. Too many businesses, however, are vulnerable to this kind of scam.

The caller might get the company's representative to accept a trial or promotional shipping of the product. He might claim to be a supplier for the company or a new salesman from a regular supplier. The product arrives and an invoice follows a couple of weeks later. If the company tries to send the product back, it is returned. To avoid further complications, the company will normally pay the bill just to put an end to the situation.

Any sort of office supply, from paper, to shelving, to cleaning products, can be part of a scam. Medical supplies shipped to doctors' offices and clinics are pushed in a similar fashion. Individual households can be the target of these ploys, as well. Water purifiers are often used in tandem with giveaway offers; the victim buys a filtering device, at an inflated cost, in order to qualify for the giveaway. Pyramid-style operations often use household products and health-related merchandise, such as vitamins or skin cream, as part of their machinations.

Phishing

Phishing is a popular scheme that involves tricking businesses or individuals into providing passwords, account numbers, or other sensitive data by claiming to be from an actual company the victim does business with. A solicitation for information appears to come from

a legitimate business and can occur over the phone (such as a call from the victim's "bank" saying his account has been compromised and requesting PINs, account numbers, or passwords) or via email (which is the most common technique). An individual receives an email that appears to come from eBay, PayPal, or a financial institution. The email states that the customer must immediately log into his account to update his information. The link directs the individual to a fake site that captures his identifying information, such as government identification number and PIN, mother's maiden name, and financial account numbers.

It is crucial for people to recognize the hallmarks and warning signs of phishing so that they don't fall victim to it:

- Phishing occurs mostly by email. The sender of the email pretends to be a legitimate bank, government agency, or retailer and asks the recipient to confirm his personal information for any of these or other made-up reasons: the person's account will be closed if he doesn't give the information, an order has been placed in his name, or his information has been lost because of a computer glitch. Do not ever respond to these emails. Legitimate banks, government agencies, and retailers would not email you for your password or other identifying information.
- Do not click on any link in an email that asks for your personal information. The links included in the emails sent by phishers will take you to a phony website that looks just like the website of the real company or agency. If you followed the instructions, you would enter your personal information, which would go straight into the hands of identity thieves.
- Phishers might say that they are from the fraud departments of popular companies and ask you to verify your information because they suspect you might be a victim of identity theft. Other tactics include the phisher claiming to be from a lottery or sweepstakes commission that requests people's banking information to deposit their "winnings" in their accounts. Again, never disclose any personal information via email.
- Phishing can also happen by phone. Verify the caller's identity and contact his company for legitimacy. Instead of fraudsters sending spam, they might call you and pretend to be from a company or government agency, making the same kinds of false claims and asking for your personal information. If someone contacts you and says that you have been a victim of fraud, verify the person's identity before you provide any personal information. Legitimate credit card issuers and other companies might contact you if there is an unusual pattern indicating that someone else might be using one of your accounts. However, they only ask if you made particular transactions; they don't request

your account number or other personal information. Law enforcement agencies might also contact you if you've been the victim of fraud. To be cautious, ask for the person's name, the name of the agency or company, the telephone number, and the address. Then get the main number and call to find out if the person is legitimate.

- Phishers also target people who list themselves on job search sites. They pretend to be potential employers and ask for your government identification number and other personal information. Before giving anyone your personal information, make sure to verify the person's identity.
- Be suspicious if contacted unexpectedly and asked for your personal information. It is difficult to determine a company's legitimacy by reading an email, going to a website, or talking to someone on the phone. If you are contacted unexpectedly and asked to give out your personal information, a red flag should go up that something is "phishy." Legitimate companies and agencies do not operate this way.
- Act immediately if you've been ensnared by a phisher. If you provided account numbers, PINs, or passwords to a phisher, notify the companies with whom you have the accounts right away.

SMiShing or Tishing

SMiShing is a hybrid of phishing and short message service, commonly known as text messaging. It uses the same approach as phishing but delivers an alarming message via SMS (the protocol used to transmit text messages via mobile devices) instead of email. Criminal activity such as SMiShing can be seen as the prelude to online frauds targeting mobile device users. As these devices continue to evolve, cyber criminals will take advantage of functionalities to obtain information, as well as delivering mobile malware to mobile devices.

Voice Phishing or Vishing

Vishing is a form of phishing attack where emails, for one reason or another, direct recipients to dial a 1-800 number, where an automated recording requests that callers enter personal information using a phone's keypad.

Pharming

Pharming is an attack in which a user is fooled into entering sensitive data (such as a password or credit card number) into a malicious website that impersonates a legitimate website. It is different from phishing in that the attacker does not have to rely on having the user click on a link in the email to direct him to the fake website. Pharming actually exploits a vulnerability in the DNS server software that allows a hacker to acquire the domain name

for a site and redirect the website traffic from a legitimate site to a false one. So even though the user types in the correct website address, the pharming program sends the user to an illegitimate site that appears authentic. Unknowingly, the user is then providing passwords and information directly to the hacker.

Recovery Rooms

Recovery room operations target those who have already lost money to a telemarketing scam. Posing as a consumer advocacy group or a law firm, telemarketers offer victims a chance to recover any funds they might have lost and bring the perpetrators to justice. Once the victim agrees, legal, investigative, and other fees will begin to emerge.

Ponzi and Pyramid Schemes

Definition

A *Ponzi scheme* is generally defined as an illegal business practice in which new investors' money is used to make payments to earlier investors. The investment opportunity is typically presented with the promise of uncommonly high returns. A simple investment scam takes in as much money as possible and then disappears, whereas a Ponzi scheme stays in business by turning some of the money back into the game. A few conspicuous rewards early on will generate interest, the business will grow, and then, if they're smart and lucky, the operators will split.

Everyone involved in promoting the scheme pretends to mount a legitimate organization, but little or no commercial activity takes place. Payoffs are made from the pool of investor funds; the rest is siphoned into operators' pockets. Schemes might run for at least a year. Some Ponzis have flourished for a decade or more.

In accounting terms, money paid to Ponzi investors, described as *income*, is actually *distribution of capital*. It is like giving away the store. Instead of sharing profits, you are sharing cash reserves.

Approaching this crime analytically, we can see into the mechanics of the fraud. Illegal cash is hidden in securities or other financial instruments. Promoters use phony accounts, phony books, and phony names. Successful prosecutions have to uncover these guises and track the

funds. Plus, the inner workings of a Ponzi operation have to be summarized for a jury, whose members are probably not mathematicians or accountants.

Red Flags of Ponzi Schemes

By their very nature, Ponzi schemes are prone to leaving a host of fraud indicators for those unaffected by the investment promoter's dubious claims. Several red flags can help investigators uncover Ponzi schemes:

- *Sounds too good to be true:* If an investment sounds too good to be true, it probably is.
- *Promises of low risk or high rewards:* Promoters of Ponzi schemes typically promise implausibly high or quick returns with little risk. As all legitimate investments include some degree of risk, any guarantee that an investment will perform in a certain way is a clear signal that it might be part of a Ponzi scheme.
- *History of consistent returns:* Any firm that generates remarkably consistent returns regardless of market conditions should raise suspicions.
- *High-pressure sales tactics:* Reputable investment firms and agents do not push potential investors to act immediately, and legitimate investment opportunities are rarely that time sensitive.
- *Pressure to reinvest:* Often, fraudsters keep Ponzi schemes alive by convincing investors to reinvest their profits rather than take a payout.
- *Complex trading strategies:* Legitimate agents should be able to provide clear explanations about their investment strategies. For obvious reasons, Ponzi-scheme boosters purposefully employ complicated strategies that confound unsophisticated investors.
- *Lack of transparency or access:* Secrecy surrounding the operations of a financial company should be an immediate warning sign. Ponzi operators are often unlicensed and their supposed investments are typically unregistered. Additionally, a lack of access to regular statements or an online account should trigger alarm.
- *Lack of a segregation of duties:* Investors should be wary of any financial manager who manages, administers, and retains custody of the fund in question.

Some other red flags to watch out for include investments that are not properly registered, agents with criminal records, unexplained gaps in a promoter's work history, prior customer complaints, regulatory problems, questionable credentials, lack of background information on the company website, and generic contact information such as a Yahoo! email address.

Illegal Pyramid or Ponzi Scheme?

What's the difference between an illegal pyramid scheme and a Ponzi scheme? They both use new investors' money to make payoffs. But they're run very differently by their promoters, and legally they're prosecuted under different laws.

First, we'll distinguish between legal and illegal pyramid schemes. Then we'll show how a Ponzi scheme and an illegal pyramid differ.

Pyramid Schemes, Legal and Illegal

> *Illegal pyramids generate revenue by continually recruiting new members. These operations might offer merchandise or services for sale, but the only significant revenues come from recruitment.*

Some legitimate merchandising companies use a pyramid structure to rank their employee-owners and to determine those people's compensation. But a pyramid structure becomes a pyramid scheme when the company makes its money by recruiting people. Instead of selling a product or service, the group deals primarily in new memberships. Joining the group allows the new member to profit by signing up new members. The process continues until the available pool of new members is drained, which happens sooner than one might think.

Usually, there's a product or a cause that fronts the illegal pyramid scheme as a legitimate enterprise. Promoters sell beeswax supplements, or claim they're working to prevent youth crime. A favorite product front offers "courses" in areas like "investor education" or "self-esteem." These materials usually convey very little pertinent information; in fact, they're nothing more than motivational tracts designed to make the victim a more enthusiastic participant in the pyramid.

In any case, regardless of the product front, an illegal pyramid emphasizes recruiting first and foremost. The product or service takes a back seat to getting new victims signed up.

In most circumstances, courts apply the *70 Percent Rule*. This requires that at least 70 percent of a distributor's profits come from retail sales. Of course, this figure can be hard to verify. Distributors routinely sign falsified compliance statements because if they don't, promoters warn, the authorities will shut the whole thing down and everyone loses.

In the final assessment, legality rests on what the operators emphasize. If the company emphasizes the recruitment of new members over the sales of products, and if the only way to recognize promised riches is through recruitment, then the operation will likely be classified as an illegal pyramid.

What's the Difference Between an Illegal Pyramid and a Ponzi Scheme?

> *Illegal pyramids are promoted as pyramids. Ponzi schemes are promoted as investment opportunities.*

The key element in a Ponzi scheme is that initial investors are paid with subsequent investors' money. There is little or no legitimate commerce.

The same thing occurs in an illegal pyramid. Nobody's selling the beeswax supplements; they're all coaxing new people to put up money. The original members of the pyramid get rich on subsequent investors' money. So, *a pyramid is a Ponzi scheme.*

How about the opposite? Is a Ponzi scheme a pyramid? The distinguishing factor of the illegal pyramid is the continual need for new investors. Each new member recruits two members, who each recruit two, and so forth.

Ponzi schemes, like pyramids, require a steady march of new investor funds to pay dividends. This ever-growing pile of loot might look like a pyramid when graphed. So, in the sense that it requires exponential growth to avoid collapse, *a Ponzi scheme is a pyramid scheme.* The difference between a Ponzi scheme and a pyramid lies in how the operation is promoted.

Illegal pyramids announce themselves as pyramids: They hype levels or stages in their literature. The pyramidal structure helps draw new players, each believing that they will rise through the ranks of the pyramid to become "golden," or "fully vested"—whatever titles the scammers have concocted.

A *Ponzi scheme*, on the other hand, masquerades as some type of investment—in financial instruments, mineral rights, or some other form of speculation. The participants believe they're buying mortgage-backed securities or partial interest in an oil well. They have no idea

they're funneling money into the coffers of manipulative criminals. Certainly no one suggests moving on to the next level of the pyramid, because the pyramid isn't part of the pitch. When an enterprise—Nu-Skin International, for example—promotes itself as an organization with levels or stages, and the only way to rise through the levels is to recruit new members, the promoters are running an illegal pyramid scheme. Before Tim and Melinda Rommel sued Nu-Skin, they were true believers, sprinkling Nu-Skin products across their bathrooms and kitchens, serving Splash, Nu-Skin's answer to Tang, for breakfast every day, and even redecorating their house at the behest of Nu-Skin consultants, all for the purpose of snaring new recruits. The Rommels sued because they were misled about their opportunities inside the organization. They knew all along they were joining a pyramid; they just thought it was a legal one.

When an enterprise promotes an investment opportunity that invests little or none of the participants' money and that uses new investments to make dividend payments, the promoters are running a Ponzi scheme.

Distinguishing between Ponzis and pyramids seems a bit academic. But the differences become significant when perpetrators are brought to justice. To prosecute an illegal pyramid, the enforcement team needs to show that the offenders generated revenue mainly through recruitment—the company's pyramidal structure is an element of the charge. Pyramid schemes are sometimes charged as illegal lotteries because, prosecutors have successfully argued, the participants are totally dependent on the actions of others for any compensation.

In another prosecution strategy, operators are charged with falsely representing potential earnings, since the mathematical limits of the pyramid make the promised $10,000 a month impossible or extremely against the odds. Again, the pyramidal structure itself is an issue in the case.

In summary:

> *If operators make the bulk of participants' earnings dependent on recruiting and emphasize levels and stages in their promotions, we call this an illegal pyramid.*
>
> *If operators claim they're offering an investment opportunity, but conduct little or no commercial activity, we call this a Ponzi scheme.*

Categories of Pyramid Schemes

Pyramid schemes are classified according to the front used in their promotion. The categories are *pure cash* (which includes endless chain schemes and fill-and-split games) and *product fronts* (which includes financial instruments, MLMs, and speculations).

Pure Cash Schemes

There are two general types of pure cash schemes: endless chains and fill-and-split games.

ENDLESS CHAINS

The most outrageous pyramid scams don't bother to conceal their true objective. They don't use services or products to establish their legitimacy. Instead, they use the "chain letter" approach. The recipient of the letter sends a sum of money (the amount varies but isn't usually very large) to the person who mailed him the letter and then passes the letter on to three or four others.

Probability studies have shown that 93 to 95 percent of the players in a pyramid (everyone but those at the earliest initiation) will lose most of their money. Half can expect to lose everything they put in.

Some Internet chains have become known as "administered" pyramid schemes—every exchange in the chain is monitored by a central administrator, who makes sure everybody's playing (and paying) along. The administrator takes a cut of each transaction.

FILL-AND-SPLIT GAMES

The best way to launch a pure cash pyramid is to augment it with gaming elements—some kind of hook to keep players' attention focused on their riches and not how absurd their latest "opportunity" really is. These are sometimes called *fill-and-split games*. A popular version of this approach has been known as "Airplane." Each player buys a seat on a fictitious airplane, paying from $200 to $2,000 a seat, depending on the scale of the game. Initial players help recruit new "passengers" and move up through the ranks of "crew," "copilot," and "pilot." When a flight is fully booked—with something like six passengers, four crew members, a copilot, and a pilot—the plane takes off, the pilots and crew are paid for the flight, and everybody moves up the ranks. Just like a real airline, a plane's investors are constantly looking to fill their seats.

Another variation of the fill-and-split game tries to capitalize on the phenomenal profits yielded over the last several decades in stock markets. Called "Financial Networking," "Market Climb," or another financial-sounding name, these pure-cash pyramids use a business metaphor in their pitch. A typical operation spreads 15 people over four levels. Eight investors buy into the network as "vice-presidents." Above them are four "presidents," just below two "cochairman" positions. At the top, is the "chairman." Every time the eight slots at the bottom are filled (average price $1,500 to $2,000), the pyramid splits. The chairman gets out of the game with a "golden parachute" and everyone moves up the corporate ladder, anxiously scanning for new recruits.

These games are usually predicated on what's become known as affinity fraud. New players are recruited by their affinity with existing participants. People comb religious groups or community associations for fresh leads. Affinities may be racial or cultural. Churches, synagogues, and other religious organizations offer fertile hunting grounds and great cover from promoters—an endorsement from a clergyperson is as good as gold, and law enforcement authorities are often reluctant to meddle in religious affairs. Affinity frauds might also prey on social groups or professional organizations.

Product Fronts

The category of product fronts is subdivided into financial instruments, MLMs, and speculations.

FINANCIAL INSTRUMENTS

Financial instruments—such as stocks, borrower's certificates, currency exchanges, loan scams, and investment pools—are perfect tools for the Ponzi artist. Charles Ponzi's victims in 1920 thought they were investing in postal reply coupons that, Ponzi assured everyone, yielded whopping profits by playing off the exchange rates of international currency. In our own time, as currencies around the world fluctuate from one extreme to the next, the currency exchange still makes an ideal Ponzi front.

A stock market that gains 25 to 30 percent a year (and individual stocks quadrupling, sometimes in a matter of months) encourages the impression that all anyone has to do is put down their money and wait. Unscrupulous promoters like to tout new items like Internet stocks and biotechnology startups, but any product will do. Even in this highly technological age, commodities futures—from soybeans to pork bellies—are still numbered among the most common bait for Ponzi schemes.

Financial instruments are especially effective fronts because most people don't understand how legitimate financial operations take place. When investment analysts are enthused by derivatives of futures contracts, and hedge funds are betting that the market will rise at the same time they are betting it will fall, how is an average investor supposed to understand his options?

MULTILEVEL MARKETING

When most people hear about a pyramid scheme, they think multilevel marketing, or MLM, as it's often abbreviated. These organizations hawk nutrition supplements, household goods, cosmetics, television antennas, insurance, long-distance phone service, and everything from antiques to zinc. Also among the offerings might be copies of *How to Make a Million Dollars in an MLM*. One of the industry's primary money-makers is a string of "training materials" designed to prime the sales force for ever higher feats of ruthless merchandising.

Math remains the great enemy, as well as the primary tool, of MLMs. Promoters draw *matrices* (never pyramids) on a chalkboard and compute what 20 people mailing money to a distributor's house every month would amount to in a year's time. These schemers ignore other aspects of the equation. First, the market for any product outside those owned by large national brands is extremely small. Cashing in on a submarket requires an excess of savvy, finance, and luck, which most MLM-ers lack. Then there is pyramidal mathematics—after a couple of levels, you run out of people willing to hear your spiel (which was already less than 5 percent of any area's population). In fact, between 90 and 95 percent of MLM operations fail in their first two years (compared to an estimated 50 percent failure rate for small businesses in general).

As a general rule, any organization that recruits distributors into a pyramid-style compensation plan, offers big payoffs for recruiting, and spends more time extolling its distributor levels than its product lines is probably illegal.

SPECULATIONS

The term *speculation* describes any investment proposition not covered as financial instruments or MLMs. This includes franchise offerings and business opportunities in general, work-at-home promotions, and investments in areas like real estate or mineral rights. These are traditional investments, except when they're Ponzi schemes.

Franchise scams hawk such opportunities as internet terminals or vending machines. By their nature, such businesses are spread out geographically and don't involve much direct contact with the promoter and the franchise holder.

Work-at-home promotions are also favorite tools of the franchise scammer. Computer technology is a popular front, since countless people really are setting up businesses from their homes. A few early dividend checks, per the Ponzi playbook, are often enough to overcome a client's hesitation and provoke a more sizeable investment. Then the promoters can take their profits and move to another location.

Big-money speculations often base their high-flown claims in the ground beneath our feet. Land and the minerals drawn from it, like gold, coal, and oil, has long been regarded as the ultimate commodity. The ground is the fundament of every human endeavor, so perhaps the land swindle is also the fundament of fraud. Someone, somewhere, it seems, has always been selling flooded lots to homesteaders, salting gold mines with chunks of pyrite, or assuring a rich merchant the new aqueduct will cut across the thousand acres of desert he just bought for a song.

Obviously, a commercial environment that thrives on speculation is highly susceptible to Ponzi fraud. Remember, the Ponzi element in a Ponzi scheme is only a technique—giving back a few dollars to sweeten the pot. Anything that can coax people to part with their money, from emu farms to underwater land developments, can be run as a Ponzi. All the name *Ponzi* really means is that a few marks get paid. This lends a competitive element to an otherwise mundane fraud. Instead of everyone losing, some lucky players do make money.

Speculation frauds don't always start out as cons, but when their rollercoaster dips, many speculators find it too tempting to hang on and ride—they figure they can phony their way through the crisis, and pick up again later. Again, it's math that usually dooms these players. They simply can't make money fast enough to feed the deficits. They need a payoff so big that nothing short of a miracle—or more fraud—will suffice.

Speculators can quickly get caught in a chain reaction, where each fraud demands more fraud. By the time these organizations are shut down, they're spending half of their resources or more just covering up their criminal acts.

Spotting Pyramid Schemes

Almost everyone knows what a pyramid scheme is. People see them exposed on television and read about them constantly in magazines and newspapers. So, if everyone is so well informed about the pyramid, how does it survive?

It could be that familiarity has lulled the public into a false sense of security. Pyramiders have several strong weapons at their disposal:

- They do pay off. Unlike a simple con game in which the fraudster throws the ruse, grabs the cash, and exits, pyramiding builds up the take by paying initial investors. This makes for excellent testimonials. Early players circulate the word and bring in new marks. Initial payoffs also keep early players coming back. Payoffs make the enterprise look legitimate and fuel the expansion process.
- They operate mainly through preexisting affiliations. Community groups, religious organizations, and social clubs all make enticing targets for pyramiders. Any pyramid requires a healthy pool of participants, so a large group already gathered together is ideal. Besides that, pyramiders know how to manipulate the trust that people place in these groups.
- They use ingenuity and false logic in their pitches. The product fronts available for pyramiding are myriad, from bath soap to electronics. Fronts in financial instruments and real estate are especially effective because most people don't understand how those businesses work anyway. Pure cash games find clever metaphors—like a conceptual airplane or a business executives' hierarchy—to make themselves attractive.

Pyramiders of every stripe use a seductive, though false, logic in their pitch: "Everybody has friends and associates; you only have to sign up three or four people below you." Of course, the laws of mathematics spell doom to this logic. There simply aren't enough players to keep even a small pyramid running. Three people, each finding three people, will quickly play out their available friends and associates—if not mathematically, then socially. There's also a reasonable limit on how quickly money can grow.

The pyramid, then, is built to overcome people's most common misgivings about investing. Promoters offer far more than an "undertaking of great advantage, nobody to know what it is." They are very specific in their prospectus. The offer sounds good and (within its own logic) makes sense. The "opportunity" is usually pitched by someone familiar to the victim, or at least by someone with an affinity the victim trusts. Most important, the pyramid does return people's money, with the incredible profits attached as promised.

Speed is another potent weapon in the pyramid arsenal. Cons say, "Get in now, or regret it forever." They don't have time—because of market demand or commitments elsewhere—for the person to check out the deal. That's because a moderate amount of due diligence research will expose the deal as a scheme.

Identity Theft

Identity theft is a common type of fraud that is non-discriminatory in nature. Anyone can be targeted; the victim might be a college student, a retiree, a schoolteacher, or a successful attorney. Even businesses are susceptible to identity theft.

Although there is no universal definition of identity theft, most law enforcement organizations use a definition similar to the following:

> *Identity theft and fraud are crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.*

Personal identification data includes name, address, government identification number, date of birth, mother's maiden name, or other identifying information. The perpetrator exploits this information by opening bank or credit card accounts, taking over existing accounts, obtaining loans, leasing cars or apartments, or applying for wireless telephone and utility services in the victim's name without his knowledge.

Technological advancements that facilitate the electronic transfer of personal information and the transmission of financial transactions have greatly contributed to the recent increase in occurrences of identity theft. As such technologies continue to develop, this type of fraud will likely remain a serious problem that affects many people.

Business Identity Theft

Business identity theft, or the misappropriation of an organization's sensitive identifying information necessary to imitate the business's identity for illicit purposes, has become a growing problem. Criminals obtain businesses' identifying information through various means, such as searching for them online, examining filings with regulators, reviewing tax forms, phishing, or social engineering.

Numerous schemes related to business identity theft have been reported, ranging from fraudulent credit card applications to complex multi-million-dollar bogus stock sales. In some cases, long-dormant businesses have been fraudulently reinstated and used for nefarious purposes.

Owners of small businesses are particularly at risk for business identity theft. This segment of the business community possesses the lines of credit, capital, and other features desired by fraudsters, while often lacking the resources and technology needed to properly defend against identity theft. Smaller companies and individually owned businesses often rely heavily on the owner's personal credit, making the impact of business identity theft even more destructive. Furthermore, small businesses might be especially wary of revealing identity theft out of fear that consumers will take their business to a larger company that ostensibly offers an increased level of data security.

Profile of the Fraudster

Unlike some fraudsters who steal as a result of a perceived need, most identity thieves make a living stealing identities for profit or, at the very least, to supplement their incomes generously. Although he can be an employee, friend, or relative, the fraudster usually falls into one or more of the following profiles:

- Been convicted, served time in prison, wishes to conceal his identity
- Been convicted, served time in prison, and is looking for a "safer" way to commit a crime and stay out of prison
- College student looking for an "easy" way to work his way through school
- Landlord
- Rental car agent
- Undocumented immigrant needing an identity
- Illegal telemarketer

Common Ways of Obtaining Information

While an individual might think that he is careful with his personal information, in reality, a lot of information can be easily found and acquired by identity thieves without him even realizing it. An innocent inquiry for the most basic of information, such as verifying an address or mother's maiden name for a banker's files, can be the start of a financial nightmare. The most common ways information is obtained are:

- Sorting through discarded trash
- Shoulder surfing

- Searching through coworkers' desk drawers
- Stealing incoming or outgoing mail
- Using an accomplice within the organization
- Soliciting identifiers through false job application schemes
- Checking utility companies, health clubs, and schools
- Examining certifications and licenses placed on workplace walls
- Using pretext, ruse, or gag calls
- Looking at rental and loan applications
- Consulting public records
- Using the Internet

Sorting Through Discarded Trash

Most people do not destroy their personal financial data; they simply throw it away with the rest of their trash. Solicitations for pre-approved credit cards are some of the most valuable pieces of trash that an identity thief can steal. Additionally, "dumpster diving," as it is more popularly known, can yield checks, credit card and bank statements, or other records that bear a person's name, address, and telephone number. In addition to targeting an individual's trash, dumpster divers target the trash at banks, insurance companies, hospitals, and other businesses—locations that an individual has no control over.

Shoulder Surfing

Shoulder surfing is another popular way that the identity thief obtains information. The person watches from a nearby location and listens to someone's telephone conversation or watches the numbers being punched for a calling card or credit card, thus obtaining enough information to use or procure a credit card. Identity thieves also watch potential victims as they fill out bank deposit slips, thus getting account information.

Searching Through Coworkers' Desk Drawers

When people leave for a break, go to lunch, or take vacation or sick leave, many, if not most, do not lock up their desks or offices. Many people also leave personal items in their desk drawers—such as bank statements and monthly credit card statements—all of which have useful information for an identity thief.

Stealing Incoming or Outgoing Mail

Stealing both incoming and outgoing mail provides useful information to the fraudster. Outgoing checks left for the mail carrier to pick up provide bank account numbers and other information that can be used for illegal purposes.

EXAMPLE

Using just a driver's license number and bank account number, a thief was able to withdraw more than $30,000 from a security guard's checking account. In this case, the thief used the drive-through at the security guard's bank to deposit a series of stolen money orders and simultaneously make large withdrawals.

Using an Accomplice Within the Organization

Sometimes the identity thief is able to compromise someone within an organization and obtain enough information so that credit can be obtained. It might be a bank employee who has access to government identification numbers and bank balances, or an insurance clerk who has access to personal information such as name, address, government identification numbers, and medical information—all useful when assuming someone's identity.

Soliciting Identifiers Through False Job Application Schemes

Having an individual fill out a job application might also be a source of information to identity thieves. People believe that they are filling out a job application, when in reality they are only supplying personal information to a thief.

Utility Companies, Health Clubs, and Schools

Utility companies, health clubs, and school records all carry identifiers that a fraudster can use to steal someone's identity. Government identification numbers, such as Social Security numbers, are used on many applications and are instrumental in obtaining other information.

Certifications, Diplomas, Licenses Placed On Workplace Walls

Something as innocent as a diploma, professional certification, or license can be the identifying information that a fraudster uses to obtain a false identity. In the case of a professional license, some states require that it be displayed in a prominent place. Consequently, information such as the name, address, and license number is readily available to the thief.

Using Pretext, Ruse, or Gag Calls

Using pretext, ruse, or gag calls claiming to be a person to whom personal information would normally be released is common in an identity theft. Since there is no way to verify the person on the end of a phone line with photo identification, having only a small amount of information can yield the additional data the fraudster seeks.

Pretexting is the act of impersonating someone else or making false or misleading statements to persuade a target to release information or perform some action. Pretexting can occur in-person, over the phone, or through some other form of communication.

Identity thieves often engage in pretexting by posing as the owner of a targeted account. As customer accounts are typically secured by a password, information thieves are adept at distracting or manipulating customer service agents during the security verification phase of a pretexting incident.

To make matters worse, in the event that an account password is unknown, many organizations employ insufficiently difficult backup security procedures, such as requesting a government identification number, date of birth, or mother's maiden name, any of which are easily obtainable for the sufficiently motivated identity thief.

Identity thieves might also pretend to be a person of authority, a member of tech support, someone who has legitimate access to the target's network, an individual who needs help, a government employee, and so on.

For example, a number of individuals have reported being called by people claiming to be court personnel. The caller states that there is an outstanding warrant for the individual due to unpaid tickets or failure to appear for jury duty. When the individual protests his innocence, the caller says that it must be a mistake, and asks the individual to provide his driver's license number, government identification number, and birth date so that the caller can confirm that a mistake has been made. The caller now has all the information needed to steal the individual's identity.

Rental and Loan Applications

Almost without exception, rental and loan applications yield enough information that can be used to establish a false identity. An applicant's name, government identification number, previous address(es), employment history, telephone numbers, and credit history are

required to complete the application. Once the thief obtains that information, it is usually quite easy to establish an identity.

Public Records

Public records yield a wealth of personal data for the identity thief. Real estate records, tax liens, licenses, litigation records, and, in some areas, driver's license numbers all reveal enough information that can be used to steal a person's identity or at least provide a start for the fraudster.

The Internet

The Internet offers many opportunities to the identity thief. It has made much information available to more people at a small cost. It has also been an attractive place for identity thieves to find their victims. Once you have logged on, information you thought was private might now be traced by anyone who is interested in finding personal information about you. Identifying information such as passwords, credit card numbers, and, in some cases, banking information has been made available via the Internet. Spam, or unsolicited email, is frequently responded to by many people who are unaware that the sole purpose of the email is to obtain personal information.

EXAMPLE

A woman was accused of trying to get a $25,000 loan through a bank using personal information she found on the Internet. The victim, a college professor, called law enforcement when the bank sent the completed application to her home rather than to the home of the accused. The same woman reportedly obtained a credit card under another professor's name and ran up almost $3,000 in charges.

In addition, some database companies sell information—your personal information—online to persons or organizations that you might not want to have that information, thus increasing the chance for fraud and abuse. For example, information you provide by responding to a questionnaire online might be collected and sold to insurance and drug companies without your knowledge. The same can be true when applying for a low-interest credit card or consumer loans. Do you know who is actually receiving the information that you provide online? There is no physical address to check out in most cases.

The Internet is also a source for "information brokering." For a fee, information brokers will reveal the most personal aspects of your life—from financial information to medical

information. For a nominal search fee, they will disclose everything from unpublished mobile telephone numbers to the location of your safe deposit box. While much of the information provided can be found in public records or private databases, some of it is obtained illegally.

Tracking Down the Thief

There are many ways that the fraud examiner can track down an identity thief. Some require the assistance of law enforcement, while others do not. Examples of techniques that have been successfully used to catch an identity thief are:

- Establish surveillance of the address in question.
- Have overnight delivery services "flag" the address in question.
- Obtain a subpoena or court order for the telephone records for the telephone(s) being used by the perpetrator.
- Contact credit bureaus and have them "flag" the true account holder's file.
- Obtain videos from retailers showing the perpetrator making purchases using the victim's identity.
- Obtain a copy of the perpetrator's picture on the fictitious driver's license.
- Track down addresses and telephone numbers that do not belong to the victim but show up in the person's file.
- Have the victim notify the fraud examiner when further breaches occur.
- Report the fraud to law enforcement.

Preventing False Identity Fraud

While identity theft might seem to be an inevitable consequence of modern technology and participation in the global economy, there are ways to reduce the chances of being victimized. Furthermore, if a person's identity is stolen, there are many steps that can be taken to minimize the crime's impact.

Consumer Protection Measures

How do you protect yourself and your clients from identity theft? Some useful methods are:

- Before providing personal information, make sure the individual or business requesting it has a valid reason for requiring the information.
- Never write your credit card numbers or government identification number on checks or on the outside of envelopes.
- Don't give account numbers over the telephone or to persons/companies with which you are not familiar.

- Don't use mobile phones, cordless phones, unsecured Wi-Fi, or email to transmit financial or private personal information.
- Keep all financial documents in a secure place.
- If you have your driver's license information pre-printed on your checks, shred canceled checks before discarding them.
- Check your financial information regularly, looking for what should and shouldn't be there.
- Obtain a copy of your credit report on a regular basis.
- Shred pre-approved credit applications.
- Have yourself taken off of pre-screened lists.
- Mail bills from the post office or your business location.
- Consider having your name and telephone number removed from the telephone directory or having the address removed.
- Don't provide personal information over the telephone unless you initiated the call and know with whom you are speaking.
- If telemarketing companies call, tell them that you want to be on their "do-not-call" list.
- Keep your birth certificate in a safe place.
- Choose passwords that are difficult to figure out, and use different passwords for all accounts.
- Change passwords and PIN codes often.
- Don't put your government identification number on any document that you are not legally required to.
- Shred any papers with financial information and identifiers rather than simply throwing them in the trash.

In addition, insurance companies are now offering insurance for identity theft. For an annual fee, the policy typically covers the cost of clearing the policyholder's name and correcting his financial records, including legal expenses, loan re-application fees, telephone and certified mailing charges, notary expenses, and lost wages, for the time it takes to deal with the fraud.

What To Do If Your Identity Is Stolen

- Start keeping detailed records.
- File a police report with your local law enforcement agency and keep a copy of that report. Many banks and credit agencies require such a report before they will acknowledge that a theft has occurred.

- If your wallet or purse is stolen, immediately cancel your credit and debit cards and get replacements.
- Put a "stop payment" on all lost or stolen checks.
- Report unauthorized charges and accounts to the appropriate credit issuers and credit bureaus immediately by phone and in writing. Change account numbers or close all accounts that are affected by the fraudulent activity.
- Check for and repair further breaches of your identity.
- Notify law enforcement agencies (e.g., Federal Trade Commission or Federal Bureau of Investigation in the United States).
- Contact the primary credit reporting bureaus to have a security alert or freeze placed on your credit report, and request a copy of your credit report and review it for unauthorized account activity.

COMPUTER AND INTERNET FRAUD

Computer systems continue to improve rapidly. They are more powerful, smaller, cheaper, and more user-friendly. As they have advanced, computers have proliferated in our society, our businesses, and our personal lives. Modern businesses and governments depend on computer systems to support their operations, from personnel to financial management and everything in between.

Computers have become integral to business and government processes, and without them, most of today's businesses and government operations would cease to function. Imagine trying to manually process tax returns, maintain accounting records, conduct audits, compile budgets, build automobiles, build weapons systems, or check law enforcement files without the aid of computers.

The proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals depend on computers as necessary tools, so, too, do criminals. Computer crimes and frauds are increasing and will no doubt continue to increase as more computers are networked internationally, thus giving global access to computer criminals.

While there is no truly accurate way to determine how many organizations and individuals are victimized by computer and internet fraud, surveys can serve as a gauge and provide an insight into the extent of the problem.

According to the Identity Theft Resource Center (ITRC), during 2014, there were at least 783 data breaches, and since 2005, more than 675 million records have been exposed.[1]

The following results were derived from the *2014 US State of Cybercrime Survey*, conducted by PricewaterhouseCooper (PwC):[2]

- *During 2014, a security event was detected by 77 percent of survey respondents.*

[1] ITRC, "Identity Theft Resource Center Breach Report Hits Record High in 2014," www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

[2] PwC, *2014 US State of Cybercrime Survey*, www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.

- Of the respondents who detected a security event, 26 percent could not identify the source of the attack.
- Cybersecurity threats appear increasingly more threatening, with 59 percent of respondents stating that they were more concerned about threats this year than in the past.
- Of the U.S. executives surveyed, 69 percent are worried that cyber threats will impact business growth.

Unlike traditional fraud cases, computer fraud cases can be difficult for the fraud examiner because they:

- Lack a traditional paper audit trail.
- Require an understanding of the technology used to commit the crime.
- Usually require an understanding of the technology of the victim computer.
- Typically require the use of one or more specialists to assist the fraud examiner, even when the fraud examiner is computer savvy.

In the commission of computer fraud, computers can be the target of the scheme, the tool used to execute the scheme, or—as is often the case—both.

Computer Fraud

While there are a number of possible definitions for computer fraud, it can be summed up into the following broad definition:

> *Computer-aided activity involving a deliberate misrepresentation of fact or alteration of data to obtain or receive something of value that causes a financial loss to some person or organization.*

The distinguishing characteristic of computer fraud is that the perpetrator accesses or uses a computer with the intent to execute a fraudulent scheme. However, the definition above provides a broad scope for actions that constitute computer fraud and serves to encompass new schemes resulting from developments in technology. This is important because in some situations, employees have used company computers to further criminal acts that do not fall within the standard legal definition of fraud. For example, employees could use their company's computers to run an illegal gambling operation or to compose and send (via email) death threats. Although such incidents might not cause direct financial harm to the

company, they could raise potential liability questions and should be addressed by the company's computer-use policy and security program.

Computer Hacking

Hacking refers to the use of technology to gain unauthorized access to sensitive information on a computer system.

The desire to gain unauthorized access to computer systems can be prompted by several motives, from simple curiosity—as exemplified by many hackers—to computer sabotage or espionage. Intentional and unjustified access by a person not authorized by the owners or operators of a system might often constitute criminal behavior. Unauthorized access creates the opportunity to cause additional unintended damage to data, system crashes, or impediments to legitimate system users. Often, however, hacking is motivated by profit.

There are several types of hackers. Black-hat hackers are malicious hackers who infiltrate computer systems for criminal purposes. Conversely, white-hat hackers are well-intentioned hackers who are hired to identify weaknesses in an organization's network before they are exploited by malicious hackers. Hacktivists are politically motivated hackers; they commit cybercrimes, including data breaches, to gain publicity, earn public support, gather new members, embarrass their targets, and so on.

Hackers use various ways to gain unauthorized access to computer systems. Often, unauthorized access is accomplished from a remote location using one of several means. The perpetrator might be able to take advantage of lax security measures to gain access or might find loopholes in existing security measures or system procedures.

Frequently, attackers gain unauthorized access by impersonating legitimate system users; this is especially common in systems where users employ common passwords or maintenance passwords found in the system itself.

But, the most direct way of gaining access to a computer is to use someone else's password or generate (without authorization) a new password. Passwords are supposed to keep computers safe, but most passwords are created by users, who tend to choose weak passwords, use passwords that follow certain patterns, and use the same password for multiple accounts. Consequently, most passwords are not secure.

People usually pick something familiar and easy as their password. For example, a deep-sea fisherman might use *marlin*, and a theater aficionado might use *Broadway*. If the attacker knows or can learn something about his target, cracking the password becomes even easier. That fisherman, for example, probably has a huge marlin mounted on his wall. It might be located directly in his line of sight as he logs on each morning.

Moreover, some attackers use rogue software applications to penetrate a system, while others trick unsuspecting users into downloading harmful programs. These programs and applications operate in the background of the infected computer and can disable security settings and capture information that is sent back to them.

Methods Used to Gain Unauthorized Access

Some common methods for gaining unauthorized access are discussed below.

Social Engineering

Social engineering is a method for gaining unauthorized access to a computer system in which the attacker deceives victims into disclosing personal information or convinces them to commit acts that facilitate the attacker's intended scheme.

Often, social engineering schemes attack companies, and when carrying out these attacks, the attacker tricks one of the target company's employees into revealing information. The hacker might assume a number of different guises to accomplish this deception. He might pose as a new or temporary worker and ask IT employees for a password so that he can begin work. Alternatively, he might pose as someone in a position of authority and intimidate employees into revealing confidential information.

Deception, however, is not always required. In large corporations, attackers can take advantage of certain anonymity among employees. By donning office attire, they can blend into the crowd and peruse the premises, providing them with an opportunity to obtain a password written down at an employee's desk.

To prepare for social engineering schemes, the attacker might search a company's dumpster for relevant documents, such as internal telephone directories and correspondence.

Reverse Social Engineering

In most social engineering scams, the attacker approaches the computer user, pretending that he needs help; however, in reverse social engineering schemes, the attacker gets the user to make the contact. In these schemes, the attacker disguises himself as a technical assistant or someone from whom the user needs help (a need often created by the attacker through sabotage beforehand). It is the reverse of social engineering—the user asks the attacker for help.

Password Cracking

Password cracking is an automated process by which an attacker attempts to guess a system user's most likely passwords. A password cracker typically exploits users who create personal, easy-to-figure-out passwords such as their name, their children's or spouse's name, their nickname, the name of a pet, and so forth. Fraudsters sometimes obtain this type of information with fake surveys, fake prizes, or some other type of social engineering.

Altering the Way a System Generates Passwords

Not all passwords are supplied by users. Some passwords are generated by a computer system's randomizer function. For example, many Internet service providers (ISPs) give first-time users a randomly generated password (and sometimes a random username as well) that gets the person online. Then the users change the log-on information to fit their own preferences.

By learning how a certain system's randomizer works, someone can attack a system by generating valid passwords or altering how the system generates passwords. For example, with some tinkering, the randomizer can be set to give every new user the same, seemingly random, password: EVBDCL8. But that will not work for long. It is better to have the machine make a password built off some information about the user, which is publicly available. Using a relatively simple set of algorithms, an attacker can convert a username, such as "halbfish" into an obscure looking string like "rueavzhr." (Letters are read as numbers by computers speaking ASCII code, so the algorithms use sine values to convert the ASCII values into a new set of numbers.)

Phishing

Phishing schemes occur when a fraudster manipulates victims into providing sensitive information by falsely claiming to be from an actual business, bank, Internet service provider (ISP), or other entity with which the target does business.

In this type of scam, phishers typically use emails to direct Internet users to websites that look like legitimate e-commerce sites, such as online banks, retailers, or government agencies. Phishers actually control these sites and use them to steal sensitive information, such as bank account details and passwords.

To aid in preventing phishing emails, computers should be armed with spam filters, antivirus and antispyware software, and a firewall. They should also be kept up to date. A spam filter can help reduce the number of phishing emails received. Antivirus software, which scans incoming messages for troublesome files, and antispyware software, which looks for programs that have been installed on a computer and tracks a user's online activities without his knowledge, can protect users against pharming and other phishing techniques that fraudsters use.

Additionally, to prevent identity theft through phishing emails, computer users should delete unsolicited emails from banks, credit unions, investment firms, and government agencies with which they do not have an established relationship. If the recipient does have an existing relationship with the supposed originator of the email, the user should call the organization to confirm whether the email is legitimate before taking any further action.

Additionally, there are various types of phishing schemes, including:

- Spear phishing
- Catphishing
- Vishing
- SMiShing or tishing
- Rock phishing
- Pharming

SPEAR PHISHING

Spear phishing is a targeted attack generally focused on a corporate entity. The ruse is meant to fool the corporate employee into believing that the phishing email originated not from a bank or financial institution, but from his own IT or HR department. The goal is to obtain the employee's username and password to access the corporate network.

CATPHISHING

Catphishing involves the creation of a fictitious online persona for the purpose of luring victims into emotional relationships under false pretenses. The fraudster will typically

fabricate multiple fake social media accounts and profiles for dating websites featuring photographs of someone other than himself. The catphisher's ultimate goal might be to ask for money, obtain sensitive information, or embarrass the target.

VISHING

Voice phishing, or *vishing,* is the act of leveraging Voice over Internet Protocol (VoIP) in using the telephone system to falsely claim to be a legitimate enterprise in an attempt to scam users (both consumers and businesses) into disclosing personal information. Government and financial institutions, as well as online auctions and their payment services, can be targets of voice phishing.

A vishing scheme is generally transmitted as an incoming recorded telephone message that uses a spoofed (fraudulent) caller ID matching the identity of a misrepresented organization. The message uses an urgent pretext to direct unsuspecting users to another telephone number. The victim is invited to punch his personal information on his telephone keypad. The criminals capture the key tones and convert them back to a numerical format.

There are several types of information at risk from vishing, including payment card information (numbers, expiration dates, and the last three digits printed on the signature panel), PIN (personal identification number), government identification number, date of birth, bank account numbers, and passport number.

Security experts have seen another variation of vishing where the criminals leave a voice mail message or make telephone calls directing people to the bogus phone number. With Voice over Internet Protocol (VoIP) and other Internet-based telephone technology, criminals can make calls inexpensively and can mask their identity, location, and even make it look like they are calling from a legitimate company on caller displays.

Some potential uses of the personal information gathered through vishing schemes includes control of the victim's financial accounts; opening new bank accounts; transferring bank balances; applying for loans, credit cards, and other goods/services; making luxury purchases; hiding criminal activities; receiving government benefits; and obtaining a passport.

SMISHING OR TISHING

SMiShing is a hybrid of phishing and short message service (text messaging). These schemes use text messages or other short message systems to conduct phishing activities. That is, in SMiShing schemes, the attacker uses text messages or other short message systems to dupe an individual or business into providing sensitive data by falsely claiming to be from an actual business, bank, ISP, or other entity with which the target does business.

Criminal activity such as SMiShing can be seen as the prelude to online frauds targeting mobile device users. As these devices continue to evolve, cyber criminals will take advantage of functionalities to obtain information, as well as to deliver mobile malware to mobile devices.

ROCK PHISHING

Rock phishers use botnets to send massive amounts of phishing emails to huge volumes of Internet users. The emails contain a message from a financial institution, enticing users to click on a fraudulent URL. There is some indication that rock phishers cycle through multiple email lists and attempt to reach the Internet users most likely to use the brands that they are targeting.

Unlike phishers who compromise a Web server and install a phishing site, rock phishers implement an elaborate process whereby multiple domain names are registered at multiple registrars—often with less-known country-code-based top-level domains. Multiple DNS (domain name system) servers are also set up, which provide names to IP services for the pool of domain names. The IP addresses used—and there might be more than 100 at a time—point to multiple compromised servers that simply forward Web connections to the real phish sites. These proxy servers typically handle connections for multiple targets at a time.

One of the best ways to combat rock phishing is to implement a sender policy framework (SPF) or Domain Keys on one's email system. More and more, ISPs are rejecting, or at least sending to the spam folder, email that fails SPF or Domain Key authentication.

PHARMING

Pharming is a type of phishing attack in which a user is fooled into entering sensitive data (such as a password or credit card number) into a malicious website that imitates a legitimate website. It is different from phishing in that in pharming schemes, the attacker does not

have to rely on having the user click on a link in the email to direct him to the malicious website that is impersonating a legitimate website. Pharming actually exploits a vulnerability in the domain name system (DNS) server software that allows a hacker to acquire the domain name for a site and redirect the website traffic from a legitimate site to a false one. So even though the user types in the correct website address, the pharming program sends the user to an imitation website. Unknowingly, the user is then providing passwords and information directly to the hacker.

Browsing

Browsing is one of the simplest ways to attack a system. It involves searching through large quantities of available data to find sensitive information. Browsing, for example, can involve searching physical memory for the system password table, or scanning files in disk storage for confidential information. The best way to defend against browsing attacks is to establish a strong access control system.

Keystroke Logging

Keystroke logging is the process of monitoring and tracking the keys pressed on a keyboard. Keyloggers can be based on software or hardware, and they can record every action a person performs on a computer (e.g., every cut, copy, move, and delete command). Both hardware and software keyloggers save the logged keystrokes to a file that the attacker can retrieve later.

Software keyloggers are generally delivered like Trojans and act in a similar way. Once installed, the software records the keystrokes, letter by letter, that a user makes on a computer keyboard. These programs are designed to record usernames and passwords for the victim's computer and other secured Internet sites, such as banking and online auction accounts.

Hardware keyloggers are small devices that attach to the signal path between the target's keyboard and computer. They can be attached between the computer and the keyboard cable, to other parts of the computer's hardware, or inside the keyboard. Most users would not distinguish the device from any of the other wires and plugs attached to a machine. Like software loggers, hardware loggers record keystrokes and either transmit the data or store it for later retrieval. Although hardware loggers require the attacker to have physical access to the target machine, this is often easily accomplished in a corporate environment.

Backdoors

Backdoors let attackers bypass a system's security through the use of undocumented operating system and network functions.

Remote Access Trojans

A *remote access Trojan* (RAT) is a type of malicious software that provides the attacker with complete control of the target's system. These programs can be delivered in a number of different ways, including via program patches, electronic birthday greetings, and so on. Additionally, victims might unknowingly and easily transmit them to other victims. Once the RAT is in operation, the fraudster can usually access everything on the victim's machine, stealing any data deemed valuable or turning the victim's computer into a server for at-will access or for use in a botnet.

Packet Sniffing

Packet sniffers are computer programs that monitor traffic on areas of a network and search for packets of data as they pass through the network. When a message is transmitted across the Internet, for example, it flows through many computer nodes as it makes its way to its final destination. Sniffing programs can be embedded in nodes so that they read all the packets of information that pass through those nodes, looking for passwords to help the hacker gain access to a restricted system.

When a user logs on to an Internet service provider, he sometimes has to type in a username and a password. Most sniffing programs collect the first portion (128 bytes or more) of each network connection being monitored. (This is where the username and password are most likely to be found.) Items like usernames and passwords are then sniffed out of the collected information.

Trapdoors

A *trapdoor* is a secret entry point into a program that allows someone who is aware of the trapdoor to gain access without going through the usual security access procedures.

HTTP Exploits

The World Wide Web is a graphical interface to Internet resources. It uses a hypertext transfer protocol, known as HTTP, to transfer hypertext documents across an array of computer systems.

HTTP exploits involve using Internet server applications to perform malicious activities. These attacks are common because firewalls typically block most Internet traffic to keep it away from corporate servers, but firewalls almost always allow HTTP traffic, which is used for unhindered browsing. Thus, HTTP exploits provide attackers with a direct line to the target's server. If the attacker can coerce the server into performing malicious activities, he will be able to access resources that would otherwise be unavailable.

Due to the inherent vulnerability of the HTTP standard, a migration to a far more secure standard known as Hypertext Transfer Protocol Secure (HTTPS) has occurred in recent years. HTTPS uses either the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol to allow encrypted communication between a website and its associated Web server, thus preventing many of the attacks associated with HTTP. The stark security difference between the two standards has led Google and other search engines to prioritize HTTPS sites over HTTP sites in search results.

Spoofing

Spoofing refers to the process whereby a person or program masquerades as another to obtain unauthorized access to a targeted system. There are several types of spoofing attacks, including:

- *IP spoofing*: In this technique, the attacker mimics another system's IP address to access the target machine without authentication. By doing this, the intruder can send commands to the server under the disguised IP source addresses, making it difficult or impossible to trace the actual source of the messages.
- *ARP spoofing*: In this technique, the attacker sends fake address resolution protocol (ARP), which basically translates IP addresses into Ethernet or MAC addresses, to associate his MAC address with the IP address of another node. As a result, any traffic meant for that IP address would be misdirected to the attacker.
- *DNS spoofing*: The Domain Name System (DNS) tracks domain names and translates them into their numerical equivalent so that computers can understand the address and locate the relevant computer. DNS spoofing involves making a DNS entry point to an IP address other than the one to which it is supposed to point.
- *Email spoofing*: Email spoofing involves misrepresenting parts of the email header, such as the sender address, to make it look like the email came from a different source.

Shoulder Surfing

In this method, the attacker hides near the target and obtains sensitive information by listening to telephone conversation, watching the target enter credit card numbers or fill out bank deposit slips, and so forth.

Rummaging Through Offices

Because employees often leave important information in and around their desks when they leave their office to take a break, lunch, or vacation, many attackers obtain information by rummaging through employees' workstations.

Using an Accomplice

Sometimes the attacker is able to compromise someone within an organization and obtain enough information to gain unauthorized access into a system. Furthermore, criminals have been known to offer money to company employees in exchange for network usernames and passwords.

Discarded Media Drives

Fraudsters commonly obtain important information on improperly discarded media drives, copiers, printers, and other multifunction machines. The data stored on a computer system, hard drive, or external storage device are an ideal source for thieves wanting to commit computer and Internet fraud. And because it is possible to recover deleted data, many attackers search for sensitive information on second-hand drives they purchased online or obtained from some other source.

For this reason, when discarding or selling a used media drive, users must ensure that the drives are scrubbed clean to make certain that the drives contain no residual data.

Like computers, some copiers, printers, and other multifunction machines have internal hard drives that store sensitive data, and therefore, the hard drives on these machines also must be scrubbed before sale or disposal.

Piggybacking

Piggybacking is a method used to gain access to restricted areas, including computer systems, in which the attacker exploits the access capability of another person. Unlike most other methods of attack, piggybacking can be done to gain physical or electronic access.

Physical access via piggybacking involves gaining access to an area that is secured by locked doors, and it occurs when an attacker exploits a false association with another person who has legitimate access to the area. Examples of piggybacking to gain physical access into a restricted area would include:

- Following behind an individual who has been cleared for access into the restricted area
- Tricking an authorized individual into believing the piggybacker is authorized and convincing the individual to agree to allow the piggybacker to tag along into the restricted area
- Surreptitiously following behind an individual who has been cleared for access into a restricted area, giving the appearance of being legitimately escorted
- Pretending to be a member of a large crowd authorized to enter a restricted area

Electronic piggybacking occurs when an attacker gains access to an electronic system by exploiting the access capability of another person with legitimate access. One type of electronic piggybacking occurs when the attacker takes advantage of a legitimate computer user's active session when the user did not properly terminate the session, the user's logoff is unsuccessful, or the user attends to other business while still logged on.

Scavenging and Dumpster Diving

Fraudsters employ a variety of techniques to obtain the information that can be used to gain unauthorized access to systems, but such information can be obtained simply by scavenging or dumpster diving for items with sensitive information (e.g., credit card receipts; bank statements; or other sensitive records that bear an individual's name, address, or telephone number). Scavenging involves obtaining information left around a computer system, in the computer room trashcans, and so on. Dumpster diving refers to gleaning sensitive information from trash receptacles and dumpsters.

Data Manipulation and Destruction

Data manipulation refers to the use or manipulation of a computer to perpetrate a crime, and *data destruction* involves the unauthorized modification, suppression, or erasure of computer data or computer functions, with the intent to alter or hinder the normal functions of the targeted system.

Data manipulation and destruction involves either direct or covert unauthorized access to a computer system by the introduction of malicious software such as viruses, worms, or logic bombs.

This section describes some of the methods used to destroy and manipulate data, including:

- Malware
- Salami technique
- Fraud by input manipulation
- Data leakage
- Wire tapping
- Buffer overflow exploits
- Privilege escalation exploits

Malware

Malware is an umbrella term for any kind of malicious software, including viruses, worms, Trojans, spyware, and ransomware. Often, the term is used interchangeably with *virus,* which is frequently used somewhat inaccurately to cover the same types of threats.

Malware uses popular communication tools to spread, using worms sent through email and instant messages, Trojan horses dropped from websites, and virus-infected files downloaded from peer-to-peer connections. Malware also exploits existing vulnerabilities on systems, often making its entry imperceptible. Malware is discussed in more detail below.

Salami Technique

The *salami technique* is a type of fraud where the perpetrator steals a substantial amount of money by "slicing" off "thin" amounts of cash repeatedly over time. To carry out these schemes, the perpetrator (usually a computer programmer) executes an unauthorized program that repeatedly steals small, nearly unnoticeable amounts of assets from a large number of sources without obviously reducing the whole, and then transfers them into another account. By skimming funds in extremely small quantities, this technique seeks to bypass internal controls and escape detection. For example, in most banking systems, the amount of interest to be credited to an account is typically rounded off. A fraudster might set up the system so that instead of rounding off the number, that fraction of it is credited to a special account that he owns.

Fraud by Input Manipulation

Fraud by input manipulation, often referred to as *data diddling,* occurs when false or misleading information is entered into a system to achieve a specific fraudulent purpose. Input manipulation does not require sophisticated computer knowledge and can be committed by anyone with access to normal data processing functions at the input stage. Examples include

forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements.

Data Leakage

Data leakage refers to the unauthorized transmission of data from within an organization to an outside destination. Often, confidential information, intellectual property, customer data, and health records are leaked. Data can be leaked in a number of ways, including via email, laptop theft, hacker break-ins, lost or stolen backup tapes, removable media, and so on.

Wire Tapping

Wire tapping into a computer's communication links is another technique used to gain unauthorized access. This method enables perpetrators to read the information being transmitted between computers, or between computers and terminals.

Buffer Overflow Exploits

Buffer overflows can be used to exploit computer systems. To launch a buffer overflow attack, the attacker sends inordinate amounts of data to a running program that is waiting to receive input. The program copies the data into a *buffer*—memory used to store data temporarily during input and output operations. Buffers have a fixed size. Thus, if an attacker sends an amount of data that exceeds the size of a data buffer, the buffer overflows, but the extra data has to be put somewhere. The result is that the extra data is placed in an adjoining area of memory that is overwritten by the data sent by the attacker. Thus, attackers can exploit this effect to hack into a computer system and assume control.

Privilege Escalation Exploits

Privilege escalation refers to the act of exploiting a bug, design flaw, configuration oversight, or other vulnerability in an operating system or software application to gain access that is beyond the user's authorized access level.

Malware

To review, *malware* is an umbrella term for any kind of malicious software, including viruses, worms, Trojans, and spyware. Malware can infect computer systems from many sources. Some of the more common carriers of malware include:

- Unknown or unchecked application software
- Infected websites

- Banner ads
- Software or media employees bring to work
- Files downloaded from the Internet
- Infected software from vendors and suppliers
- Uncontrolled and shared program applications
- Demonstration software
- Freeware and shareware files
- Email attachments

Types of Malware

Some of the most common types of malware include:

- Viruses
- Worms
- Trojan horses
- Spyware
- Adware
- Ransomware
- Trapdoors
- Logic bombs
- Keyloggers

Viruses

The industry-accepted definition of a *virus* is:

> *"… a program that can 'infect' other programs by modifying them to include a version of itself."*

By using strings of code, virus programmers can infect a computer with a virus through various means (e.g., downloads, email, portable media, or websites) and then watch their work spread. Viruses can be designed to modify infected systems in various ways. Modifications caused by viruses include making a copy of the virus program, which can then go on to infect other programs.

Like its biological counterpart, a computer virus can replicate itself and cause damage to its host. Moreover, a computer virus can spread from one computer to another. Thus, unsuspecting users who swap disks or send programs to one another over a network can

spread the infection from computer to computer. In a network environment, the ability to access applications and system services on other computers provides a perfect culture for the spread of a virus.

A virus can do anything that other programs do; the only difference is that it attaches itself to another program and secretly executes itself every time the host program is run. Once a virus begins executing, it can perform any number of functions, including erasing files and programs.

During its lifetime, a typical virus goes through the following four stages:

1. *Dormant phase*: In this phase, the virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have a dormant phase.
2. *Propagation phase*: During this phase, the virus places an identical copy of itself into other programs or certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
3. *Triggering phase*: In this phase, the virus is activated to perform its intended function. The triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
4. *Execution phase*: During this phase, the virus performs its function. The function might be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Many virus scares are hoaxes, but even so, these phony warnings cause harm of their own. They slow down transmission of information and have been known to cause overloads of organizational email networks. Most of these fraudulent warnings from hoax viruses urge recipients to "forward this to everyone you know." Before forwarding a questionable warning, it is wise to consult a few authorities who track viruses. The following sites can be accessed to confirm or debunk virus notifications:

- www.symantec.com/avcenter/hoax.html
- www.snopes.com/computer/virus/virus.asp

There are many different types of computer viruses; however, it is not possible to discuss all of them here. But the way viruses work affects how they spread, and with this in mind, it is of value to provide a brief discussion of some major types of viruses in circulation. The following are some of the most common types of computer viruses:

- Boot-sector viruses
- Overwrite viruses
- Parasitic viruses
- Multi-partite viruses
- Directory viruses
- Stealth viruses
- Resident viruses
- Direct action (non-resident) viruses
- Network viruses
- File infectors
- FAT viruses
- Companion viruses
- Polymorphic viruses
- Macro viruses

BOOT-SECTOR VIRUSES

The *boot sector* is a sector of a hard disk, or similar storage device, that contains instructions carried out every time a computer is turned on. It is the first logical sector of a hard disk. Boot-sector viruses infect the boot sector and, because the instructions contained on a boot sector are processed before any other programs are run, the infected computer loads these viruses before other programs.

Once a boot-sector virus infects a system, every disk in the system becomes infected, allowing the virus to spread to other systems.

These viruses, however, were more popular when floppy disks were common.

OVERWRITE VIRUSES

Overwrite viruses are characterized by the fact that they delete the information contained in the files they infect, rendering files useless. Infected files do not change size, unless the virus occupies more space than the original file, because the virus replaces the content of a file rather than hiding within it. The only way to clean a file infected by an overwrite virus is to delete it completely.

PARASITIC VIRUSES

Parasitic viruses (sometimes called *binary file infectors*) attach themselves to program files (i.e., executables). When a user launches a program that has a parasitic virus, the virus is also launched. The parasitic virus is given the same rights as the program to which the virus is attached because the operating system considers it to be part of the program. These rights allow the virus to replicate, install itself into memory, or release its payload.

MULTI-PARTITE VIRUSES

Multi-partite viruses use a combination of methods to infect files; if they cannot infect a system using one method, they try another.

DIRECTORY VIRUSES

An operating system finds files by looking up the path (composed of the disk drive and directory) in which each file is stored, and *directory viruses* corrupt a directory entry so that it points to itself instead of the file it is replacing. That is, these viruses change the paths that indicate the location of a file. If a user executes a program (file with the extension .exe or .com) that has been infected by a directory virus, the user unwittingly runs the virus program instead of the original files that the virus replaced.

STEALTH VIRUSES

Stealth viruses use a number of different techniques to conceal themselves from users and virus scanners. They constantly change their patterns to blend into the system. Stealth viruses also encrypt their virus code to evade anti-viral software, and they remove their code from any infected files before a requesting program accesses the file.

RESIDENT VIRUSES

A virus can be either a resident virus or a direct action (non-resident) virus. A *resident virus* installs itself in the infected computer's memory. Upon execution, this type of virus searches for other files or programs to infect.

DIRECT-ACTION (NON-RESIDENT) VIRUSES

In contrast to resident viruses, *direct-action viruses* load themselves onto the target system's memory, infect other files, and then unload themselves.

NETWORK VIRUSES

Network viruses use network protocol, commands, messaging programs, and data links to spread. These viruses are generally developed to attack the file servers.

FILE INFECTORS

File infectors are viruses that attach themselves to programs or executable files (files with an .exe or .com extension). When an infected file or program is run, whether directly or indirectly, the virus is activated, producing the damaging effects it is programmed to carry out.

FAT VIRUS

A FAT virus attacks the file allocation table (FAT), a type of file system used to organize data and locate files. A FAT virus can be especially dangerous because it prevents access to certain parts of the disk where important files might be stored. These viruses can cause damages resulting in information losses from individual files or entire directories.

COMPANION VIRUSES

Companion viruses can be considered file-infector viruses. They are known as companion viruses because once they get into the system, they accompany other files that already exist on the infected system; that is, once these viruses attach themselves to a legitimate program, they create a program with a different filename extension; when the system's user tries to execute the legitimate program, he executes the companion virus instead.

POLYMORPHIC VIRUSES

A *polymorphic virus* is a virus that mutates itself and changes its structure to avoid detection. Some polymorphic viruses use different encryption schemes and require different decryption routines. Thus, the same virus might look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands in the attempt to thwart antivirus software.

MACRO VIRUSES

Macro viruses exploit macros in application programs. A *macro* is a stored series of commands that automate repetitive tasks. For example, a macro can tell Microsoft Word to spell-check a document automatically every 15 minutes. Many common applications (e.g., word processing, spreadsheet, and slide presentation applications) use macros.

Worms

Considered a subclass of a virus, a *computer worm* is a malicious self-replicating computer program that penetrates operating systems to spread malicious code to other computers. Worms have many of the same effects on a system as computer viruses. A worm is self-contained but, unlike a virus, does not need to be part of another program to propagate itself—a worm can spread by itself. Worms are often designed to exploit the file-transmission capabilities of computers (e.g., email) and are almost always spread through email, networks, and online chat.

In addition to replication, worms are designed to perform a variety of functions, such as deleting files on a host system or sending documents via email. Worms may be multi-headed and carry other executables as a payload. But even in the absence of such a payload, a worm can wreak havoc just with the network traffic generated by its reproduction. For example, Mydoom, also known as W32.MyDoom@mm, Novarg, Mimail.R and Shimgapi, was a computer worm that became the fastest-spreading email worm, causing the Internet to slow down at the peak of its spread in January 2004.

Worms can also carry backdoors as payloads, and once a system is infected with such worms, the compromised systems are used for various functions such as spamming or to collect information located on the host.

Like viruses, worms can infect the boot sector. Similarly, network worms use network connections to spread from system to system. Once active within a system, a network worm can behave as a computer virus or *bacteria* (i.e., programs that do not explicitly damage any files or other data), implant Trojan horse programs, or perform any number of disruptive or destructive actions. Network worms are designed to penetrate systems—the worm attempts to plant replicas of itself on other computers in a network. And although these programs can exist without damaging files, they reproduce at rapid speeds, saturating networks and causing them to collapse.

Trojan Horses

A *Trojan horse* is a program or command procedure that gives the appearance of being useful but in fact contains hidden code that causes malicious damage. When the hidden code in a Trojan horse is activated, it performs some unwanted or harmful function. Often, viruses and worms attach themselves to other legitimate programs, becoming Trojan horses and spreading to other systems.

Trojan horses might be used for a variety of reasons. Trojans have the capacity to delete files, to destroy information on hard drives, and to gain unauthorized access to information in a system. Often, Trojan horses are used to steal password files or other personal information.

Trojan horses are one of the most common techniques used to commit computer-based frauds and sabotage.

Spyware

Spyware is a type of software that collects and reports information about a computer user without the user's knowledge or consent. The presence of spyware is typically hidden from the user and can be difficult to detect.

Spyware performs many different functions, including the delivery of unrequested advertising (pop-up ads in particular), harvesting private information, re-routing page requests to illegally claim commercial site referral fees, and installing stealth phone dialers.

Spyware usually installs itself in one of two ways:

- The spyware component comes bundled with an otherwise apparently useful program.
- The spyware takes advantage of security flaws in the Internet browser.

The most common use of spyware for fraud is the theft of personal information (including financial information, such as credit card numbers).

Adware

Adware is any software application in which advertising banners are displayed while a program is running. The authors of these software applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. These Internet nuisances, which perform actions such as repeatedly sending advertising pop-ups, are justified on the basis that they help recover programming development costs and help lower the user's costs. Unfortunately, adware can also be programmed to deliver so-called *drive-by* downloads that take advantage of known system vulnerabilities to install malware without the user's knowledge. These malicious pop-ups might mimic a computer error message or dupe the user into accepting the installation via a pre-selected checkbox or radio button. Advertisement-blocking browser extensions are

available for most of the popular Web browsers and can alleviate many of the problems associated with adware.

Ransomware

Ransomware, as its name implies, is a form of malicious software (malware) that locks a user's operating system and restricts access to data files until a ransom is paid. To intimidate Internet users into compliance, ransomware often employs a convincing professional interface, commonly emblazoned with police insignia or an official government logo. Messages typically consist of threatening accusations that the user has been caught viewing illegal videos, downloading pirated media, or otherwise accessing forbidden Internet content, with the only remedy being to pay a fine. Other forms are far more direct and make no effort to conceal their obvious attempts at extortion.

While some ransomware simply prevents access to files, other forms, known as *cryptoviral ransomware*, actually encrypt users' files. This is of particular concern to businesses due to the potentially disastrous threat of encrypted network drives. These schemes typically promise that, after payment is received, the user will be provided with a key to release the system and unencrypt files; however, even after money is transferred, the virus typically remains installed on the machine and a key is never provided.

Trapdoors

Again, a *trapdoor* is a secret entry point into a program that allows someone who is aware of the trapdoor to gain access without going through the usual security access procedures. The trapdoor is code that recognizes some special sequence of input, or that is triggered by being run from a certain user ID or by an unlikely sequence of events.

Trapdoors have been used legitimately for many years by programmers to debug and test programs. The entry points allow programmers to bypass a program's setup and access procedures while they are developing the software. Trapdoors also ensure that there is a way to activate the program if something goes wrong with the authentication procedure that is built into the application.

Trapdoors become threats when they are used by malicious programmers to gain unauthorized access. It is difficult to implement operating-system controls for trapdoors. Security measures must focus on the program development and software update activities.

Logic Bombs

A *logic bomb* is code embedded in a legitimate program that is set to activate (or explode) and set off a malicious function when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application. Once triggered, a bomb can alter or delete data or entire files, cause a machine to halt, or cause some other form of damage. For example, an employee could create a logic bomb to damage his employer's computer network in an effort to drive down the company's stock once the logic bomb activated. Similarly, a former employee could, before his network access is revoked, plant a logic bomb to wipe out the organization's servers.

Keyloggers

Keyloggers monitor and log (or track) the keys pressed on a system's keyboard, and they can be either software or hardware based. Accordingly, some keyloggers are malware, but others are not. Keylogger malware is designed to capture a user's keystrokes, providing a method to collect passwords or other authentication information. Some keyloggers capture every keystroke while others only capture certain keystrokes, as when an individual visits an online banking site. Keylogger malware can be delivered through a variety of methods, including Trojans and browser exploits.

Crimeware

Crimeware is not a type of malware, but rather a classification of malware denoted by its intent to facilitate criminal behavior. Crimeware can be described as malware designed to simplify or automate online criminal activities, such as programs to fraudulently obtain financial gain from the affected user or other third parties.

Crimeware might result in any of the following:

- Theft of private information
- Identity theft
- Financial losses through the theft of online passwords
- Financial losses through accessing online services
- Invasion of privacy
- Loss of productivity because of system slowdowns, system errors, and so on
- Unwanted advertising (e.g., spam or pop-ups)

Botnets

A *botnet*—short for *robot network*—is a group of Internet-connected servers, computers, or mobile devices that interact to accomplish a distributed task. Typically, botnet systems are composed of computers that have been infected with malware that allows them to be taken over and controlled remotely by a third party. With remote access, the third party can control and harness the power of multiple compromised systems into a powerful network. The compromised computers are known as *zombies* or *drones*, and the malicious software programs running on them are *bots*. A *botmaster* takes over the botnet and operates the computers remotely without their owners' knowledge. Because their operators often rent their networks to others who wish to bring down websites, botnets can be very profitable.

Compromised systems are infected using a variety of techniques, including worms, remote exploits that affect the operating system or the browser, and malware-dropping Trojans.

Botnets can be used for various nefarious reasons, such as spamming, hosting phishing sites, installing malware, harvesting information from infected computers, installing adware, and so on.

Botnets have been around for years, but the schemes behind them have evolved. For example, in 2014, authorities from the United States, the UK, Australia, Japan, Germany, France, and Ukraine disrupted a massive botnet named Gameover Zeus that had been the primary distributor of the notorious CryptoLocker ransomware. For nearly a year, the CryptoLocker virus swept across the Internet, infecting more than 234,000 computers and generating an estimated $27 million in its first two months alone. Meanwhile, the Gameover Zeus network amassed more than $100 million in illicit proceeds.

Botnets are also used to launch distributed denial of service (DDOS) attacks against companies and organizations. DDOS attacks use botnets to overwhelm target servers with data in an effort to make the targeted website inaccessible and thus deny service to its intended users. DDOS attackers are often very difficult to identity due to the distributed nature of botnets.

DDoS attacks have now evolved into much more powerful and insidious varieties, such as DNS amplification attacks and application layer attacks, both of which are far more powerful than traditional DDoS attacks.

Malware Symptoms

The following are some symptoms that might indicate a malware infection:

- The system suddenly, and for no apparent reason, slows down its response time to commands.
- The computer stops responding or locks up frequently.
- The computer crashes then restarts every few minutes.
- The computer restarts on its own.
- The computer does not run as usual.
- The computer experiences a sudden and sometimes dramatic decrease of free space.
- The size of some files increases.
- The operating system or other programs and applications begin behaving in unpredictable ways.
- Files cannot be accessed or are suddenly erased with no warning.
- There has been a change in the length of executable files, a change in their content, or a change in their file date or time stamps.
- Disks or disk drives are inaccessible.
- An attachment that was recently opened has a double extension, such as a .jpg, .vbs, .gif, or .exe extension.
- The system does not boot up.
- There are unusual graphics and messages.
- The user cannot access a hard disk drive.
- There are unexplained and repeated maintenance repairs.
- There are unexplained changes to memory.
- System or data files disappear or become fragmented.
- Items cannot be printed correctly.
- Unusual error messages appear.
- Menus and dialog boxes are distorted.
- New icons, which are not associated with any new programs, appear on the desktop.
- Programs experience unexplained changes in size.
- Antivirus program is disabled for no reason.
- Antivirus program cannot be restarted.
- Antivirus program displays messages stating that a virus has been encountered.
- The Web browser's home page is changed automatically.
- When performing an Internet search, the Web browser visits a strange site.
- The user is unable to stop the excessive popup windows that appear without cause.
- The user receives a lot of bounced back email.

- There is evidence that emails are being sent without the user's knowledge.
- Unusual and unexpected toolbars appear in the system's Web browser.

Measures to Prevent Infection

Prevention is the best approach to combating viruses and other malicious software. Although prevention efforts can reduce the number of successful attacks, absolute protection is generally impossible to achieve. But even so, the following measures can help avoid infection from a malicious program:

- Use anti-malware software to scan all incoming email messages and files.
- Regularly update virus definitions in anti-malware programs.
- Use precaution when opening emails from acquaintances.
- Do not open email attachments unless they are from trusted sources.
- Only download files from reputable sources.
- Regularly update the operating system.
- Regularly update with the latest security patches available for the operating system, software, browser, and email programs.
- Ensure that there is a clean boot disk to facilitate testing with antivirus software.
- Use a firewall and keep it turned on.
- Consider testing all computer software on an isolated system before loading it.
- In a network environment, do not place untested programs on the server.
- Secure the computer against unauthorized access from external threats such as hackers and crashers.
- Keep backup copies of production data files and computer software in a secure location.
- Scan pre-formatted storage devices before using them.
- Consider preventing the system from booting with a removable storage device; this might prevent accidental infection.
- Establish corporate policies and an employee-education program to inform employees of how malware is introduced and what to do if malware is suspected.
- Encourage employees to protect their home systems as well. Many malware infections result from employees bringing infected storage devices or files from home.

Also, in case of data loss due to infection, steps should be taken to ensure that any lost data can be recovered. For example, companies should back up all programs and files, and they should keep the backup copies in a secure location. In extreme cases, it might be necessary to reload uncontaminated copies of files and data. Backups should be created frequently enough to avoid having to re-enter large amounts of data. Backups should be retained for a

sufficient time to have a clean set of files and programs in case a malicious program has been in place but not activated for a period of time.

Investigating Malware Infections

Malware infections can be investigated by taking the following action:

- Isolate the infected system and its media.
- Run antivirus software and document the findings.
- Interview the system custodian and all users, and determine:
  - Symptoms
  - Damage
  - Prior clean-up conducted
  - Access controls in place and working
  - System malfunction
  - Personal media used
  - Unauthorized media used
  - Virus identification
- Follow the audit trail of the infection.
- Determine the source of the virus—person, system, or media.
- Make users aware of protection policies and procedures.
- Ensure countermeasures are in place and working.
- Track the costs of virus problems.

Email

Email, while an essential component of an organization's communication infrastructure, presents a degree of vulnerability that needs to be addressed in a fraud prevention program. Consider the following applications for which email can be used:

- Company employees can use email to disclose sensitive company materials to unauthorized recipients, increasing the opportunity for corporate espionage.
- Company employees can transmit viruses via email to sabotage and crash organizations' networks.
- The original senders of emails can disguise or obscure their identity.
- Companies that employ a company-wide email system can be held responsible for any unethical or illegal activities employees perform on the email system.

- Companies must be concerned with the repercussions of the actions of any disgruntled or rash employees. The speed with which a disgruntled employee can "fire off" an email creates the opportunity for ill-advised communications.
- Once an email message has left a company's system, it might travel through any number of "foreign" email systems before reaching its destination. An email transmission can quite easily be intercepted or compromised if not encrypted.
- Without a security-enhanced email system, the receiver of an email message has little assurance that the email is authentic. Email addresses can be easily "spoofed" or cloned by a knowledgeable user.

Moreover, email can be delivered almost instantaneously anywhere. In fact, one of the emerging security problems concerning email is the huge volume of space required to archive old messages. In some organizations, people are regularly asked to cull through their old email messages and delete those no longer needed. Likewise, some organizations will delete any old email messages left on the mail server machines after a certain amount of time (e.g., one or two months).

Email Security Concerns

Because email has created vulnerabilities for most organizations, it is appropriate to discuss some email security concerns from both a user-based and an organizational perspective. Organizations often fail to set boundaries for employees regarding email and might later face legal ramifications as a result.

Email Ownership

Who owns email messages on an organization's system? This is the common question, but it is not necessarily the right question. An email message that an employee wrote himself is a work of authorship and, as such, the rules of copyright apply. In general, if the employee wrote the message as part of his duties for his employer (i.e., "in the scope of his employment"), the employer owns the copyright. If the email was not part of the employee's duties (something personal or related to another activity, whether permitted by the employer or not), then the user has copyright, but the employer, as owner of the system on which it was created or passed through, might have some rights to the copy on the system. If an employee is forwarding a message written by someone else, the issue gets even more complicated. For instance, does the original author have the right or the intention to authorize any forwarding?

Organizational Liability

As with any communications media, legal issues involving the Internet are emerging at a rapid rate, but they are of limited consensus so far. Nevertheless, it can be said that employers do have some liability for how employees use a company's email system. The issues are similar to an employee's use of the company telephone, the company postage meter, the company vehicle, and so on.

The best general advice is to exercise some caution when dealing with an email system. Within the company, email can become a vehicle for sexual harassment, creating a hostile work environment, or setting up gambling pools. Outside the company, employees can use email to operate their own businesses or to send out fabricated messages in the name of other employees or their employer. Some employers monitor their email systems, but doing so presents legal issues, such as invasion of privacy. Email has also been used to gather evidence against employers or employees. Of course, the dangers and pitfalls presented by email are not greater than those caused by any form of communication, whether inside or outside the organization.

As with any potential liability issue, employers must set guidelines for the proper internal and external use of email, just as they would for the proper use of the company telephone, stationery and postage, vehicles, and so on. For instance, the organization should have a written policy informing employees that email must not be used to send inappropriate and unprofessional messages. That is, the policy should prohibit the use of email for:

- Harassing other users of the system
- Consuming unreasonable amounts of available resources
- Intentionally sending other users viruses
- Evading software licensing or copying mechanisms
- Crashing/disrupting system services
- Impersonating another user anywhere on the Internet
- Bypassing system security mechanisms
- Translating encrypted material without authorization
- Eavesdropping on other email interactions
- Using the system for any personal gain, either monetarily or politically, unless permitted by the organization

Some commentators recommend that employers monitor employees' email, but the decision to monitor employees' email should not be taken lightly. For instance, the fact that the

company does try to monitor email might be used against the company when something slips through that monitoring.

Due to rapid growth of the Internet and email, there is a great deal of uncertainty in the law. Organizations might want to seek legal counsel in establishing proper use guidelines and before taking disciplinary action against employees because of alleged abuses.

Internet Fraud

The Internet is used by billions of people worldwide and is a major means of conducting business globally.

The Internet is also a tool for recreation, finding jobs and homes, making travel arrangements, and researching business and investment opportunities. But because of its appeal to consumers—those who want to fix their credit, shop, and find a good investment—it can also serve as a means of facilitating fraud.

Despite the dangers of Internet fraud, official policing of the Internet remains minimal. The Internet Crime Complaint Center (IC3), the Federal Bureau of Investigation (FBI) in the United States, and similar entities provide consumer warnings of current Internet fraud schemes. Yet these anti-fraud efforts, while worthwhile, are no match for the phony investment, credit, and get-rich-quick schemes that pop up every day online.

In addition, the laws that currently apply to the Internet are difficult to enforce because the Internet crosses virtually every international border. The lack of international laws and the difficulty enforcing those laws gives Internet fraudsters a better than average chance of avoiding capture and prosecution.

According to the *2014 Internet Crime Report*, the Internet Crime Complaint Center (IC3) received more than 269,000 complaints related to fraudulent and non-fraudulent issues on the Internet during 2013. The total dollar loss from all referred cases of fraud was more than $800 million. Frauds related to automobiles prompted the highest number of complaints, followed by government impersonation email scams, extortion schemes, real estate fraud, and romance scams all in the top five.

Commonly reported crimes included:

- Auto-auction fraud
- Government impersonation email scams
- Intimidation and extortion scams
- Real estate fraud
- Romance scams
- Auction fraud
- Credit card fraud
- Debt elimination
- Employment and business opportunities
- Identity theft
- Investment schemes
- Lotteries
- Phishing and spoofing
- Reshipping scams
- Spam
- Hit-man scams
- Ransomware/Scareware

As evidenced in the report, the Internet presents fraudsters with myriad opportunities to multiply the devices at their disposal. Some fraudsters have even used reputations of charitable organizations to exploit the most benevolent of human impulses. Perhaps the best way to guard against Internet-facilitated scams is to stay informed and be very skeptical of anything that seems too good to be true. Keeping informed of the latest scams on the Internet might enable Internet users to recognize and report these scams instead of losing money to one of them.

The majority of scams and schemes that have found new and lucrative homes on the Internet are similar to the conventional frauds that have plagued consumers for ages.

Electronic Commerce and Information Security

Electronic commerce, or *e-commerce*, is the process of two or more parties making business transactions via computer and some type of network (e.g., a direct connection or the Internet). This includes business-to-business transactions, online retail, and the digitalization of the financial industry.

Information Security Goals

All branches of an information system, including the e-commerce branch, strive to provide security to its users and asset holders. Below is a list of common information security goals that should be provided to users and account holders of information systems:

- Confidentiality of data
- Integrity of data
- Availability of data
- Authentication
- Non-repudiation

Confidentiality

The information involved in an information system transaction must only be accessible to authorized parties. This also requires that transactions, which have been captured in some way, retain their confidentiality even under attack.

Integrity

Integrity requires that transactions be incapable of modification by unauthorized parties. This is done to ensure that there is no doubt as to the validity of the transactions.

Availability

Information resources must be available. Businesses that offer products or services are very concerned with their accessibility because each moment their resources are not available results in lost opportunities.

Authentication

Authentication refers to the validation of a customer's identity. E-commerce entities must make sure that they can determine with whom they (or their computers) are communicating.

Transaction authentication protects two parties that exchange messages from any third party, but it does not protect the two parties from each other. The digital signature is the most popular solution to protecting the two parties from each other. A *digital signature* is an authentication technique that also includes measures to counter repudiation by either party. The digital signature is analogous to the handwritten signature but, to be legally binding, a digital signature must have the following properties:

- It must be able to verify the sender.
- It must be able to verify the date and time of the signature.

- It must be able to authenticate the transaction at the time of the signature.
- It must be verifiable by third parties.

Thus, the digital signature functions to authenticate e-commerce transactions. And based on the above properties, the necessary requirements for a valid digital signature can be determined. These requirements include:

- The signature must be a bit pattern that depends on the transaction being signed.
- To prevent both forgery and denial, the signature must use information unique to the sender.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new transaction for an existing digital signature or by constructing a fraudulent digital signature for a given transaction.
- It must be practical to store a copy of the digital signature.

To be effective, digital signatures use sophisticated cryptographic technology to make them resistant to forgery. Thus, a digital signature not only authenticates the user's identity before processing the transaction, it also provides cryptographic after-the-fact evidence of the transaction.

Non-Repudiation

Non-repudiation refers to a method to guarantee that the parties involved in an e-commerce transaction cannot repudiate (deny) participation in that transaction. That is, concerning information security, non-repudiation is a method to guarantee that the sender of a message cannot later deny having sent the message and that the recipient of the message cannot deny having received the message.

Again, in e-commerce transactions, non-repudiation is obtained through the use of digital signatures, confirmation services, and timestamps.

Consumer Confidence

Consumer confidence in e-commerce is also important. For consumers to retain their confidence in online transactions, the perception that the Internet is safe must be fostered. Unfortunately, some cases cause consumers to lose confidence in e-commerce. In the following example, a hacker crafted a sophisticated scam that hurt millions of consumers.

EXAMPLE

Albert Gonzales had already been caught hacking into the Indian government's website and trafficking a million credit/debit card numbers before he was caught stealing many more credit/debit card numbers from TJX Companies, the company that operates retail stores such as TJ Maxx and Marshall's.

Starting in 2005, Albert found non-secure wireless networks on TJX Companies' systems and worked with others to identify vulnerable servers to attack, infiltrate, and later use to jump into other more secure servers. From there, he and his conspirators were able to install malware used to steal data and sniffing software onto the networks of TJX and all the stores operating under the company, even outside of the United States.

TJX discovered the breach in December of 2006; it notified the authorities and was under the belief that it had only been losing data for six to seven months. After further investigation, however, TJX found that it had been losing sensitive data since 2005. In fact, TJX Companies discovered that two years' worth of sensitive data and 45.6 million credit card and debit card numbers were compromised. But by the time TJX discovered the extent of the security breach, Albert had already moved on to bigger and better operations.

In 2008, Albert was arrested on charges related to hacking into other companies' networks, and in 2010, he was sentenced to 20 years in prison.

Applying Encryption to E-Commerce Security

Generally speaking, the solutions offered by conventional and public key encryption technologies are usually adequate to ensure that e-commerce transactions are as secure as the value of the transactions requires.

Insider Threats

Employees inside an organization also pose a threat to information systems in terms of computer crime. It is not uncommon for operators, media librarians, hardware technicians, and other staff members to find themselves in positions of extraordinary privilege in relation to the key functions and assets of their organizations.

A further complication is management's tendency to tolerate less stringent supervisory controls over information system personnel. This tendency is based on the premise that such

work is not only highly technical and specialized, but also difficult to understand and control. For example, systems software support is often entrusted to a single programmer who generates the version of the operating system in use, establishes password or other control lists, and determines the logging and accounting features to be used. In addition, companies often permit, and sometimes encourage, such personnel to perform these duties during non-prime shift periods, when demands on computer time are light. As a result, many of the most critical software development and maintenance functions are performed in an unsupervised environment.

It is also clear that information system personnel often enjoy a degree of freedom quite different from that which would be considered normal in a more traditional employment area.

Insiders are typically aware of the holes in the system of internal controls and often exploit weaknesses just to see if they can get away with it. The most prevalent method of committing computer fraud is probably alteration or falsification of input transactions (and/or documents), including:

- Alteration of input
- Alteration of output
- Data file manipulation
- Communications systems
- Operating systems
- Computer operations

The characteristics of the traditional insider computer fraudster are very similar to those of the hacker or other computer criminal: intelligent, hardworking, seldom takes time off, bored with the routine of the job, and has a very large ego. Many computer technicians have demonstrated a greater loyalty to the technology than to the organization for which they work. This technology loyalty can create an attitude that any behavior is acceptable if it is in the name of technology.

The following are indicators of insider computer fraud:

- Access privileges are beyond those required to perform assigned job functions.
- Exception reports are not reviewed and resolved.
- Access logs are not reviewed.

- Production programs are run at unusual hours.
- Lack of separation of duties exists in the data center.

Computer Security

Computer security is defined as the protection of data in a system against unauthorized disclosure, modification, or destruction, and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain controls inhibit productivity, security typically involves a compromise in which security officers, system users, and system operations and administrative personnel work together to achieve a balance between security and productivity.

Effective computer security ensures the availability of accurate data in time to meet an organization's needs at a cost that is commensurate with the risks involved. Key elements to an effective computer security system include:

- Security policies and awareness training
- Data classification
- Risk assessments
- Computer security controls
- Physical security and controls
- Technical and administrative controls
- Security audits and tests
- Incident response plans
- Insurance for cyber risks

The most important step is to obtain management support for effective security. Without such support, any security plan will falter.

Security Policies and Awareness Training

Security policies provide the foundation for security in an organization. Policies provide a framework that ensures that informational assets are secured within a governing policy and are composed of a clear and concise set of guiding statements supported by management. Well-written and effectively communicated information security policies provide employees with guidance on the proper use of information assets, which allows management to mitigate the risks associated with the inappropriate use of computer systems, software, email, and the Internet.

Effective information security policies also help protect the organization against computer fraud. Security policies should take into account all facets of computer abuse and address key areas of concern, such as computer fraud.

Therefore, company management should state, in writing, what policies and standards must be followed by employees, vendors, and business partners with regard to network and communications security. These policies should outline what must be done, who must do it, and the consequences of not complying. Also, management should ask every employee to sign an agreement to follow the company's confidentiality and security standards.

Moreover, as a condition of employment, all company personnel should be given security awareness training so that they know their role in furthering company security. Likewise, management should update employees as new risks and vulnerabilities are discovered. Organizations should ensure that the training includes employees at satellite offices, temporary help, and seasonal workers.

Furthermore, leaders should offer their employees training on common issues and directives addressing how to identify red flags and how to deal with the high-risk issues the employees are likely to encounter, and training should be based on the organization's operations and needs. Accordingly, organizations should consider providing advanced instructions for personnel assigned to higher-risk areas or responsibilities.

Additionally, training must be user friendly; communications should be written in the local language and easily understood. This makes it more likely that employees will buy into the program, understand it, and appreciate it. For example, management should not give employees a large handbook that contains confusing terminology and is difficult to understand. Also, managers should train employees to recognize security threats, and impose disciplinary measures for security policy violations.

There are many different training formats available. Some popular formats include:

- Live seminars
- Online training
- Role-playing simulations
- Handbooks
- Compliance news updates
- Quizzes

Data Classification

Organizations should also classify their data. *Data classification* refers to the categorization of data for its most effective and efficient use. Data classification allows organizations to assign economic value to data and enables them to establish a structured approach for data management. Accordingly, to determine which controls are most appropriate for protecting an organization's information, management must properly classify data. Data can be classified according to any criteria, often by its importance or frequency of use.

Working closely with each department, proprietary documents should be classified according to the level of security that best meets the company's needs. For instance, documents might be labeled "private" for personnel matters and move up to "restricted" for pricing or marketing information. Trade secrets or highly sensitive information should be labeled "authorized access only." Notes and drafts of documents should also be safeguarded or destroyed when the final document is completed.

Government and military data classification standards abound, but there are no set standards for classifying commercial or nongovernment data. The following table contains a typical list of classifications that a private organization might use, from highest to lowest.

Commercial Data Classification

Classification	Description
Sensitive	Data that must be protected with the highest security; the disclosure of this data will cause the most harm to the organization
Confidential	Data that is less restrictive within the organization than sensitive data, but its disclosure might damage to the organization
Private data	Information that is private and should be guarded from disclosure (e.g., human resources data)
Proprietary	Information not generally available to parties outside the organization
Public	Information that is for the general public

Even without set standards, an organization's data classification should have several characteristics. The system should be dependent on the overall sensitivity of the information and the level of confidentiality desired. Some organizations use a simple system with two distinct classes: confidential and public. Others use more complex rating levels, including

sensitive, confidential, private, proprietary, and public. Establishing these categories depends on the level of protection required by the data an organization possesses.

To classify its data, an organization should answer the following questions to help determine how its data should be protected:

- What is the use of the information?
- What is the value of the information?
- How old is the data?
- What damages would the organization sustain if the information were disclosed?
- What damages would the organization sustain if the data were modified or deleted?
- What laws and regulations govern the protection of the information?
- What would be the impact on national security if the information were disclosed?

Once data has been classified, management can conduct a risk assessment to determine the most cost-effective means of protecting it.

Computer Security Risk Assessment

As organizations grow, their information technology and data change in type and quantity. Thus, organizations should evaluate their security controls.

Risk assessment plays a critical role in protecting their digital assets. *Risk assessment* is the process whereby management identifies its risks, assesses the probability that those risks will materialize, calculates the damage that would result if the risks materialized, and determines the costs of applying the necessary safeguards to mitigate the identified risks.

In general, risk assessment has four main objectives:

- Identify the risks that make an organization vulnerable.
- Identify where fraud is most likely to occur.
- Quantify the economic impact that would result if the risks materialized.
- Provide an economic balance between the economic impact if the risks materialized and the costs needed to safeguard those risks.

More specifically, the risk assessment process can be summarized in the following six steps:

1. *Identify assets*: The first step is to identify physical and digital assets that the organization needs to protect and determine where that data is located.
2. *Value the assets*: Next, determine the value of each asset.

3. *Identify risks and threats*: Once management has identified and valued its assets that need to be protected, it should identify any threats to each asset and calculate the probability of each of those risks materializing for a single event and on an annual basis.
4. *Calculate the loss per risk*: Next, management should calculate the damage that would result if those risks materialized.
5. *Recommend countermeasures or other remedial activities*: After calculating the loss per risk, management should review the current security measures and identify any steps that must be taken to counter the risks and calculate the cost of implementing those measures for a single event and on an annual basis.
6. *Reduce, transfer, or accept the risk*: Finally, management should manage the risk by reducing the risk by adding controls, improving processes, modifying the environment, and designing a contingency plan to apply if the risks occur; transferring the risk by acquiring an insurance policy; or accepting the risk.

The risk assessment process is a time-consuming process, and many organizations employ outside security consultants to reduce its effect on day-to-day operations.

Computer Security Controls

Computer security controls guard or countermeasure to avoid, undermine, or minimize security risks relating to computer systems, and they are essential to effective computer security. Controls for providing security can be technical, administrative, or physical.

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Examples of technical security controls include password systems, firewalls, encryption, access control software, antivirus software, and intrusion detection systems.

Administrative security (or *personnel security*) consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances. Examples include security policies and procedures, security awareness and training, adequate supervision of employees, and security reviews and audits.

Physical security involves the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage; theft and destruction; or damage by accident, fire, or natural disaster (e.g., floods and earthquakes).

Physical Security and Control

A computer security system must not only provide protection against technical and administrative threats, but it must also protect against physical threats. Physical security threats strike directly at the availability of information. In the arena of corporate espionage, physical threats to security include things such as vandalism, sabotage, and theft of proprietary information. Any physical security system, however, should be built to encompass all potential physical threats, not just those involving espionage. Thus, this section will also discuss other potential physical threats such as fire, natural disaster, and threats to supporting utilities.

Physical security and control is the protection of information system resources against human-made and natural hazards, whether accidental or intentional. The idea of physical security is to protect against unwarranted intrusions to the data center; to prevent damage to the data center that might occur through sabotage, vandalism, or natural disaster; and to put the organization in a position where, should damage occur, adequate backup is available. Furthermore, a comprehensive physical security system should provide for the early detection of intruders or forms of damage, such as fire, so that losses and downtime can be minimized.

Types of Physical Threats

A physical security system should be designed to protect against all foreseeable physical threats to information assets, including:

- *Crime*: Information operations can be threatened by such criminal activities as vandalism, sabotage, theft, or terrorist acts.
- *Physical damage*: This is damage to the information system assets as a result of such hazards as fire, smoke, and explosion.
- *Natural hazards*: Assets can be damaged by earthquake, lightning, windstorm, hurricane, tornado, flood, or volcanic eruption.
- *Environmental hazards*: Information operations can be damaged as the result of flammable, toxic, or corrosive chemicals within or outside the data center.

- *Threats to supporting utilities*: These can include loss of electrical power or communications lines inside or outside the computer facility or loss of climate control in the computer room.

Although criminal activity is the focus of the material, a complete security system should blend elements of prevention and detection for all potential threats, including physical damage, natural hazards, environmental hazards, and threats to supporting utilities.

Physical Controls

An effective computer security system contains physical controls to, among other things, keep unauthorized personnel from entering physical facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media), to help protect against natural disasters, and to warn personnel that physical security measures are being violated.

EXAMPLES OF PHYSICAL CONTROLS

Examples of physical controls include:

- Selecting sites that minimize the physical risks to computer-based assets (e.g., sabotage, arson, earthquakes, tornadoes, floods, or hurricanes)
- Putting fences around the perimeter of a computing facility
- Having security guards stationed at the entrances of facilities to intercept intruders and ensure that only authorized persons are allowed to enter
- Installing double door systems at entrances of restricted areas (e.g., computing facilities) to force people to identify themselves to security personnel before they can access the secured area
- Having sources of backup power to ensure that computer services are in a constant state of readiness and to mitigate damage to equipment if normal power is lost because of sabotage, vandalism, natural disaster, or some other unforeseen occurrence
- Maintaining backup files and documentation to guard against losses due to theft, arson, sabotage, or non-malicious disasters
- Storing backup copies of the most current records at a reliable offsite location
- Installing detective physical controls to warn personnel that physical security measures are being violated (e.g., motion detectors, smoke and fire detectors, closed-circuit television monitors, and sensors and alarms)

PHYSICAL ACCESS CONTROLS

For computer security purposes, physical access controls are a notable type of physical control. *Access control* is a process by which users are identified and granted certain privileges to information, systems, or resources, and with access control systems, management can control access to information, systems, a physical facility's areas, or resources. *Physical access controls* refer to the process by which users are allowed access to physical objects (e.g., buildings). These controls can be used to verify a person's identity and privileges before granting the person physical access (to a building or site).

There are various types of physical access control devices that can be used to control access to physical objects. Some common types of physical access control devices include:

- Locks and keys
- Electronic access cards
- Biometric systems

LOCKS AND KEYS

Locks and keys are the most common method used to control access to physical objects. Locks and keys are inexpensive and easy to install, and therefore, they are commonly used for controlling access to restricted areas. But because keys are easily lost or duplicated, many organizations use cipher locks (i.e., combination locks containing buttons that open the lock when a particular code is punched in). With cipher locks, care must be taken to conceal the combination, and combinations should be changed on a regular basis, especially after employee terminations.

ELECTRONIC ACCESS CARDS

Many organizations use electronic access cards that verify to an electronic card reader that the cardholder has the right to access particular areas. Electronic access cards and card readers offer several advantages. Management of an organization with an electronic access card system can deny access rights without having to change locks or re-code cipher locks, it can limit access to physical areas to certain times, and this type of system can provide audit trails for incident investigations.

Electronic access cards and card readers, however, have disadvantages. These systems are prone to piggybacking, cardholders can share their cards with unauthorized persons, cards can be stolen and used by unauthorized persons, and they are more expensive than traditional locks.

There are various types of electronic access cards, including:

- Magnetic stripe cards
- Embedded wire cards
- Proximity cards

BIOMETRIC SYSTEMS

Biometric technology systems control access by measuring some physiological or behavioral characteristics to label and describe individuals. Common physiological characteristics measured include finger prints, palm prints, and iris patterns. These systems use such physiological properties to verify user access. Behavioral biometrics are related to the behavior of a person, and they include typing rhythm, gait, and voice.

Because biometric identifiers are unique to individuals, they cannot be lost, stolen, or shared; therefore, biometric identifiers provide a higher level of security than most other types of controls for physical access. But due to the high cost involved in implementing biometrics access controls, they are usually recommended only for high-security, low-traffic entrance control.

Technical and Administrative Controls

Computer networks and communications are inherently insecure and vulnerable to attack and disruption, and it follows that management must use technical and administrative controls to protect systems against threats like unauthorized use, disclosure, modification, destruction, or denial of service.

Again, *technical security* involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices, and *administrative security* involves the use of tools to provide an acceptable level of protection for computing resources.

The objective for securing computer systems and communication networks is to provide connectivity with acceptable response times, user-friendly access, and a secure mode at an acceptable cost to the organization.

Common technical and administrative controls used to secure computer systems and communication networks include:

- Logical access controls
- Network security
- Operating system security
- Encryption
- Application security
- Separation of duties

Logical Access Controls

Logical access refers to the process by which users are allowed to use computer systems and networks, and *logical access control* refers to a process by which users are identified and granted certain privileges to information, systems, or resources. These controls are designed to protect the confidentiality, integrity, and availability of informational resources.

In fact, one of the most effective methods for preventing system attacks by hackers, corporate spies, or other unwanted intruders is to implement a logical access control system to verify a person's identity and privileges before granting the person logical access to information or other online resources.

Generally, logical access can be established in three steps:

- Identification
- Authentication
- Authorization

IDENTIFICATION

When a user starts to interact with an information system, he is required to provide an identifier (e.g., a username, employee number, or account number), and the system must recognize the user attempting to access a resource. The user's identifier should be unique, unlikely to change, and need not be kept secret. Thus, employees should not have the same type of usernames because it makes it easier for an attacker to spoof or log in using an employee's information.

In addition to being used during processing for authorization controls, the identifier can be used for variance detection and for other purposes, such as accounting and billing.

AUTHENTICATION

Once a user is identified, he must be authenticated. There are three primary considerations associated with user authentication:

- A user must be prevented from fooling the computer system into thinking he is someone else. (False positive verification must be avoided.)
- The computer system must accept an accurate user identity. (False negative verification must be avoided.)
- Verification procedures must be easy for users to comply with.

There are three primary methods of authentication:

- Something the user knows (e.g., a secret password)
- Something the user has (e.g., a magnetic stripe card or smart card)
- Something the user is (e.g., biometrics information)

Ideally, the authentication process requires the user to comply with at least two of the three methods above—a strategy known as two-factor authentication—to gain access to the system. In reality, however, most organizations with medium security requirements still depend solely on re-usable passwords.

The following materials discuss the following options for authenticating users in information systems:

- Passwords
- Card-based systems
- Biometric systems
- Multifactor authentication
- Profiling software

PASSWORDS

Passwords are the most common method to authenticate users for logical access. Password authentication uses a secret string of characters to control access to a particular resource. Passwords should only be known to the user and the access control system.

Weak passwords are often exploited to breach system security; therefore, effective password administration is essential for maintaining security. Organizations should enforce policies requiring the use of strong passwords. Passwords should be kept in accordance with

sound security practices, and the following measures are essential in maintaining effective password security:

- Passwords should be of sufficient length (usually a minimum of eight characters). Generally, the longer the password, the more difficult it is to crack.
- Passwords should be a mix of letters, numbers, and characters.
- Passwords should be different from the user's identifier (e.g., username).
- To maintain individual accountability, management should prohibit group passwords and the sharing of passwords.
- Passwords should be changed periodically.
- Passwords of all terminated employees should be revoked immediately.
- Employees who have changed job functions or been transferred should have their old passwords canceled and new ones issued, if appropriate.
- Systems should lock out users who do not enter the correct passwords within a designated number of attempts.

Passwords are not impervious to human error or misuse. The downside of using passwords to prevent unauthorized access is that they can be bypassed, guessed, lost, written down, or given away.

Employees should be warned about possible calls from fraudsters attempting to deceive them into giving out their passwords by impersonating individuals who would need access to that type of information. Let employees know that calls such as this are always fraudulent, and that no one should be asking them to reveal their passwords.

CARD-BASED SYSTEMS

Again, a unique personal possession such as a coded card can be used to identify individuals accessing a system. There are various types of technology that can be used to verify the identity of persons attempting to gain access to a system, including smart cards. Smart cards—cards embedded with a built-in chip for onboard data storage or computation—are similar to ATM cards; like ATM cards, they are susceptible to loss and forgery.

BIOMETRIC SYSTEMS

To review, biometric systems measure physiological properties to identify and authenticate users. Common physiological characteristics measured include finger prints, palm prints, and iris patterns.

MULTIFACTOR AUTHENTICATION

Organizations should consider implementing a multifactor authentication security system. Multifactor authentication requires the presentation of two or more authentication factors to verify the legitimacy of a transaction, and it is a preferred method for preventing attackers from cracking passwords. To review, the methods of authentication are:

- Something the user knows (e.g., a password, PIN, or pattern)
- Something the user has (e.g., USB tokens, smartcards, magnetic stripe cards, virtual tokens, soft tokens, etc.)
- Something the user is (e.g., biometrics, such as fingerprint or retina pattern)

To be effective, multifactor authentication needs to be user-friendly or it defeats its own purpose. If users find it burdensome, they might resort to shortcuts that end up compromising their security, like writing their password on notes that are taped to their computer.

PROFILING SOFTWARE

Profiling software authenticates users by monitoring their statistical characteristics, such as typing speed and keystroke touch.

AUTHORIZATION

Authorization determines the privileges a user has on a system once he has been authenticated; that is, once a user has been verified and authenticated, the system should check each request to determine whether it is legitimate for that user. Some users might be authorized to perform only certain functions and to have access only to certain data. Moreover, each employee should only be allowed access to the information that he needs to perform his duties. For example, an entity's logical access control system might grant a high-level manager access to files that contain sensitive financial or strategic marketing information, while it does not grant such access to low-level employees.

By limiting access to sensitive information, an organization minimizes the risk of information theft. If only a few employees have access to a secret distribution plan, for instance, then the majority of employees are precluded from revealing the information unless they are able to circumvent the authorization scheme. It also makes it more difficult and risky for an unauthorized person to access the information. Moreover, by limiting access to sensitive information, management reduces the number of potential leaks and creates fewer potential recruits for corporate spies.

Network Security

Network security is the protection of the network perimeter, as well as the segmentation of the internal corporate network. Oftentimes, management devotes resources to protecting its network from outsiders but fails to properly segment its internal network based on risks. Much like logical access control, network resources and segments should only be made available to those who require them. An example of this would be segmenting the Research and Development network from the rest of the organization due to the sensitive nature of the information that is handled in such an environment.

Network security defenses include:

- Firewalls
- Intrusion detection systems
- Intrusion prevention systems
- Network access controls

FIREWALLS

Firewalls are network hardware and software that block unauthorized or unverified access to computer systems and network assets. These tools survey incoming and outgoing transmissions and decide what type of traffic to permit onto an organization's internal network based on factors such as origination or destination address, content of the message, protocol being used to transmit the message, and other filtering methods.

Firewalls act as the first line of defense against network-based threats by enforcing an access control policy for traffic flowing between networks. A company's firewall policy determines which information can flow in and out of each protected network segment by examining packet information such as origination or destination address, content of the message, protocol being used to transmit the message, and other filtering methods. The most effective policy is one that is designed to restrict all traffic except that which is expressly permitted.

INTRUSION DETECTION SYSTEMS

An *intrusion detection system* (IDS) is a device or software application that monitors an organization's inbound and outbound network activity and identifies any suspicious patterns of activity that may indicate a network or system attack or security policy violations. An IDS alerts administrators when someone or something is trying to compromise the information system through malicious activities or security policy violations. These systems are designed to supplement firewalls and other forms of network security by detecting malicious activity

coming across the monitored entity's network or system activities. They act much like a motion sensor would; detecting individuals who have bypassed perimeter security.

IDS can be instructed to look for particular violations of the company security policies—such as an excessive number of unsuccessful log-ins by the same user—and report them, as they occur, to the network administrator. The software can prevent this type of attack from occurring in the future by terminating the user's log-in account so that future attempts to use the account, even if accompanied by the correct password, will be unsuccessful.

Intrusion detection systems can react in a number of ways, including reconfiguration of the organization's firewall to block messages from the intruder. Most systems will log the attack to a centralized management for future review by systems administrators. A system might also set off an alarm or send an email to the administrator to notify him of the attack.

INTRUSION PREVENTION SYSTEMS

In contrast to intrusion detection systems, which are reactive, *intrusion prevention systems* (IPS) are proactive. They are designed to stop intrusions from occurring, blocking the offending traffic before it does any damage instead of simply raising an alert as, or after, the malicious payload has been delivered.

NETWORK ACCESS CONTROL

Network access control technology is designed to limit access to a network based on a user's credentials and his system's security posture. The user's credentials indicate to which network segments a user has access. For example, a user in a company's accounts payable department would have access to the entire corporate network with the exception of Research and Development and some servers, while a guest could be limited to Internet access only.

The security posture of the system is determined by the patch level of the system and the presence of certain security software on the user's system. A user with an up-to-date operating system and virus signature files would be granted access to the network, while a user who is behind on his virus signatures would be placed in a quarantine network until his signatures are updated.

This type of access control ensures that the network is properly segmented, that only authorized users have access, and that their systems present no major vulnerabilities to the network and its applications.

Operating System Security

The operating system is at the core of every computer system. It is responsible for the direct control and management of hardware and basic system operations, as well as running application software.

Often, attackers exploit operating system weaknesses to gain access to the system, as well as the applications and data residing on the system. To protect operating systems, system administrators should implement a variety of measures, such as hardening the operating system, installing the vendor- or community-provided patches, employing warning screens, and so on.

SYSTEM HARDENING

Hardening is the process of eliminating basic vulnerabilities on an operating system. Out-of-the-box operating systems are generally not secure because they contain a multitude of tools and features that are ripe for exploitation. Hardening helps safeguard a system from intrusion.

To harden an operating system, administrators remove the nonessential tools and utilities. Next, administrators ensure that all off the system's security features have been activated and properly configured. There are many tools and guides to help an administrator harden an operating system, and many of these are available on the Internet for free.

PATCH MANAGEMENT

Every week, new vulnerabilities are discovered in operating systems and applications, and attackers exploit these vulnerabilities to gain access to systems. To protect against such exposures, system administrators should install patches as soon as they become available. Proper patch management can prevent worms and older exploits from being exploited.

WARNING SCREENS

Companies should install warning screens that appear before a user logs in to his employer's system. Many corporate computer systems display a welcome screen upon start-up. These screens should be replaced with a warning screen that informs the user that he is about to access a proprietary network. Additionally, the screen should warn that unauthorized access is prohibited and will be prosecuted under the law. This screen, however, should not identify either the organization or the network.

More specifically, the screen should warn users of the following matters:

- What is considered to be proper use of the system
- That the system is being monitored to detect improper use and any other illicit activity
- That the user should have no expectation of privacy while using this system

Organizations should consult with their legal counsel to ensure that the banner is sufficient for legal issues that might arise.

Encryption

Encryption is one of the most effective methods of protecting networks and communications against attacks. *Encryption* is the deliberate scrambling of a message so that it is unreadable except to those who hold the key for unscrambling the message. There are, however, drawbacks to encryption, such as maintaining encryption keys and the inherent delays incurred by the extra steps required for processing. The decision to use encryption should be made in light of such issues.

Application Security

Application security encompasses controls implemented to prevent exceptions to the security policy of an application and its underlying systems through flaws in design, development, or deployment. Controls built into the application reduce the likelihood that it will be manipulated to access, steal, modify, or delete data.

Separation of Duties

Separation of duties is a key element in a well-designed internal control system, and it is fundamental to data security. Separation of duties is achieved by diffusing the tasks and associated privileges for a specific security process among multiple individuals, and to establish separation of duties with information security, organizations should be set up so that no person acting alone can compromise security controls. Accordingly, separation of duties limits the amount of power held by any person.

Below is a list of IT technologies that create separation of duties concerns:

- Application administrator access
- Security administrator and user setup
- Programmer access to production
- Strength of authentication

- Shared passwords
- Access to edit/change audit tables

There are various options for achieving separation of duties in information security, and the options vary depending on department responsibilities. For example, some of the best practices for ensuring segregation of duties within the information systems department and between information systems and business unit personnel include:

- Programmers should not have unsupervised access to production programs or have access to production data sets (data files).
- Information systems personnel's access to production data should be limited.
- Application system users should only be granted access to those functions and data required for their job duties.
- Program developers should be separated from program testers.
- System users should not have direct access to program source code.
- Computer operators should not perform computer programming.
- Development staff should not have access to production data.
- Development staff should not access system-level technology or database management systems.
- End users should not have access to production data outside the scope of their normal job duties.
- End users or system operators should not have direct access to program source code.
- Programmers should not be server administrators or database administrators.
- IT departments should be separated from information user departments.
- Functions involving the creation, installation, and administration of software programs should be assigned to different individuals.
- Managers at all levels should review existing and planned processes and systems to ensure proper separation of duties.
- Employees' access to documents should be limited to those that correspond with their related job tasks.

Security Audits and Tests

In addition to establishing mechanisms to prevent unauthorized access, management must actively monitor and test their security systems to identify and address deficiencies and to maintain a secure system over time.

This material discusses:

- Log management and analysis
- Data security
- Security auditing
- Penetration testing

Log Management and Analysis

Almost all systems maintain a log file that records system-related events, such as access attempts. *Logging*, also known as *journaling*, is the process of making a record of system-related events or logs for analysis. A log is a record of the events occurring within an organization's systems and networks. Logs are composed of entries, and each entry contains information related to a specific event that occurred within the system or network.

Recording logs as they occur within a system provides a basis for identifying and tracing events involved in the processing of data, in the use of computer resources, or in the operation of computer and network devices and systems.

Moreover, logs can be useful in various circumstances. They can provide valuable information when performing auditing and forensic analysis, and they can be used to support internal investigations, establish baselines, and identify operational trends and long-term problems.

It is difficult to detect security violations unless there is a record of events for analysis, and recovery from system failures can be aided by logging appropriate events. Likewise, management can generate reports from their log files (e.g., sign-on and sign-off activity and unsuccessful access attempts), and the person in charge of the company information security program should examine the logs in the journal records (e.g., event logs, audit file, records journal, or any other similar entity) on a regular basis for any entries that appear abnormal or out of the ordinary.

Moreover, users are less likely to engage in malicious activities and to make errors in their day-to-day interaction with an application if they know that their activities could be recorded.

Applications should take advantage of automated journaling systems to track user activity. One or more automated journals might be employed; the application designers should structure the journals to permit flexibility while minimizing overhead.

Logging, however, is not without challenges. Log entries are vulnerable to accidental or deliberate events that can endanger the logging process or the log contents, such as:

- The log contents can be partially or totally lost in a system crash caused accidentally (e.g., by a power failure to a volatile storage device) or deliberately (e.g., by someone trying to avoid detection).
- The logging process can be disabled or the log entry destroyed by a system penetrator.

Moreover, many organizations find it difficult to balance limited resources with a constant supply of log data. The level of detail monitored, the amount and type of data saved, the length of time data must be saved, and the complexity of processing the data affect the logging process and influence the cost and hardware requirements. A log management system can help tame the volumes of data.

The National Institute for Standards and Technology (NIST), which offers a measure of assurance that the tools used by U.S. law enforcement officials in the investigations of computer-related crimes produce valid results, defines *log management* in *Special Publication 800-92: Guide to Computer Security Log Management* as: "the process for generating, transmitting, storing, analyzing, and disposing of computer security log data."

Log management is essential to ensure that logs are stored in adequate detail for an appropriate period. The NIST provides several recommendations to establish efficient and effective log management in *Special Publication 800-92: Guide to Computer Security Log Management*. According to NIST, management should:

- Prioritize log management appropriately throughout the organization.
- Create and maintain a log management infrastructure.
- Provide proper support for all staff with log management responsibilities.
- Establish standard log management operational processes.
- Establish the architecture for the log management system by determining what events will be recorded in logs, from which systems, where to record event data, and how long logs will be retained.
- Consolidate event records to a central collector.

Data Security

Organizations must have effective data security. Effective data security ensures the availability of accurate data in time to meet an organization's needs at a cost that is commensurate with the risks involved.

An organization's data security function should have sufficient resources and staff to administer passwords, maintain the security software, review system activity reports, and follow up on *all* potential security violations.

Security Auditing

An entity should hire experienced and qualified consultants or internal or external auditors to conduct periodic reviews of its system's security. A *security audit* involves testing the operating system and applications of a system or systems within a network or networks, focusing on the elimination of any security or access loopholes. To perform their work, security auditors conduct personal interviews, perform vulnerability scans, examine operating system settings, and analyze network shares and historical data.

Typically, security audits involve five phases:

1. Initiate and plan the audit:
   - Meet with management to identify possible areas of concern
   - Become familiar with the IT organization chart and job responsibilities of data center employees
   - Research the operating systems and software applications
   - Examine the organization's security policy and procedures
   - Assess the organization's IT budget and systems planning documentation
   - Examine the organization's data recovery plan
   - Establish audit objectives
2. Perform fieldwork:
   - Interview users
   - Inspect equipment
   - Examine and document the organization's policies and procedures
   - Assess the physical security controls
   - Verify backup procedures
   - Perform tests
3. Conduct analysis:
   - Confirmation

- Verification
- Reconciliation
- Exit conference

4. Issue a report:
   - Findings
   - Recommendations
   - Schedule client corrective action report
   - Plan for follow-up engagement
   - Archive the report
5. Follow-up:
   - Confirm corrective action
   - Address challenges
   - Repeat phases (as necessary)

Penetration Testing

Some organizations that have the resources test their computer and network security by subjecting themselves to *penetration testing*—when a group of trusted individuals test an entity's network security by attempting to breach it.

Most penetration tests are conducted by a trusted team of outsiders, known as a tiger team. In a penetration test, the tiger team attempts to exploit security vulnerabilities to determine whether unauthorized access or other malicious activity is possible; they identify vulnerabilities that exist in a system or network with security measures in place.

Penetration testing is done so that management can assess the organization's security programs during real-world attacks that can be controlled. The period to conduct a penetration test varies, depending on the situation.

Incident Response Plans

To ensure a comprehensive security strategy, management should plan and implement an incident response plan that defines how to respond to network intrusions. The incident response plan is an emergency plan of sorts. If a suspicious event is identified, management can take any number of possible actions, including:

- Suspend or terminate the offending process while the issue is investigated and send a message to notify the users.

- Automatically invoke special monitoring (e.g., complete logging of all activities and interactive traffic of the offending process).
- Provide real-time information on a designated console that displays the full interactive traffic of an offending terminal.

The methodology for an incident response plan can be summarized in the following steps:

- Planning for intrusions
- Detecting intrusions
- Handling the incident
- Breach notification
- Recovery
- Follow-up

Planning for Intrusions

It is critical that organizations have a plan for dealing with intrusions before they occur. If staff is trained to handle security incidents quickly and efficiently, it can minimize downtime as well as the amount of resources that are dedicated to responding to the intrusion.

Additionally, the response plan should be tested to see how well it functions in the event of an actual intrusion. Some organizations conduct dry runs to measure the effectiveness of their response systems, and in some cases, this process is combined with penetration testing.

It is important for a response plan to prioritize actions in the event of a security breach occurs. The *Site Security Handbook*, a guide to developing computer security policies and procedures, offers the following suggestion for prioritizing the goals of an incident response strategy:

- Protect human life and people's safety.
- Protect classified and sensitive data.
- Protect other data, including scientific, proprietary, and managerial information.
- Prevent damage to systems, such as loss or alteration of system files.
- Minimize disruption of computing resources.[3]

Management must delineate whom to contact if a security incident occurs, and it must define the roles and responsibilities for investigating events. These responsibilities might depend on

[3] Ed Fraser, ed. RFC 2196, *Site Security Handbook*, Internet Engineering Task Force, September 1997.

the type of event. For example, if a database becomes riddled with errors, responsibilities could be assigned to the people who generate the data, unless the data was corrupted by errors in the programs, operations, data entry, or other functions that exceed such users' responsibilities.

To make such delineations, management must determine who will be in charge of coordinating the incident response. The coordinator will determine how the response action proceeds and what roles other affected parties should have. The coordinator is also the contact person for outside entities, such as law enforcement, if the incident is reported. The coordinator is the hub of the internal investigation and is in charge of gathering evidence. Thus, the coordinator should have a working knowledge of investigatory procedures. In addition, this person must have enough technical expertise to understand how the compromise occurred and to direct the efforts of systems administrators in responding to the attack.

Moreover, the coordinator should immediately notify the organization's legal counsel in the event of an attack. Lawyers can help determine potential liability, as well as the company's interests in publicizing or downplaying the incident. Furthermore, the legal department should advise on if and when to call law enforcement authorities.

If an organization has a computer security incident response team, the team should be notified as early as possible. If the breach occurred due to some breakdown in computer hardware or software, the hardware or software vendor should be contacted.

It might also be necessary to inform employees, vendors, and customers about problems that could occur as a result of the incident and about any information they should divulge to outsiders about the attack.

Detecting Intrusions

Once the initial plans have been laid, management must concentrate on identifying incidents as quickly as possible. In general, this is accomplished through intrusion detection systems and security auditing, which are discussed below.

Handling the Incident

When an attack does occur, management must fall back on its preparation and planning to deal with the incident as quickly as possible. The idea is to restore control of the affected

systems and limit the damage. Other considerations, such as identifying the intruder, are important, but maintaining control of the system is a primary concern.

Moreover, as soon as an intrusion is detected, the appropriate personnel must be notified in accordance with the incident response plan. Information about the attack should be distributed on a need-to-know basis. Systems administrators and incident response teams need very precise technical details about the intrusion to effectively counteract it. Other employees, customers, vendors, and so on probably do not require such detailed information. Managers need to pass out enough information to effectively combat the problem without giving so much that it creates a panic or additional vulnerabilities.

Also, before deciding how to repair damage or uncover the intruder's identity, the response team should begin by gathering as much information about the intrusion as possible. As soon as an attack is detected, the team must assess the resulting damage. Several crucial pieces of information must be uncovered when assessing the attack, including:

- Which systems were compromised?
- What kind of damage did the intrusion cause?
- Is the intrusion still causing problems?

Any time a breach occurs, the entire computer system should be considered suspect, and organizations should check all system software and files for irregularities. The audit file function of a security-auditing program and logs generated by firewalls and routers are helpful in detecting anomalies.

The intrusion response coordinator must also make two copies of all systems believed to be compromised: one copy that can be used in attempts to rebuild any damage caused by the intruder, and another copy that can be used as evidence in any future litigation resulting from the break-in. The copy to be used as evidence should not be altered or compromised in any way.

As the organization responds to the intrusion, it is imperative to maintain an accurate log of all details relating to the event. This not only will help investigators follow the course of events and track down the problem, but it can also provide legal evidence should the attack lead to a criminal prosecution or civil litigation.

Once the response team has identified exactly which network systems have been compromised, these systems should be contained. Containing compromised systems can be as simple as shutting down the affected systems, disconnecting the affected systems from the rest of the company system, or a combination of both. Obviously, shutting down portions of the company's computer network will cause substantial delays for company employees, reducing the company's workplace efficiency dramatically. But this action can also alert company customers and, if the company is large enough, media outlets that the company is experiencing computer problems. It is generally preferable to shut down a system and prevent additional damage, but in some cases, management might find it more prudent to keep an infected system up and running, risking some additional damage in hopes of identifying the intruder or preventing bad press. The level of acceptable risk should be included in the advance planning stages so that this decision can be made quickly and decisively when the time comes.

If the team does shut down the affected portions of the system, all access to the affected areas should be denied. The company should change the passwords to these areas and attempt to sew up any holes in the system that the intruder exposed. Through audit trails and the logs recorded by the affected systems, the response team should be able to uncover the intruder's means of entry because any unusual patterns are detectable.

Further, the team should find and eliminate vulnerabilities exploited by the intruder. If malicious software was introduced, it should be copied (for evidentiary purposes) and then deleted. At this point, any patches or reconstruction programs should be applied to the system to correct holes. After the causes of the breach have been eliminated and any malicious code has been removed, the system can be returned to normal.

Breach Notification

In addition to taking proper actions to handle a breach, management must determine whether they are obligated to notify their customers of a security breach. For example, 46 states in the United States, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted security breach notification laws that typically require businesses to notify their customers of a breach involving personal information. Likewise, an increasing number of European countries are developing rules on data breach notification. Mexico and United Arab Emirates have mandatory breach notification laws, whereas Australia, Canada, and New Zealand allow for voluntary reporting of data breaches.

Although most jurisdictions' breach-notification laws contain similar provisions, they vary. Thus, management operating in multiple jurisdictions faces the difficulty of ensuring compliance with different notification laws. Therefore, before establishing new policies and practices, management should consult with legal counsel to identify what laws apply.

Recovery and Follow-Up

After management handles an incident, the affected systems should be returned to an operational level and monitored to ensure it is functioning on adequately.

After the computer network is up and running again, management should review the experience to determine how well the response plan worked and what changes could make the plan work more smoothly in the future.

Keeping a journal of the response activities provides management with tools to reflect on what worked and did not work during the restoration. The follow-up period is a good time to conduct a new risk analysis, revise security plans, and begin an investigation into the attacker. By spending some post-response time analyzing weaknesses in the security system, as well as the efficiency of the company's response to the security breach, management can better protect its computer network from future catastrophes.

Insurance for Cyber Risks

In recent years, insurers have begun offering coverage via specifically designed policies to address new forms of exposure in the information age. Today, an entity might be exposed to theft, damage or disclosure of data, denial of service attacks, theft of intellectual property, unauthorized access, loss of revenue, infringement of copyright and trademark, and the consequent damage to business reputation.

Often, cyber insurance is necessary because traditional comprehensive general liability policies and traditional errors and omissions policies generally do not cover Internet-related losses. Many businesses believe that their traditional business coverage will cover Internet-related incidents, or failing that, their Web host or ISP will cover damages caused by any cyber-attacks, but they are probably wrong. Unless the entity's insurance policy or Internet service level agreement specifically includes language addressing such risks, any damages will probably not be covered.

Coverage provided by cyber-insurance policies can include various types of coverage, including first-party coverage or third-party coverage. First-party coverage includes coverage against losses such as data destruction, extortion, theft, and hacking. Third-party coverage provides coverage when a company is sued. It covers the company if it is being sued for problems caused by technology product errors and omissions; the pilfering, public release, or misuse of sensitive or confidential information; the unwitting spread of disruptive viruses; hacker tampering to the information and advertising carried on websites; email-facilitated sexual harassment; and privacy infringement.

CONTRACT AND PROCUREMENT FRAUD

The procurement system is the collection of processes, procedures, and entities involved in purchasing goods and services by public or private entities. And because the primary objective of an effective procurement policy is to achieve the best value of money, it is important that procurement processes avoid incidences of fraud.

This section will address fraud in the procurement process, focusing on the following topics:

- Basics of contract law
- Methods of acquiring goods or services
- Phases in the contracting process
- Types of procurement fraud schemes
- Methods of preventing and detecting contract and procurement fraud

Basics of Contract Law

Entities purchase goods and services through contracts; therefore, it is helpful to understand the elements of a contract. Legal systems, however, deal with some of the basics of contract law differently. In fact, there are differences in the way that common law and civil legal systems deal with contract law. Despite such differences, this discussion provides a general overview of the basics of contract law, which are applicable in most situations.

Elements of a Contract

A *contract* is a mutual oral or written agreement under which two or more parties have undertaken an obligation to render performance. To be enforceable, a contract generally must contain the following elements:

- Lawful subject matter or objective
- Competent parties
- Intent to be legally bound
- Agreement
- Legal consideration
- Form permitted by law

Lawful Subject Matter or Objective

To be enforceable, the subject of the contract must not be contrary to law or public policy.

Competent Parties

The parties to the agreement must have the legal right or capacity to make a contract. This generally means that the individual parties must be of lawful age and that other entities are properly and legally organized.

Intent to Be Legally Bound

To be enforceable, the parties to a contract must intend to be legally bound.

Agreement

To form a contract, the parties involved must agree to what the contract covers and the main terms of the deal.

Generally, agreement is reached by one party's acceptance of the other party's offer. An *offer* is an expression to another person of a willingness to be legally bound to a legal obligation by the stated terms. An *acceptance* is an expression of agreement to an offer made by another party. Generally, to become effective, an acceptance must be communicated.

Legal Consideration

In common law, a contract will not be enforceable unless it is supported by *consideration*. Thus, in most cases, consideration is required for a contract to be enforceable in the United States and the United Kingdom; however, the doctrine of consideration is irrelevant in many jurisdictions, such as France, Germany, and China. In basic terms, to be supported by consideration, the parties to a contract must exchange something of value. Consideration may take the form of money, services, or circumscription of action, and it must provide some legal benefit or detriment to the parties involved.

Form Permitted by Law

To be enforceable, a contract must be in a form permitted by law. For example, some types of contracts must be in writing to be enforced.

Breach of Contract

A victim of procurement fraud might be able to recover fraud losses by bringing a breach of contract action. A breach of contract occurs when one party fails to perform, or announces that it does not intend to perform, without just cause. If a party breaches, the other party may sue for damages—the loss caused by the other party's failure to perform—or in some

instances, for specific performance (i.e., an order from the court compelling the defaulting party to perform).

Methods of Procurement

There are various contracting methods that a procuring entity might use to acquire goods or services. The choice of method generally depends on the complexity of the procurement. Procurement methods range from using a purchasing card (or p-card) for small-dollar, off-the-shelf items to a negotiated multi-million-dollar contract for financial computer terminals.

Although there are various methods of procurement, purchasers typically use processes that provide open and free competition.

Specifically, organizations often procure goods and services through the following means:

- Competitive bidding using sealed bids
- Contracting by negotiation
- Simplified acquisition procedures

Competitive Bidding Using Sealed Bids

One method of procurement is competitive bidding using sealed bids. This method employs competitive, sealed bids, containing price and terms, from prospective contractors to a procurement entity that awards the contract to the bidder with the best price and terms. This method of procurement is designed to place all bidders on a plane of equality, requiring prospective contractors to bid on the same terms and conditions.

A procuring entity typically uses sealed bidding when the following conditions are present:

- The entity's requirements are clear, accurate, and complete.
- The dollar value of the purchase is large enough to justify the resources needed to conduct a sealed bid.
- There is enough time to solicit, obtain, and evaluate the bids.
- The contract award will be made on the basis of price.
- It is not necessary to have discussions with the responding bidders.
- There is a reasonable expectation that the procuring entity will receive more than one sealed bid.

This type of competitive bidding process uses a solicitation document called an invitation for bid (IFB), which typically contains a purchase description, the conditions for purchase, all contractual terms, and the deadlines for submitting bids. IFBs are publicly solicited. This process reduces the opportunity for procurement fraud.

Contracting by Negotiation

An organization might obtain goods or services through contracting by negotiation, which is a method of procurement whereby the procuring entity secures a procurement agreement through discussion and bargaining with prospective contractors. There are two main methods of contracting by negotiation:

- Competitive negotiation using a request for proposals (RFPs) or a request for quotations (RFQs)
- Sole-source contracting

Competitive Negotiation

Competitive negotiation permits bargaining between the procuring entity and prospective contractors before the contract is awarded. Organizations use this process when cost is not the most important factor of evaluation, and typically when:

- Sealed bids are not appropriate.
- The procuring entity needs to conduct discussions with potential providers because of differences in laws, regulations, or business practices.
- The acquisition is complex or vague.
- The procuring entity cannot accurately determine the risks.
- There is a relatively long, drawn-out production time.
- The procuring entity is contracting for a production effort (and not a specific item for delivery).

In general, when engaging in competitive negotiation, procuring entities issue a document to solicit proposals from prospective contractors on how they intend to address the procuring entity's needs and price quotes for implementing their proposed solutions. After the procuring entity receives the proposals, it negotiates with prospective contractors. Typically, this method allows the potential contractors to revise their offers before the contract is awarded.

Competitive negotiation allows for more flexibility in awarding contracts than competitive bidding, but it is time consuming.

Sole-Source Contracting

Although most procurement transactions are conducted in a manner that provides open and free competition, one exception is sole-source contracting.

Sole-source contracting is a noncompetitive procurement process accomplished through the solicitation of only one source. Sole-source contracting does not require a bid or quotes, and a sole source purchase does not involve competition among prospective contractors. Therefore, this method does not provide for full and open competition.

In sole-source procurement, the purchasing entity can negotiate by having back-and-forth discussions with the vendor to agree upon technical approach and price.

Additionally, because sole-source contracting does not provide for full and open competition, organizations that use this form of procurement typically require justification for its use. For example, in the United States, the Federal Acquisition Regulation, the system of regulations that applies to the government's procurement of goods and services, provides the following seven reasons that can be invoked to justify sole-source contracting:

- Only one responsible source and no other supplies or services will satisfy agency requirements
- Unusual and compelling urgency
- Industrial mobilization; engineering, developmental, or research capability; or expert services
- International agreement
- Authorized or required by statute
- National security
- Public interest

Simplified Acquisition Procedures

Simplified acquisition procedures are designed to speed up the procurement process by minimizing applicable rules, and they are generally used to acquire small items or services. Typically, simplified acquisition procedures apply to purchases for goods or services valued at an amount that falls below predetermined monetary thresholds. For example, an organization's purchasing guidelines might provide: An employee may purchase needed work-related or administrative items from any vendor he wishes if the purchase does not exceed $250.

Simplified acquisition procedures offer a number of advantages over other methods of procurement, including simplicity, a reduced decision cycle, and lower administrative costs.

In general, simplified acquisition procedures might include any of the following contracting mechanisms:

- Charge accounts
- Purchasing cards
- Purchase orders
- Petty cash funds

Charge Accounts

Charge accounts are a simplified way for management to meet anticipated, repetitive needs for services and products from trusted suppliers. A *charge account* is a pre-arranged agreement with an organization that is signed before any business is conducted.

They allow management to order and pay for supplies and services from approved vendors several times a year. Therefore, these agreements simplify the purchasing process.

Purchasing Cards (P-Cards)

A *purchasing card* (*p-card*, *PCard*, or *corporate credit card*) is an organizational charge card that allows employees to purchase goods and services without using a traditional purchasing process. Entities use p-cards to streamline their purchasing process, which helps to reduce cost. Typically, p-cards will have guidelines and spending limits for employees who use them.

Purchase Orders

A *purchase order* is a commercial document issued from a buyer to a seller that represents the formal and final approval of a purchasing transaction between the purchaser and vendor. It is a formal request to deliver goods or services according to the agreed-upon terms and prices.

Purchase orders can be used to keep track of purchasing activities, to evaluate the goods or services provided by suppliers, and to determine if items are delivered on time.

Typically, a purchase order identifies:

- The vendor
- The goods or service the vendor will provide to the buyer

- The types, quantities, and agreed-upon prices for the goods or services
- The delivery dates and terms of deliveries
- Freight
- The terms of payment
- Any other obligations and conditions related to the purchase

Sending a purchase order to a seller constitutes a legal offer to buy products or services, and a purchase order becomes a binding contract when accepted by the seller.

Petty Cash Funds

A *petty cash fund* is an amount of cash that is kept entirely separate from an organization's general cash and is intended to be used for small, incidental purchases. Thus, petty cash funds provide a simple and economic method of making small cash purchases (e.g., postage dues and delivery fees).

Generally, one person, called the custodian or cashier, is responsible for controlling the petty cash fund and documenting the disbursements made from the fund.

Phases in the Procurement Process

Although there are various methods that a procuring entity might use to acquire goods or services, purchasers typically use bidding processes that provide open and free competition. This discussion examines the phases of procurement processes employing competitive bidding mechanisms.

To review, in competitive bidding using sealed bids, each bidder competes for a contract based on the bid specifications set forth by the purchasing company. Contractors, suppliers, or vendors submit confidential bids stating the price at which they will complete a proposed contract in accordance with the purchaser's bid specifications. Accordingly, competitive procurement processes require contractors to bid competitively on contracts, and they are designed to maximize the benefits of free and open competition.

Competitive bidding, however, can create a cutthroat environment that is conducive to fraud, and any advantage one bidder can gain over his competitors is valuable. Consequently, procurement through competitive bidding is susceptible to fraud.

For the purpose of fraud detection, procurement processes that employ competitive bidding mechanisms can be reduced to four basic stages:

1. The presolicitation phase
2. The solicitation phase
3. The bid evaluation and award phase
4. The post-award and administration phase

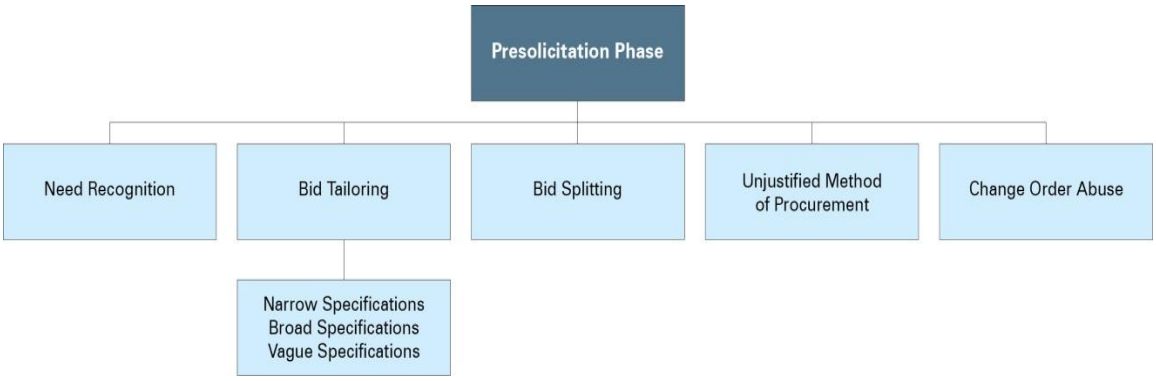
Fraud can occur in each of these phases, and the following discussion explaining the phases of procurement contains corresponding flowcharts showing the types of procurement fraud schemes that occur during each of them. The procurement fraud schemes used in the flowcharts are discussed in the "Categories of Procurement Fraud Schemes" section that follows.

The Presolicitation Phase

In the presolicitation phase, the procuring entity identifies its needs, develops the bid specifications (what, how much, and how good), determines the method to use for acquiring the goods or services, and develops the criteria used to award the contract.

Bid specifications are a list of elements, measurements, materials, characteristics, required functions, and other specific information detailing the goods and services that a procuring entity needs from a contractor.

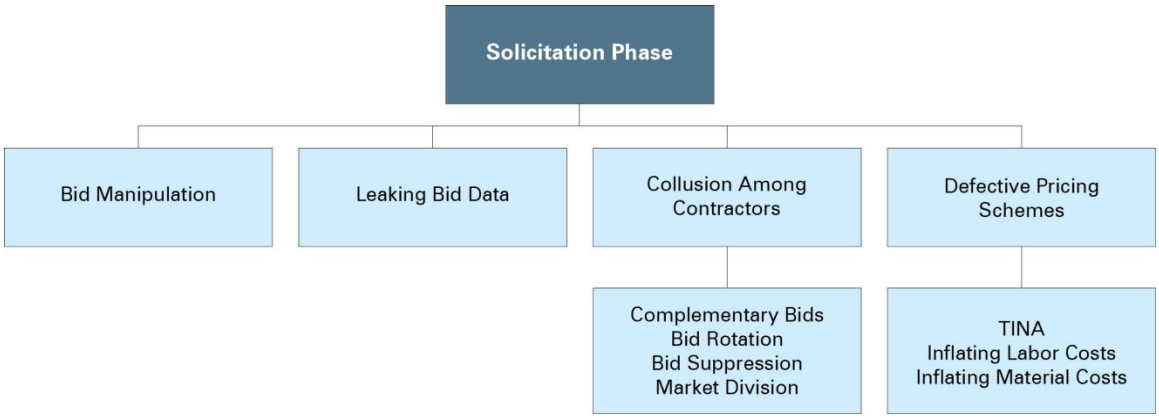
The following flowchart shows the types of procurement fraud schemes that occur during the presolicitation phase.



The Solicitation Phase

The solicitation phase involves the bid solicitation, bid preparation, and bid submission. During this phase, the procuring entity prepares the solicitation document, provides notices of solicitation, and issues the solicitation document. After the procuring entity issues the solicitation document, the bidders prepare and submit their bids or proposals.

The following flowchart shows the types of procurement fraud schemes that occur during the solicitation phase.



The Bid Evaluation and Award Phase

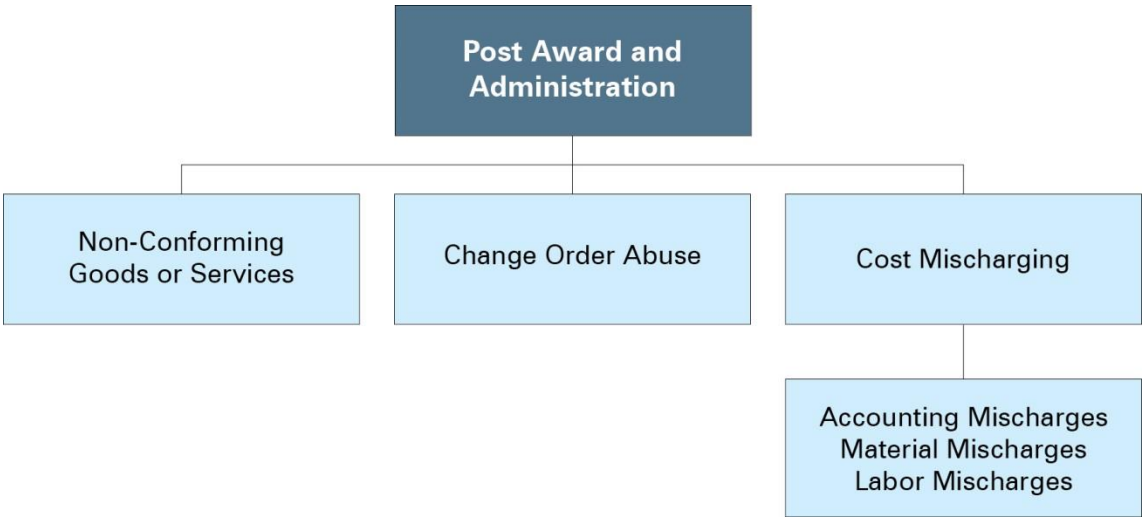
In the bid evaluation and award phase, the procuring employees evaluate the bids or proposals, conduct discussions and negotiations, and give the bidders an opportunity to revise their proposals. Procuring employees then select the winning bid or proposal.

The following flowchart shows the types of procurement fraud schemes that occur during the bid evaluation and award phase.

The Post-Award and Administration Phase

During the post-award and administration phase, the contracting parties fulfill their respective duties through the performance of their contractual obligations. Activities that occur during this phase include contract modifications (i.e., change orders); review of completed portions and release of monies; and assessment of deliverables for compliance with the contract terms, including quality control.

The following flowchart shows the types of procurement fraud schemes that occur during the post-award and administration phase.



Categories of Procurement Fraud Schemes

Although there are many types of procurement fraud schemes, a discussion of every different type is beyond the scope of this material. Instead, this discussion focuses on procurement fraud schemes that fall under the following categories:

- Schemes involving collusion among contractors
- Schemes involving collusion between contractors and procurement employees
- Defective pricing schemes in negotiated contracts
- Schemes in the post-award and administration phase

Collusion Among Contractors

Schemes involving collusion among contractors seek to circumvent the competitive bidding process. In these schemes, competitors in the same market collude to defeat competition or to inflate the prices of goods and services artificially. When competitors commit such

schemes, the procuring entity is cheated out of its right to the benefits of free and open competition.

The most common forms of collusion between competitors involve the following types of schemes:

- Complementary bidding
- Bid rotation
- Bid suppression
- Market division

Complementary Bidding

Complementary bidding (also known as *protective*, *shadow*, or *cover* bidding) occurs when competitors submit token bids that are not serious attempts to win the contract. Token bids give the appearance of genuine bidding, but, by submitting token bids, the conspirators can influence the contract price and who is awarded the contract.

Often, conspirators in complementary bidding schemes submit token bids that:

- Are too high to be accepted
- Appear to be competitive in price but deliberately fail to meet other requirements
- Contain special terms that will not be acceptable to the buyer

Bid Rotation

Bid rotation, also known as *bid pooling*, occurs when two or more contractors conspire to alternate the business among themselves on a rotating basis. Instead of engaging in competitive contracting, the bidders exchange information on contract solicitations to guarantee that each contractor will win a share of the purchasing entity's business.

EXAMPLE

Vendors Ace, Binko, and Cooper are up for three separate contracts, and they agree that Ace's bid will be the lowest on the first contract, Binko's bid will be the lowest on the second contract, and Cooper's bid will be the lowest on the third contract. None of the vendors will get all three jobs, but they are all guaranteed to get at least one. Furthermore, because they plan their bids ahead of time, they can conspire to raise their prices.

Additionally, bid rotation schemes might be coupled with a scheme involving an agreement that the winning bidder will award subcontracts to losing bidders. This allows losing bidders

to improve their cash flow as they wait for their turn to win. Similarly, losing bidders might receive a percentage of the winning company's profits.

Bid Suppression

Bid suppression occurs when two or more contractors enter into an illegal agreement whereby at least one of the conspirators refrains from bidding or withdraws a previously submitted bid. The goal of these schemes is to ensure that a particular competitor's bid is accepted.

Bid suppression schemes, however, can take on other forms. Because many schemes involving collusion among competitors require that a limited number of bidders agree to the conspiracy, price inflation should become apparent if a new or uncooperative bidder enters the competition. To prevent this, conspirators might pay off outside companies to refrain from bidding or withdraw an already submitted bid. Conspirators might also use more forceful means to discourage uncooperative entities from participating in the bidding process. For example, to protect their monopoly, conspirators might fabricate bid protests or coerce suppliers and subcontractors to avoid dealing with non-cooperating companies.

Market Division

Market division (or *market allocation*) schemes involve agreements among competitors to divide and allocate markets and to refrain from competing in each other's designated portion of the market. In these schemes, the competitors generally divide the markets according to geographic area (i.e., the competitors take turns on contracts according to the geographic area), or they make divisions based on the customer (i.e., the competitors allocate specific customers or types of customers among themselves).

The result of these schemes is that competing firms will not bid against each other, or they will submit only complementary bids when a solicitation for bids is made by a customer or in an area not assigned to them. The customer thereby loses the benefit of true competition and ends up paying a higher price than would be dictated by fair bidding under normal economic forces.

Corrupt contractors often conceal market division schemes by submitting bids from *shell companies* (i.e., companies that have no physical presence and generate little independent economic value). Submitting bids from fictitious entities gives the appearance of competition. Furthermore, the real contractor can raise his prices because the other bids are

fraudulent and are sure to be higher than his own. In effect, the bids from fictitious suppliers serve to validate the exaggerated quote from the winning contractor.

Red Flags of Schemes Involving Collusion Among Contractors

Common red flags of schemes involving collusion among contractors include:

- The industry has limited competition.
- The same contractors bid on each project or product.
- The winning bid appears too high.
- All contractors submit consistently high bids.
- Qualified contractors do not submit bids.
- The winning bidder subcontracts work to one or more losing bidders or to non-bidders.
- Bids appear to be complementary bids by companies unqualified to perform the work.
- Some bids fail to conform to the essential requirements of the solicitation documents (i.e., some bids do not comply with bid specifications).
- Some losing bids were poorly prepared.
- Fewer competitors than usual submit bids on a project or product.
- When a new contractor enters the competition, the bid prices begin to fall.
- There is a rotational pattern to winning bidders (e.g., geographical, customer, job, or type of work).
- There is evidence of collusion in the bids (e.g., bidders make the same mathematical or spelling errors; bids are prepared using the same typeface, handwriting, stationery, or envelope; or competitors submit identical bids).
- There is a pattern where the last party to bid wins the contract.
- There are patterns of conduct by bidders or their employees that suggest the possibility of collusion (e.g., competitors regularly socialize, hold meetings, visit each other's offices, subcontract with each other, and so on).

Collusion Between Contractors and Employees

Often, procurement fraud schemes involve collusion between contractors and the procuring entity's employees. The manner in which these schemes are perpetrated generally depends on the corrupt employee's level of influence. The more power a person has over the bidding process, the more likely it is that the person can influence which entity is awarded the contract. Therefore, procurement employees involved in procurement fraud schemes tend to have a good measure of influence on the competitive bidding process.

Various types of procurement employees are potential targets for corrupt contractors, including buyers, contracting officials, engineers and technical representatives, quality or product assurance representatives, subcontractor liaison employees, and anyone else with authority over the awarding of contracts.

Frequently, when a vendor bribes an employee of the purchasing organization to help him in a scheme, the cost of the bribe is included in the corrupt vendor's bid. Therefore, the purchasing company ends up bearing the cost of the illicit payment.

Procurement fraud schemes involving the purchasing entity's contractors and employees generally include the following:

- Need recognition
- Bid tailoring
- Bid manipulation
- Leaking bid data
- Bid splitting
- Unjustified sole-source awards or other noncompetitive methods of procurement

Need Recognition

Generally, procurement actions begin with the procuring entity making a determination of its general needs. These initial determinations include assessments of the types and amounts of goods or services required to meet the entity's needs. In need recognition schemes, a procurement employee convinces his employer that it needs excessive or unnecessary products or services. Accordingly, need recognition schemes occur in the presolicitation phase.

Often, in need recognition schemes, the purchasing entity employee receives a bribe or kickback for convincing his employer to recognize a need for a particular product or service. There are several red flags that might indicate a need recognition scheme. An organization with unusually high requirements for stock and inventory levels might reveal a situation in which a corrupt employee is seeking to justify unnecessary purchases from a certain supplier. Likewise, if an organization's materials are not being ordered at the optimal reorder point, this should raise a red flag. An employee might also justify unnecessary purchases of inventory by writing off large numbers of surplus items as scrap. As these items leave the inventory, they open up spaces to justify additional purchases. Another indicator of a need recognition scheme is a "need" that is defined in a way that can only be met by a certain

supplier or contractor. In addition, the failure to develop a satisfactory list of backup suppliers might reveal an unusually strong attachment to a primary supplier—an attachment that is explainable by the acceptance of bribes from that supplier.

Other common red flags of need recognition schemes include:

- The assessment of needs is not adequately or accurately developed.
- There is no list of backup suppliers for items, spare parts, and services continually purchased from a single source.
- Estimates are either not prepared or are prepared after solicitations are requested.
- Items, parts, and services are obtained from a single source.
- A suspect employee displays sudden wealth, pays down debts, or lives beyond his means.
- A suspect employee has an outside business.
- Multiple purchases are made that fall below the threshold limit.
- Purchases are made without receiving reports.

Bid Tailoring

Bid tailoring schemes (also known as specifications schemes) occur during the presolicitation phase. In these schemes, an employee with procurement responsibilities, often in collusion with a contractor, drafts bid specifications in a way that gives an unfair advantage to a certain contractor.

Again, *bid specifications* are a list of elements, measurements, materials, characteristics, required functions, and other specific information detailing the goods and services that a procuring entity needs from a contractor. Specifications assist prospective contractors in the bidding process, informing them what they are required to do and providing a firm basis for making bids, and they provide procurement officials with a firm basis for selecting bids.

There are three primary methods used to commit bid-tailoring schemes. One method involves drafting narrow specifications. In these schemes, a corrupt employee tailors the bid specifications to accommodate a vendor's capabilities and to eliminate other competitors so that the favored contractor is effectively guaranteed to win the contract. For instance, the tailored bid might require potential contractors to have a certain percentage of female or minority ownership. Such a requirement is not illegal, but if it is placed in the specifications as a result of a bribe, then the employee has sold his influence to benefit a dishonest vendor.

A second method involves drafting broad specifications. In these schemes, a corrupt employee of the buyer designs unduly broad qualification standards to qualify an otherwise unqualified contractor.

A third method involves drafting vague specifications. In these schemes, the buyer's personnel and the contractor collude to write vague specifications or intentionally omit bid specifications. This enables subsequent contract amendments, allowing the contractor to raise the contract's price.

Some common red flags of bid tailoring include:

- Weak controls over the bidding process
- Only one or a few bidders respond to bid requests
- Contract is not re-bid even though fewer than the minimum number of bids are received
- Similarity between specifications and winning contractor's product or services
- Bid specifications and statements of work are tailored to fit the products or capabilities of a single contractor
- Unusual or unreasonably narrow or broad specifications for the type of goods or services being procured
- Requests for bid submissions do not provide clear bid submission information (e.g., no clear time, place, or manner of submitting bids)
- Unexplained changes in contract specifications from previous proposals or similar items
- High number of competitive awards to one supplier
- Socialization or personal contacts among contracting personnel and bidders
- Specifications developed by or in consultation with a contractor who is permitted to compete in the procurement
- High number of change orders for one supplier

Bid Manipulation

In bid manipulation schemes, a procuring employee manipulates the bidding process to benefit a favored contractor or supplier. Thus, these schemes occur during the solicitation and evaluation phases.

In short, bid manipulation involves a fraudster who attempts to influence the selection of a contractor by restricting the pool of competitors from whom bids are sought. Therefore, in these schemes, a corrupt vendor persuades a purchasing company employee to ensure that

one or more of the vendor's competitors cannot bid on the contract, thereby improving that vendor's chances of winning the contract.

Some common ways to commit these schemes include:

- Using obscure publications to publish bid solicitations
- Publishing bid solicitations during holiday periods
- Accepting late bids or falsifying the bid log
- Altering bids
- Extending bid opening dates without justification
- Prematurely opening bids
- Releasing confidential information
- Discarding or losing a bid or proposal
- Disqualifying bids for improper reasons (e.g., voiding bids for alleged errors in specifications)
- Adding new vendors to the qualified bidder list for no apparent reason
- Limiting the time for submitting bids so that only those with advance information have adequate time to prepare bids or proposals

A variation of these schemes involves a corrupt sales representative who deals on behalf of a number of potential bidders. The sales representative bribes a contracting official to rig the solicitation process, ensuring that only those companies that he represents will get to submit bids. Likewise, in some sectors, it is not uncommon for buyers to "require" that bidders be represented by certain sales or manufacturing representatives. To protect their client's interest, these representatives might pay a kickback to the buyer. The result of such transactions is that the purchasing company is deprived of the ability to get the best price on its contract.

Some common red flags of bid manipulation schemes include:

- Weak controls over the bidding procedures are present.
- There is evidence of changes to bids after they were received.
- The winning bid is voided for errors and the job is re-bid or awarded to another contractor.
- An otherwise qualified bidder is disqualified for seemingly arbitrary, false, frivolous, or personal reasons.
- A procurement employee accepts late bids.
- The contract is awarded to a non-responsive bidder.

- Competing bids are lost.
- Bid deadlines are changed.
- Despite receiving fewer than the minimum number of bids, the contract is not re-bid.
- Invitations for bids are sent to unqualified contractors.
- Invitations for bids are sent to contractors that previously declined to bid.

Leaking Bid Data

Competitive bids are confidential. They are supposed to remain sealed until a specified date when all bids are opened and reviewed by the procuring entity. Accordingly, employees of a procuring entity can leak pre-bid information or confidential information from competing bidders to a favored bidder, giving that bidder an unfair advantage in the bidding process. Thus, in such schemes, the employee does not alter the specifications to suit the vendor; instead, he gives the favored vendor a head start on planning his bid and preparing for the job.

Typically, these schemes involve a corrupt vendor who pays a procurement employee for the right to see the specifications earlier than the competition. Consequently, the person or persons who have access to sealed bids are often the targets of unethical vendors seeking an advantage in the process.

EXAMPLE

Gifts and cash payments were given to a majority owner of a company in exchange for preferential treatment during the bidding process. The supplier who paid the bribes was allowed to see his competitors' bids and adjust his own bids accordingly.

Leaking schemes might also involve measures to restrict the time for submitting bids. Because leaking schemes give favored suppliers advance notice of contracts, they are able to develop their bids before their competition. And if a procurement employee also restricts the time for submitting bids, he will limit the period bidders have for developing bid proposals, and the supplier with advance knowledge will have an advantage over the competition.

Some common red flags of leaking bid data schemes include:

- The procuring entity has weak controls over its contracting system.
- The winning bid is just under the next lowest bid.
- The winning bid is unusually close to the procuring entity's estimates.
- The last party to bid wins the contract.

- The contract is unnecessarily re-bid.
- A contractor submits false documentation to get a late bid accepted.
- Contracting personnel provides information or advice about contracts to a contractor on a preferential basis.

Bid Splitting

In general, procuring entities must use competitive methods for projects over a certain amount. To avoid this requirement, a dishonest employee might break up a large project into several small projects that fall below the mandatory bidding level and award some or all of the component jobs to a contractor with whom he is conspiring.

Some common red flags of bid splitting schemes include:

- Two or more similar or identical procurements from the same supplier in amounts just under upper-level review or competitive-bidding limits
- Two or more consecutive related procurements from the same contractor that fall just below the competitive-bidding or upper-level review limits
- Unjustified split purchases that fall under the competitive-bidding or upper-level review limits
- Sequential purchases just under the upper-level review or competitive-bidding limits
- Sequential purchases under the upper-level review or competitive-bidding limits that are followed by change orders

Unjustified Sole-Source Awards or Other Noncompetitive Methods of Procurement

Noncompetitive methods of procurement, like sole-source contracting, exclude competition; therefore, such methods can be used improperly to eliminate competition and steer contracts to a particular vendor.

Again, sole-source contracting is a noncompetitive procurement process accomplished through the solicitation of only one source, thereby limiting full and open competition. Sole-source contracting is more vulnerable to fraud than competitive methods because it provides a greater freedom for manipulation and collusion with a vendor or contractor; consequently, procurement organizations typically require justification to use this form of procurement. Typically, justification occurs when the goods or services are available only from a single source, when exigent circumstances do not permit delay resulting from a competitive solicitation, or when solicitation is determined inadequate after soliciting a number of sources.

Additionally, in cases involving unjustified sole-source awards, the supplier typically charges a much higher price than the company could have obtained through bidding.

EXAMPLE

A requisitioner distorted the requirements of a contract up for bid, claiming the specifications called for a sole-source provider. Based on the requisitioner's information, competitive bidding was disregarded and the contract was awarded to a particular supplier. A review of other bids received at a later date showed that certain materials were available for up to $70,000 less than what the company paid in the sole-source arrangement. The employee had helped divert the job to the contractor in return for a promise of future employment.

Some common red flags of unjustified sole-source award schemes include:

- Frequent use of sole-source procurement contracts
- High number of sole-source awards to one supplier
- Requests for sole-source procurements when there is an available pool of contractors to compete for the contract
- Procuring entity did not keep accurate minutes of pre-bid meetings
- False statements made to justify noncompetitive method of procurement
- Justifications for noncompetitive method signed or approved by employees without authority
- Employee fails to obtain the required review for sole-source justifications
- Sole-source justifications developed by or in consultation with a contractor who is permitted to compete in the procurement

Defective Pricing Schemes in Negotiated Contracts

Defective pricing arises when contractors intentionally use inaccurate cost or pricing data to inflate costs in *negotiated contracts* (i.e., the contracting method that permits negotiations between the procuring entity and prospective contractors).

Defective pricing schemes are more limited than other forms of procurement fraud because they primarily occur in negotiated contracts. Typically, procuring entities use negotiated contracting when conditions are not appropriate for competitive, sealed bidding.

Generally, when engaging in negotiated contracting, contractors submit cost or pricing data. Examples of cost or pricing data include information such as vendor quotes or bids,

make/buy decisions, known upcoming production changes, already-bargained-for discounts, and so on. In negotiated contracts, contractors can submit defective pricing data to inflate the contract price. A contractor submits defective cost or pricing data when more current, more complete, or more accurate data existed, but was not disclosed to the procuring entity, resulting in an increase in the contract price.

However, it should be noted that not every instance of defective pricing is the result of the contractor's fraudulent behavior. In fact, defective data might be submitted for various non-fraudulent reasons, such as negligence, accident, incompetence, mistake, and so on.

Methods of Defective Pricing

A contractor can use various defective pricing schemes to increase the cost of the contract and thereby its profits, but generally, defective pricing schemes involve inflated labor costs or inflated material costs. A contractor can inflate labor costs by:

- Using outdated cost schedules
- Using lower-wage personnel to perform work at higher rates
- Using salaried personnel to perform uncompensated overtime
- Failing to account for learning-curve cost reductions
- Subcontracting to affiliated companies at inflated rates

A contractor can inflate material costs by:

- Failing to disclose discounts and credits
- Using outdated standard costs
- Using small-quantity costs to price large-quantity purchases
- Subcontracting to or purchasing from affiliated companies at inflated prices
- Failing to disclose residual materials inventory
- Using phantom suppliers to inflate costs
- Failing to disclose changes in "make or buy" decisions
- Estimating costs based on invalid cost allocation methods
- Using unsupported cost escalation factors

Red Flags of Defective Pricing Schemes

The following are general red flags that relate directly to defective pricing schemes:

- Contractor provides inadequate, inaccurate, or incomplete documentation to support cost proposals.

- Contractor is late in providing, delays providing, or cannot provide supporting cost or pricing data.
- Contractor's cost estimates are inconsistent with its prices (i.e., discrepancy between quoted prices and actual prices).
- Contractor uses out-of-date pricing information (e.g., outdated cost schedules) in cost proposals.
- Contractor fails to update cost or pricing data when past activity showed that costs or prices have decreased.
- Contractor fails to disclose internal documents on discounts, rebates, and so on.
- Contractor fails to disclose information regarding significant cost issues that reduce proposal costs.
- Contractor uses vendors or subcontractors during contract performance that are different from the ones named in the proposal or contract.
- Materials, supplies, or components that the contractor used in production are different than those listed in the proposal or contract.
- Contractor delays releasing information that could result in price reductions.
- Evidence of falsifications or alterations of documentation used to support cost calculations.
- Contractor has unrealistically high profit margins on completed work.
- Contractor fails to correct known system deficiencies that lead to defective pricing.
- Unqualified personnel developed cost or pricing data used in contractor's estimating process.

Performance Schemes

This discussion examines procurement fraud schemes that occur during the award and performance stage of the procurement process, including:

- Non-conforming goods or services schemes
- Change order abuse
- Cost mischarging schemes

Non-Conforming Goods or Services

Non-conforming goods or services fraud, also known as *product substitution* or *failure to meet contract specifications*, refers to attempts by contractors to deliver goods or services to the procuring entity that do not conform to the underlying contract specifications. Once the contractor delivers goods that do not conform to the contract, he bills and receives payment for conforming goods or services without informing the purchaser of the deficiency.

These schemes can involve a wide variety of conduct, but generally they include any deliberate departures from contract requirements to increase profits or comply with contract time schedules.

An unintentional failure to meet contract specifications is not fraud, but it might constitute a breach of contract. But a contractor who knowingly delivers goods or services that do not meet specifications might be guilty of fraud if he falsely represents that he has complied with the contract or deliberately conceals his failure to do so.

Often, contractors substitute goods or services delivered to the purchaser. Substitution is particularly attractive in contracts calling for expensive, high-grade materials that can be replaced by comparable, much less expensive products. Substitutions often involve component parts that are not easily detected.

Similarly, the potential for a product substitution case is greatest where the procuring entity relies on contractor integrity to ensure that it gets what it paid for.

This type of scheme can be committed by the contractor acting alone, or it can be facilitated by procurement or inspection personnel as the result of corruption. In non-conforming fraud schemes involving corruption, the dishonest supplier might give gifts or favors to inspectors or pay kickbacks to contracting officials to facilitate the scheme. The supplier would then submit false documentation to conceal it.

A contractor who repeatedly fails to meet contract specifications without corrective action by inspectors or the customer's supervisory staff might indicate corruption.

A wide variety of fraudulent schemes might involve non-conforming goods or services. Some examples include:

- Delivering or using products or materials of lesser quality than specified in the underlying contract
- Substituting products or items for those specified under the agreement
- Employing less qualified staff than specified in the contract
- Delivering or using counterfeit, defective, reworked, or used parts
- Delivering or using materials that have not been tested
- Falsifying the test results of materials, products, or goods

- Making false certifications (i.e., statements that parts or materials are new, domestically manufactured, and meet the contract specifications concerning quality and quantity, or that the company is minority owned)

RED FLAGS OF NON-CONFORMING GOODS OR SERVICES SCHEMES

The following is a list of potential red flags for non-conforming schemes:

- High percentage of returns for noncompliance with specifications
- Missing, altered, or modified product compliance certificate
- Compliance certificates signed by employees with no quality assurance responsibilities
- Materials testing done by supplier, using his own personnel and facilities
- Evidence that test or inspection results were falsified (e.g., documents appear altered or modified, test documents are illegible, signatures on documents are illegible, documents were signed by unqualified or inappropriate personnel, test reports are similar or identical to sample descriptions and test results, and so on)
- Highest profit product lines have the highest number of material return authorizations or reshipments
- Discrepancy between product's description or normal appearance and actual appearance (e.g., a new product appears to be used)
- Used, surplus, or reworked parts are delivered
- Delivery of products that appear counterfeit (e.g., product packaging, appearance, and description do not appear genuine, items that are consistently defaced in the same area, items that appear different from each other, and so on)
- Offers by contractors to select the sample and prepare it for testing
- Delivery of look-alike goods
- Unusually high number of early replacements
- Contractor restricts or avoids inspections of goods or services upon delivery

DETECTING NON-CONFORMING GOODS OR SERVICES SCHEMES

To detect non-conforming schemes, the fraud examiner should, at a minimum, examine the following for red flags:

- Contract or purchase order specifications
- Contractor's statements, claims, invoices, and supporting documents
- Received product
- Test and inspection results for the relevant period, searching for discrepancies between tests and inspection results and contract specifications

Additionally, to detect non-conforming schemes, the fraud examiner should:

- Review correspondence and contract files for indications of noncompliance.
- Request assistance from outside technical personnel to conduct after-the-fact tests.
- Inspect or test questioned goods or materials by examining packaging, appearance, and description to determine if the items are appropriate.
- Segregate and identify the source of the suspect goods or materials.
- Review inspection reports to determine whether the work performed and materials used in a project were inspected and considered acceptable.
- Review the contractor's books, payroll, and expense records to see if they incurred necessary costs to comply with contract specifications.
- Review the inspection and testing reports of questioned goods or materials.
- Conduct routine and unannounced inspections and tests of questioned goods or materials.
- Examine the contractor's books and manufacturing or purchase records for additional evidence, looking for discrepancies between claimed and actual costs, contractors, etc.
- Interview procurement personnel about the presence of any red flags or other indications of noncompliance.
- Search and review external records (e.g., court records, prior complaints, audit reports, investigative reports, media sources) to determine if there is any history of misconduct.

Change Order Abuse

A *change order* is a written agreement between the procuring entity and the contractor to make changes in a signed contract.

Change order abuse is a performance scheme that involves collusion between the contractor and personnel from the procuring entity. In change order abuses, a corrupt contractor submits a low bid to ensure that it wins the contract award, but, after the procuring entity awards the contract, the corrupt contractor increases their price with subsequent change orders. If successful, these schemes will, at the very least, cause the procuring entity to lose any advantage received through the competitive bidding process.

Similarly, a dishonest contractor, acting in collusion with contract personnel, can use the change order process to improperly extend or expand contracts and avoid re-bidding.

Change orders generally receive less scrutiny than the process used to acquire the underlying contract, making them a popular way to fraudulently access funds or generate funds for kickbacks.

Even though change orders are inevitable and can develop for various reasons (e.g., design error, ambiguous specifications or omissions in specifications, change in scope, weather delays, improvement in time or cost, building code changes, etc.), fraud examiners should view all contract change orders carefully.

RED FLAGS OF CHANGE ORDER ABUSE

When a change order occurs, fraud examiners should immediately be concerned about whether the change was accidental or planned. The following list of red flags can help make this determination.

- Poor contractor internal controls over determining the need for change orders (e.g., management officials fail to ensure that all proposed change orders are necessary for work that was not known or contemplated at the time the contract was awarded)
- Procurement employee acts outside his normal scope of duties
- Numerous change orders justified on a variety of grounds, including alleged change in prices, inflation, unavailability of specific materials or equipment, and the need to substitute more expensive alternatives
- Employee of procuring entity approves numerous unexplained or unjustified change orders for the same contractor
- Repeated pattern of change orders that increases the price, scope, or period of an agreement, issued after the procuring entity awards the contract
- Questionable, undocumented, or frequent change orders awarded to a particular contractor
- After contract is awarded, bid specifications that lack detail (the requirements are vague) are clarified by issuing a change order
- Poorly drafted requests for change orders
- Pattern of change orders just below threshold limit
- Employee of procuring entity who is directly involved in both determining requirements and procuring the item
- High turnover rate among procurement personnel
- Period of an agreement is extended by change orders instead of re-bidding

DETECTING CHANGE ORDER ABUSE

Fraud examiners can detect change order abuse by engaging in the following activities:

- Examine contract change orders that add new items.
- Examine contract change orders that increase the scope, quantity, or price of the existing contract.
- Analyze contract change orders for red flags.
- Interview complaining contractors, unsuccessful bidders, and procurement personnel about the presence of any red flags.
- Search and review external records (e.g., court records, prior complaints, audit reports, investigative reports, media sources, etc.) to determine if there is any history of misconduct.

Cost Mischarging Schemes

Cost mischarging schemes, which take place during the performance stage of the procurement process, occur when a contractor charges the procuring entity for costs that are not allowable, not reasonable, or cannot be allocated to the contract directly or indirectly.

Often, contractors contend that a cost mischarge was merely a mistake, and the issue as to whether a mischarge was a mistake or a crime often depends on the contractor's intent. Thus, when investigating cost mischarging schemes, fraud examiners should investigate the issue of intent.

Here are some common methods contractors use to mischarge costs:

- Charging the same cost to more than one contract
- Charging nonexistent costs or costs at inflated amounts
- Charging unallowable costs (e.g., entertainment or advertising) to the contract
- Charging costs to the wrong category or contract
- Failing to disclose discounts and credits
- Using outdated standard costs
- Colluding with contractors directly to charge high prices and rebating part of the price increase without disclosure
- Using phantom suppliers to inflate costs
- Falsifying supporting documentation

RED FLAGS OF COST MISCHARGING SCHEMES

Red flags of cost mischarging schemes include:

- Contractor refuses, delays, or is unable to provide complete supporting data.
- Contractor's supporting documents are missing or unavailable for review.
- Contractor's supporting documents are of poor quality.
- Contractor provides different supporting documents for the same item, and unit prices vary widely.
- There is evidence of falsifications or alterations to supporting data.
- Contractor fails to submit cost or pricing data that is current, accurate, and complete.
- Contractor fails to disclose internal documents on vendor discounts.
- Cost estimates are not consistent with contractor's prices.
- Repeated noncompliance with the contractor's disclosed bidding or estimating practices.
- Old, outdated standards used to support proposals.
- Contractor fails to disclose information regarding significant cost issues that will reduce proposal costs.
- Contractor uses unqualified personnel to develop cost or pricing data used in estimating process.
- Contractor uses vendors or subcontractors other than those listed in the proposal.
- Contractor repeatedly fails to disclose bidding or estimating practices.

THREE MAIN TYPES OF COST MISCHARGING SCHEMES

Generally, contractors commit one of three types of mischarges:

- Accounting mischarges
- Material mischarges
- Labor mischarges

ACCOUNTING MISCHARGES

Accounting mischarges occur when a contractor knowingly charges unallowable costs to the buyer by concealing or misrepresenting them as allowable costs, or by hiding them in accounts, such as office supplies, that are not usually closely audited. A variation of this type of scheme involves circumventing the limits for certain cost categories by charging those expenses to other cost categories that do not have such limits. For example, a contractor might charge bid and proposal costs or independent research and development costs, which are usually cost-based but limited to a fixed amount, to salaries and wages, repairs and maintenance, or other cost categories.

MATERIAL MISCHARGES

Occasionally, material costs are mischarged, both as to their reasonableness and their allocability. *Material* means physical inventory and component deliverables. It includes raw material and purchased parts, as well as subcontractor and intercompany transfers.

In most cases, material cost mischarging is confined to instances involving raw material or interchangeable parts. Mischarges of finished materials are infrequent because the nature of the items limits their use on other contracts. Similarly, mischarging of specialized material is infrequent because the special character of such items makes it impossible for them to go undetected.

Common methods used to mischarge material costs include:

- Charging material costs incurred on a fixed-price contract to a cost-type contract
- Applying inappropriate indirect rates to material costs
- Charging at standard rather than actual rates
- Making unrecorded transfers of materials to another contract
- Purchasing excessive materials on one contract and using them on another contract
- Purchasing materials from a subsidiary or affiliated company at inflated prices
- Manipulating inventory pricing methods to inflate material values
- Charging materials from inventory at current high prices rather than the actual lower purchase prices
- Using small quantity costs to price large quantity purchases
- Obtaining vendor quotes from high-priced suppliers and purchasing cheaper items elsewhere

Below is a list of red flags of material cost mischarging schemes:

- Previously delivered items are transferred from ongoing jobs to open work orders.
- Items scheduled for delivery in the distant future are transferred from ongoing jobs to open work orders.
- The contractor transfers items at costs that are substantially different (higher or lower) from actual costs.
- There are mass transfers of items from one job order to various other job orders.
- Materials, supplies, or components used in production are different than those used in the proposal or contract.
- The contractor includes unnecessary or obsolete items in proposals.

- The contractor charges costs to the original job order when there is no physical inventory left on the job site.
- There is an increase in transfers of items to inventory write-off or a scrap account.
- The contractor makes transfers to any type of holding account.
- The contractor does not properly account for the materials.
- There are initial billings for actual material costs in excess of negotiated costs.
- Later billings show a downward adjustment in material costs as labor or overhead costs increase.
- Improper billing costs become apparent.
- Vague terms are used to bid materials based solely on management's judgment or rough estimates.
- The contractor failed to report excess or residual inventory.
- The contractor gives poor explanations for a high percentage of non-competitive subcontractor awards.
- There is no clear audit trail to verify propriety of material charges.
- Internal controls over the shipping, receiving, and warehouse receipt for goods or services are weak.
- Weak internal controls allow numerous opportunities to adjust material charges.

Material mischarges can be detected by engaging in the following activities:

- Examine contract and cost files for red flags.
- Examine material cost transfers, which can include transfers:
  - From government contracts to commercial
  - Through any type of suspense or holding account
  - From ongoing jobs to jobs not scheduled for delivery until a much later date
  - From prior lot work orders to current or future work orders
  - To inventory write-off accounts
  - To scrap accounts
- Determine if contract costs have exceeded or are expected to exceed the contract value, because they should not be diverted to other cost objectives.
- Compare contract charges to determine if materials are properly charged to the job (too much or the wrong materials).
- Examine materials ordered and charged in excess of contract requirements.
- Examine seemingly unrelated materials charged on routing slips.
- Examine material standards not updated over periods when there are improvements in manufacturing technology or product design.

- Compare material costs over a specific period to identify any unusual changes and determine the reason for the changes.
- Review the standard and actual costs of materials to determine if any significant differences exist between the two.
- Investigate the contractor to determine ownership and search for any signs of corruption.
- Scan the general ledger, accounts receivable subsidiary ledger, and sales journal for unusual adjusting entries.

LABOR MISCHARGES

In the performance of contracts, labor costs are typically the most significant costs incurred, and they form the basis for estimating labor for future contracts.

Labor costs are made up of direct labor charges to the contract and indirect labor charges allocated to the contract through a factor or rate. *Direct labor charges* are contract costs identified specifically with a contract. In general, direct labor costs are calculated by multiplying all project hours with the labor rates, which are based on actual employee wages or represent wages paid, and they are summarized for all employees within the applicable allocation unit. Indirect labor costs are those identified in two or more cost objectives.

Labor mischarging occurs when the contractor charges the procuring entity for work that was not actually performed. Labor costs are perhaps more susceptible to mischarging than material costs because, unlike other items of cost, labor is not supported by external documentation or physical evidence to provide an independent check or balance, and employee labor can readily be charged to any contract. Moreover, the only way to ensure that labor costs are charged to the correct account is to actually observe each employee's work (to determine which contract they are working), and then review the accounting records to verify that the employee's cost is charged to the proper contract.

It should be noted that even though an incorrect labor charge might be an indicator of fraud, it might also be the result of poor business practices or weak internal controls.

Labor costs can be inflated by various means, including:

- Reporting inflated salaries and consulting fees
- Using outdated salary and fee schedules
- Charging lower rate personnel at higher rates

- Failing to account for learning-curve cost reductions
- Transferring labor costs from fixed-price contracts to cost-type contracts
- Falsifying the labor distribution
- Billing for the type of service performed rather than the actual employee hours spent performing the work
- Billing for employees' expenses that were not incurred
- Fictitious time cards
- Altering time cards

Common red flags of labor cost mischarging schemes include:

- Billings not in line with estimates
- Excessive or unusual labor charges
- Sudden, significant shifts in labor charge levels
- Labor charges inconsistent with contract progress
- Vague or minimal education, credential, and experience qualification requirements for labor hour contract positions
- Procuring entity personnel who do not review or challenge qualifications of key contractor employees
- Contractor has high employee turnover rate among procurement personnel
- Contractor must hire large numbers of personnel quickly
- Contractor personnel rarely take vacation
- Significant increases in charges to overhead accounts (e.g., idle time, down time, and non-applied time)
- Contractor with a mix of cost-type and fixed-price contracts
- Increased labor hours with no corresponding increases in material used or units shipped
- Actual hours and dollars consistently at or near budgeted amounts
- Labor standards not updated after contractor improves its manufacturing technology
- Unavailable supporting documentation for proposed standards
- Lost personnel files
- No audit trail to verify propriety of labor charges
- Weak internal controls that provide numerous opportunities to adjust labor charges

Labor mischarges can be detected by engaging in the following activities:

- Examine labor cost records for the presence of red flags.
- Review audit reports, reimbursement requests, construction reports, engineering reports, and so on.

- Conduct site visits to verify that selected employees' labor costs are being properly charged to the work actually being performed.
- Examine time cards and total the hours expended on the contract, comparing them to the hours billed.
- Note, in particular, repeated instances or a pattern of labor charges that increase the cost of cost-plus contracts.
- Review journal entries used to transfer labor costs.
- Compare labor costs over a specific period to identify any unusual changes and determine the reason for the changes.
- Review the standard and actual labor rates to determine if there are any significant differences between the two.
- Calculate the percentage of total direct labor charged to each contract to determine which had the highest percentage of direct labor charges.
- Review and compare the labor distribution summaries with payroll records to determine whether the total labor distributions agree with the total labor charges.
- Compare the direct and indirect labor account totals from the prior year to the current year and note the percentage change.
- Determine the percentage of total direct labor charged to each contract or work order to reveal which charge numbers had the highest percentage of direct labor charges.
- Analyze the labor charges to determine if there were any shifts in charging patterns.
- Prepare a schedule of salary or wage changes and compare it to contract award dates and labor rates.
- Look for terminated employees who are charged to contracts.
- Compare employee personnel records to contract position qualification requirements.
- Interview individuals who changed their charging patterns during the year.
- Search and review external records (e.g., court records, prior complaints, audit reports, investigative reports, media sources, etc.) to find any history of misconduct.

Preventing Contract and Procurement Fraud

Procurement schemes have certain characteristics that make them difficult to detect and prevent. This is partly because these schemes can take on various forms, can occur in any stage of the procurement process, and tend to take place over a long period. Adding to this difficulty is the fact that most perpetrators have specialized knowledge that allows them to exploit weaknesses in the procurement system, concealing most fraud indicators from anyone not involved in the acquisition process.

Nevertheless, management should take steps to prevent and detect procurement fraud. Generally, such efforts should include, among other things, the following elements:

- Employee education
- Internal controls
- Monitoring activities
- Vendor management

Employee Education

Management should educate their employees about procurement fraud, but generally, organizations should focus education efforts on employees who are in the best position to identify vulnerabilities or red flags of procurement fraud. In fact, there is no greater tool in the detection of procurement fraud than a network of employees who are knowledgeable about fraud and look for indicators of their organization's vulnerabilities.

Internal Controls

Management must also analyze their organization's internal controls and enhance them as necessary to eliminate procurement risks. Key internal controls include, but are not limited to:

- Separation of duties
- Supervisory controls
- Receiving controls
- Authorization/approval controls
- Reconciliation controls
- Recording controls

Monitoring Activities

It is important for management to implement a continuous, self-auditing program to measure the performance of its procurement activities. Today, organizations can use technologies to obtain insight into the effectiveness of internal controls, and these tools can help companies detect red flags and aid a company's management in its efforts to monitor and improve its internal controls, respond proactively to risks, and prioritize its compliance efforts.

Continuous monitoring uses data analytics on a continuous basis, thereby allowing management to identify and report fraudulent activity more rapidly. That is, data collected from continuous monitoring can help monitor procurement fraud threats and vulnerabilities,

detect red flags of procurement fraud, improve the effectiveness of anti-corruption controls, and, based on key risk indicators and high-risk areas, be used to prioritize and focus management's compliance efforts.

Vendor Management

All organizations rely on outside vendors to assist them in their business and, because vendors often perpetrate fraud against their customers in many ways, management should take steps to prevent and detect criminal conduct by its vendors.

Vendor management should include, among other things:

- Vendor background checks
- Controls for vendor master file management
- Vendor monitoring

Vendor Background Checks

Management must conduct adequate due diligence to identify and select competent and qualified vendors, such as reviewing the business reputation, financial soundness, and experience of the vendor.

Controls for Vendor Master File Management

Effective vendor management requires strong controls for vendor master file management.

The vendor master file is a database that contains a record of all vendors with whom a company conducts business. The vendor master file contains valuable records, including records for purchasing functions (e.g., vendor name and address, contact information, and purchasing terms) and accounts payable functions (e.g., the purchasing terms, remittance address, and general ledger account number). It also contains records regarding suppliers, for both purchasing and accounts payable functions. Mainly, the vendor's name and address, contact, and terms are needed when placing purchase orders, and the terms, remittance address, and general ledger account number are needed for tracking accounts payable invoices.

In most organizations, members of the purchasing department approve new vendors, and accounts payable personnel set up new vendors in the entity's accounting system.

To manage vendors, a procuring entity must establish clear procedures for setting up new vendors and changing vendor master file records. For example, procuring entities should require accounts payable personnel to verify new vendors (i.e., ensure that the vendors are qualified) by conducting a vendor background check before entering them into the vendor master file.

Also, the person responsible for the vendor master file should not be authorized to approve invoices for payment or to sign checks.

In addition, procurement entities must maintain accurate and up-to-date vendor master file records. Inaccurate or incomplete records can result in greater risks of duplicate payments, unfavorable payment terms, and noncompliance with regulations. Thus, vendor master file records should be reviewed on a regular basis for inaccurate or incomplete records.

Moreover, purchasing entities should monitor the application of the accounts payable policies on vendor master files.

Vendor Monitoring

Procuring entities must also use monitoring and auditing systems reasonably designed to detect criminal conduct by its vendors. The procedures to monitor vendors are similar to those used to evaluate vendors, and they should be based on red flags of vendor schemes that pose the greatest risk.

MENU

LAW

TABLE OF CONTENTS

THE LAW RELATED TO FRAUD (CONT.)

BANKRUPTCY (INSOLVENCY) FRAUD

BANKRUPTCY (INSOLVENCY) FRAUD (CONT.)

SECURITIES FRAUD

SECURITIES FRAUD (CONT.)

SECURITIES FRAUD (CONT.)

MONEY LAUNDERING

MONEY LAUNDERING (CONT.)

TAX FRAUD

TAX FRAUD (CONT.)

INDIVIDUAL RIGHTS DURING EXAMINATIONS

INDIVIDUAL RIGHTS DURING EXAMINATIONS (CONT.)

THE CRIMINAL JUSTICE SYSTEM

THE CRIMINAL JUSTICE SYSTEM (CONT.)

THE CIVIL JUSTICE SYSTEM

BASIC PRINCIPLES OF EVIDENCE

LAW

BASIC PRINCIPLES OF EVIDENCE (CONT.)

TESTIFYING

TESTIFYING (CONT.)

TESTIFYING (CONT.)

OVERVIEW OF THE LEGAL SYSTEM

Basic Concepts of the Law

By its nature, fraud examination is a law-intensive field. Legal issues related to fraud are often complex, and their interpretation might require professional legal assistance. The Certified Fraud Examiner always should consult with legal advisors if legal questions arise during a fraud examination.

Even with the availability of legal guidance, however, a fraud examiner should be familiar with certain aspects of the law. Often, the success of an investigation hinges on the fraud examiner following the proper legal procedures, whether dealing with a suspect's rights, collecting documents, or interviewing witnesses.

Both the structure and substance of the legal system in each jurisdiction can vary significantly, and so legal issues that arise in fraud examinations will also be different from place to place. The materials in the Law section of the *Fraud Examiners Manual* are designed to explain the common types of legal systems and approaches to fraud-related issues. White-collar crime often crosses jurisdictional borders, and so fraud examiners should be familiar with their home jurisdiction's legal processes, as well as have a basic understanding of the systems that they might encounter in foreign jurisdictions.

Types of Law

There are different types of law that are determinative to the outcome of legal disputes. The main types include constitutional law, statutory law, common law, administrative law, and international law.

Constitutional Law

Constitutional law is the body of law established by a sovereignty's constitution, and it deals with the fundamental principles by which a government exercises its authority.

Constitutions are government charters. They establish and empower the various branches of government, and they set up the rights and obligations of individuals under the government's jurisdiction.

U.S. CONSTITUTIONAL LAW

The U.S. Constitution and its accompanying amendments are the foundation of the legal system in the United States. The Constitution defines and limits the powers of the various branches of the government and guarantees basic rights to all citizens—rights such as equal protection under the law, due process, and the right to be free from unreasonable searches and seizures.

The Constitution is the supreme law of the land. The legislature may not properly pass, the executive branch may not enforce, nor may the judiciary uphold, any law or action that violates the provisions of the Constitution. There are special processes by which the federal legislature and a supermajority of the states can *amend* the Constitution, but they may not *violate* it.

The U.S. Constitution affords certain rights to individuals, and the constitutional rights that are of particular importance to Certified Fraud Examiners include those found in the Fourth, Fifth, and Sixth Amendments. The Fourth Amendment guarantees the right of all citizens to be free from unreasonable searches and seizures. This means that the government may not seize any records in a criminal case unless reasonable grounds exist—"probable cause"—to believe that the records would constitute evidence of a crime, and that a suspect may not be arrested unless there is probable cause to believe that he committed an offense. The Fifth Amendment guarantees subjects of a criminal investigation the right to refuse to answer questions or to provide certain personal information that might be incriminating. The Sixth Amendment affords subjects in a criminal investigation the right to counsel, the right to confront (cross-examine) the witnesses against them, and the right to a speedy trial.

Note that states have their own constitutions and rights under them. Often, state constitutions provide some of the same protections included in the U.S. Constitution. The states may offer additional protections beyond the U.S. Constitution, but the minimum protections of the latter may not be diminished by the states.

CANADIAN CONSTITUTIONAL LAW

The Canadian Constitution outlines Canada's system of government, provides the fundamental rules and principles that govern Canada, and sets out the civil rights of all individuals in Canada.

The Canadian Constitution protects individuals from certain actions, and some of the most relevant protections individuals may receive are set out in the Canadian Charter of Rights and Freedoms (Canadian Charter), which is part of the country's Constitution.

Among other things, the Canadian Charter guarantees everyone in Canada certain civil rights regarding the policies and actions of government. For instance, the Canadian Charter guarantees the right against self-incrimination, which provides that a suspect or an accused person has the right to remain silent both at the investigative stage and at the trial stage of criminal cases. Also, section ten of the Canadian Charter guarantees the right to counsel to individuals under arrest and detention. Additionally, section eight protects all individuals from unreasonable search and seizure.

Statutory Law

Statutory law is written law created by a legislature or other governing authority, and it includes statutes and codes passed by the local, regional, or national legislatures (and regulations passed by administrative bodies). In most jurisdictions, criminal law is based on statutes and codes.

Common Law

The common law consists of the usages and customs of a society as interpreted by the judiciary; it is often referred to as *judge-made* law. In most jurisdictions, civil actions can be based on either statutory or common law.

Administrative Law

Administrative law is concerned with the rules and procedures of administrative agencies of government. Administrative agencies have the authority to legislate, adjudicate, and enforce laws within their specific areas of delegated power. Typically, administrative agencies exist in the executive branch and are created and assigned specific tasks by the legislature. For example, the U.S. Congress has charged the federal Social Security Administration with the administration of the nation's Social Security program.

International Law

International law is the body of legal rules, regulations, and accepted practices observed by nations, and it defines nations' legal responsibilities in their conduct with each other and with private individuals and transnational companies. International law is enforced primarily through diplomacy and for reasons of courtesy or expediency.

Sources of international law include international conventions and treaties, international customs (i.e., international law that derive from custom), general principles of law recognized by the legal systems of civilized nations, the decisions of international and municipal courts, and the publications of scholars.

Substantive and Procedural Law

Law can be categorized as substantive or procedural law.

Substantive law defines the type of conduct permissible and the penalties for violation; it is composed of the basic laws of rights and duties. If someone says an act is "against the law," he is referring to substantive law.

Substantive law can be further subdivided into public and private law. *Public law* governs the relationship between individuals and the state; it involves such areas as: constitutional law, administrative law, and criminal law. *Private law* encompasses those areas where the legal system is used to resolve disputes between private parties. Examples of private laws are the laws concerning real property, contracts, civil wrongs (e.g., negligence), wills and estates, intellectual property, business organization law, and so on.

Procedural law defines the rules by which individual cases are decided; it sets out the rules of the legal system, including the procedures to be followed in hearing a grievance. Procedural law might include deadlines, filing requirements, steps to follow in bringing a claim, rules of evidence, and so on. Substantive law sets the terms of any dispute; procedural law dictates *how* a legal dispute is handled.

Types of Legal Systems

Despite the wide variety of legal systems—from the power structures of governments to the judicial processes—there are patterns of legal systems in certain countries that makes it easier to evaluate the legal process in each jurisdiction. These patterns arise due to a combination of factors, such as regional ties, former colonial influences, and international initiatives to conform laws to model standards.

Systems of Government

The most fundamental element to understanding a particular jurisdiction's legal system is to identify the structure of its government. To know the laws that apply to a case, it is necessary

to determine the system of government in the relevant jurisdictions. For example, suppose that a person in Montreal, Canada, has engaged in questionable banking transactions. Which laws would determine whether the conduct was fraudulent—the laws of the Canadian federal government, the laws of the provincial government of Quebec, local laws, or a combination? Additionally, what sources of law apply to determine the suspect's rights regarding a potential investigation? Understanding the system of government can help answer these questions.

There are various ways to classify systems of government, but one of the most helpful for understanding the laws of a particular jurisdiction is whether the system uses a federal or unitary power structure. Moreover, almost every modern-day government can be classified as being either unitary or federal in nature.

The majority of countries are *unitary systems*, meaning that a central government holds all governmental power within the nation. This central government may delegate power to created agencies and regional governments, but it remains the supreme governmental authority in the country. While delegated powers might include law-making authority, substantive laws regarding criminal misconduct, including most fraudulent acts, are typically directly legislated by the central government.

The other major structural system of government, the *federal system*, features both a national government (typically called the *federal government*), along with semi-autonomous regional governments (often called *states* or *provinces*). Unlike unitary systems, not all governmental powers are held by a central authority. Rather than being delegated powers, the state or provincial governments are reserved certain independent powers. The relative strength of state or provincial governments to that of their respective federal government varies from country to country, but normally the federal government has wider authority.

Federal and state or provincial governments are likely to share the space of fraud-related laws. For instance, a state or provincial government might prohibit embezzlement from any party within its jurisdiction, while the federal government has a separate law prohibiting embezzlement against national banks. The laws among states and provinces and the federal government also might differ. For example, one province might restrict pre-employment criminal background checks, but the other provinces and the federal government might not.

While not always the case, geographically large countries tend to be federations, such as Russia, Canada, the United States, Brazil, Australia, and India.

One government body that does not easily fit either a unitary or federal classification is the European Union (EU), which is made up of many countries that are generally considered autonomous. At the same time, the EU has considerable power to create mandatory directives for members to implement substantive and procedural laws. Each member institutes its own version of substantive laws required by the EU, so the laws of the relevant country are the primary determinant of legal issues in fraud cases occurring there.

Common Law and Civil Law Judicial Systems

In addition to classifying countries based on federal or unitary power structures, almost every country can be classified as having either a common law or a civil law judicial system, and knowing the differences between the two is essential to understanding how legal and judicial processes work in foreign jurisdictions. Both systems tend to adopt a certain method of fact-finding—adversarial or inquisitorial, respectively. Regardless of which type of legal system is used, most countries develop their own variation or incorporate other features into their systems.

Common Law Systems

In most *common law systems*, there are laws that judges develop through court decisions (called the common law), as well as codes and statutes that establish laws. As opposed to legislative statutes, the *common law* is developed on a case-by-case basis. Again, the common law is a system of legal principles developed by judges through decisions made in courts. It consists of the usages and customs of a society as interpreted by the judiciary, and it is often referred to as *judge-made* law. Common law originated as a legal system in England, and some of the principles established hundreds of years ago in court decisions remain influential to contemporary legal issues. Today, common law systems exist in the United Kingdom, the United States, India, Australia, and many other countries that were once part of the British Empire or were influenced by such legal systems.

In common law countries, there are two sources of substantive law: statutory law and common law. Again, *statutory law* includes *statutes* passed by legislatures (and regulations passed by administrative bodies).

In the modern era of law, the trend in common law countries has been to move away from rules that originate in common law and instead rely on statutory law—laws created by a legislature or other governing authority—as the basis of a dispute. For instance, almost all substantive federal laws in the United States are based on statutes or the U.S. Constitution.

However, an additional feature of the common law system that remains important is the precedential value of court decisions. Due to the ambiguity or incompleteness of statutes, legal disputes often arise in which parties support competing interpretations of a law. To decide disputes in common law systems, judges analyze prior cases with similar circumstances and apply the basic principles set forth in those cases to the problem at hand.

In common law systems, judges, particularly at the appellate level, often set out the reasons for their decisions in a written opinion, and these written decisions serve to guide judges in deciding cases of a similar nature. Decisions that establish particular legal principles are called *precedent*. Under the doctrine of *stare decisis*, lower courts are bound to follow the precedents of higher courts until or unless the rule of law established is overturned by a higher court or the legislature. The body of judicial opinions is sometimes referred to as *case law*.

If the legislature believes that a court's interpretation of a statute is incorrect, it may amend the statute to make it clearer.

The distinction between statutory law and common law is relevant to establishing the legal elements of a potential fraud in common law systems. Although criminal fraud statutes outlaw certain behavior, they often contain provisions that do not have any obvious connection to basic principles of right and wrong. Thus, fraud examiners preparing criminal cases must be familiar with the specific technical elements of the applicable statutes, and they must carefully review the evidence to make certain that all essential elements of proof are met.

In contrast to criminal fraud statutes, civil cases brought under the common law usually contain fewer technical elements and incorporate traditional principles of fairness and morality. For example, a plaintiff may file a common law claim for fraud by alleging simply that the defendant misrepresented important facts upon which the plaintiff relied, resulting in loss to the plaintiff.

Civil Law Systems

In contrast to common law systems, *civil law systems* apply laws from an accepted set of codified principles or compiled statutes. Individual cases are then decided in accordance with these basic tenets. Under a civil law system, the judges or judicial administrators are bound only by the civil code and not by the previous decisions of other courts. In deciding legal issues, a civil law judge applies the various codified principles to each case. However, *lacunae*—gaps in the law—are sometimes present, and judges may seek to fill in such gaps by looking to other authorities or similar laws, including judicial decisions.

Civil law and common law systems may exist within the same country. For example, in Canada, the legal system in the province of Quebec is not based on the British tradition of common law (as in the other provinces); instead, it is more influenced by the French and Roman civil law systems.

Although there are many differences between common law and civil law systems, they are not entirely different. Both systems contain many of the same basic principles. The main distinction between the two is that judges under common law systems are bound by precedent while judges under civil law systems are not; instead judges under civil law systems are bound by the civil code. Judges in civil law systems have to interpret the code, but they need not rely on previous cases in doing so. As a practical matter, however, most civil judges do consider previous decisions to guide their interpretations of the code.

Furthermore, much of the distinction between civil and common law systems is procedural—involving how the case will be decided. The substantive law outlined in this manual usually exists in some variation whether a civil or common law system is in place. For instance, the elements of the crime of embezzlement (intentionally and wrongfully stealing or converting the property of another that has been entrusted to the accused) are standard throughout most countries, regardless of whether the system is based on civil or common law.

Note that the concept of a *civil law system* should not be confused with the terms *civil law* and *criminal law*. *Civil law* is the body of law that provides remedies for violations of private rights, and a civil action is a legal action that does not result in a criminal fine or incarceration. A civil suit in this context has nothing to do with whether the legal system used by the particular government is a civil law jurisdiction or a common law jurisdiction. Most often, *civil* refers to a suit between two private parties. Conversely, *criminal law* is the body of law

pertaining to crimes against the state or conduct that harms society. Thus, in this context, *civil* is used to differentiate a civil action from a criminal action.

Adversarial and Inquisitorial Processes

Adversarial and *inquisitorial* judicial processes refer to the approach that courts take to discover evidence in a case. Theoretically, neither of these processes is exclusive of common law or civil law systems. Civil law jurisdictions, however, almost always favor an inquisitorial process, while common law systems typically feature an adversarial system. The United States, for example, is a common law jurisdiction with an adversarial process. Adversarial and inquisitorial techniques can also be employed in the same country under different circumstances.

ADVERSARIAL PROCESSES

Adversarial processes are those in which the parties to a proceeding drive the discovery process (the search for evidence). The theory behind this approach is that the competing interests of the parties will serve to expose the relevant facts of the case.

In adversarial systems, the parties to the litigation gather and present the evidence to the court. For example, the parties (usually through legal counsel) conduct questioning of fact and expert witnesses. The fact finder of the court, which can be a judge, jury, or administrator, is unaware of the details of the case until the parties present evidence. Judges facilitate the production of evidence between the parties, but generally do not seek evidence on the court's behalf.

One of the distinct features of the adversarial process is its approach to criminal procedure, where the rights of defendants are of paramount concern. Most adversarial court systems do not require defendants to testify. Also, defendants are given the presumption of innocence, which puts the burden of proof on the government to prove the criminal accusations.

INQUISITORIAL PROCESSES

An *inquisitorial* process refers to a fact-finding approach that places the primary responsibility of discovering evidence on the presiding judge.

In an inquisitorial process, the primary goal is to find the truth. Rather than serving as a referee over the parties' production of evidence, the judge is actively involved in discovery. For instance, judges may request relevant documents on their own accord and ask factual

questions of witnesses themselves. As a result, attorneys play a smaller role in the evidentiary process than in an adversarial process.

Criminal rights are generally less emphasized in inquisitorial trials than in adversarial systems; the former system focuses on getting to the truth of the matter. One of the most significant departures from the adversarial process is that defendants in criminal inquisitorial proceedings may be called to testify (whereas in adversarial systems, the defendant may testify, but does not have to do so). Note that civil (as opposed to criminal) proceedings under both adversarial and inquisitorial processes typically allow the defendant to be called to testify.

Furthermore, once the trial is underway, the presumption of innocence in inquisitorial processes is not generally as strong as in an adversarial, common law system. Instead, inquisitorial processes focus on not trying a person unless there is strong evidence to believe that the suspect is likely guilty.

ROLE OF JURIES

While juries can be found in both adversarial and inquisitorial jurisdictions, most adversarial jurisdictions actively use juries as the fact-finding body, while the judge decides issues of law. However, some cases in adversarial jurisdictions (often called *bench trials*) are decided factually and legally by a judge.

The judge in an inquisitorial process both serves as the traditional fact finder and makes determinations on issues of law. However, some inquisitorial systems use juries, laypersons, or a combination of judges (or legal professionals) and laypersons in serious cases.

International Issues in Fraud Cases

Fraud has never been a strictly domestic issue, but the digital age and the ease with which activity among parties of different countries is conducted have made fraud more of a global issue than ever before. Fraud cases involving assets or parties from diverse jurisdictions can lead to several legal issues of which fraud examiners should be aware.

Choice of Law

Which court has jurisdiction over an issue could depend on several factors, such as a party's presence in the jurisdiction where the court is located. A similar issue is that courts must

choose which jurisdiction's laws to apply to each issue in a case. Problems arise because the outcome of a case might depend on which jurisdiction's laws are applied. In other words, conduct that is fraudulent in one jurisdiction might be legal, carry different penalties, or result in different remedies in another jurisdiction.

In terms of procedural law, almost every court applies the procedural rules of its own jurisdiction (which includes choice-of-law rules). However, the way that courts choose substantive law is less consistent. Generally, most courts consider some mix of the following factors to determine which jurisdiction's laws apply:

- The nationality of the parties to the litigation
- The current residence of the parties (whether temporary or permanent)
- The parties' current or past physical presence in the relevant jurisdictions
- The jurisdiction where the transaction or underlying cause of action occurred

In addition, when a dispute involves real property, the laws of the country where the property is located usually apply to resolve questions of ownership.

Enforcement of Judgments

After a fraud is discovered, fraud examiners might need to assist in making a recommendation concerning the recovery of lost assets. In cases involving suspects in foreign jurisdictions, this task can be complicated by the ability to obtain and enforce a judgment against a particular defendant. For instance, a domestic judgment against a foreign defendant is usually helpful for recovering the defendant's assets located in the domestic country, but might be worthless for obtaining the defendant's assets in a foreign country.

Some, but not all, countries enforce foreign judgments concerning parties or assets within their jurisdiction. Whether the country will enforce a foreign court's judgment usually depends on the circumstances in which the internal laws of the jurisdiction recognize foreign judgments and whether the two countries of each court have an enforcement treaty.

Alternatively, a fraud victim could seek to obtain a judgment against a foreign suspect in the suspect's home country. The cost and feasibility of this endeavor can vary widely. Therefore, whether an enforcement action against a foreign defendant is sought is a legal issue, and fraud examiners should consult legal counsel in making a recommendation.

Court Systems

Countries have different types of court systems. Many courts follow a tiered court system in which there are trial courts and appellate courts. In such systems, the trial court conducts the trial and issues a judgment. Then, the lower level appellate courts review the trial court's rulings and procedures and issue a decision. The lower level appellate court's ruling is then subject to review by subsequent levels of appellate review.

Courts are defined by their jurisdiction and venue. *Jurisdiction* is the power of a court to hear and decide a given case; it refers to both the subject matter and people over which lawful authority may be exercised by a court. For instance, a country might have a system of probate courts that only have jurisdiction to hear cases whose subject matter is related to wills, inheritance, and other probate matters. Some countries have low-level trial courts that only have jurisdiction to hear matters under a certain monetary amount. Similarly, a court's jurisdiction is defined by the parties that it may hear a case about. For example, courts usually do not have jurisdiction over foreign parties who have never been to and have had no business or presence in the court's jurisdiction.

Venue refers to the geographical area covered by the court; it is the physical location where the lawsuit is to be tried. Venue is technically an element of the court's jurisdiction. This issue may be important in deciding where to file charges or claims.

A particular court's jurisdiction is defined by the laws of its jurisdiction, but generally, there are three common elements to consider when determining whether a given court has the power to hear and determine a case. First, does the court hear cases of the type in question? For example, if a plaintiff brings a civil complaint claiming $500,000 in damages, the plaintiff needs a court that hears civil complaints of that magnitude.

Second, does the court have the authority to exercise its power over a particular defendant or piece of property? This element usually requires the party to have some sort of current or past presence or activity within the jurisdiction.

Third, most jurisdictions require the court to have proper venue as an element of jurisdiction. Rules of venue can be based on a mixture of factors, including convenience to the parties (e.g., where they reside) and where the acts that underlie the case occurred. In some instances, there will be multiple courts that have jurisdiction over a case, and the

parties that believe they are subject to prejudice in a court will seek to change the venue to a court more favorable to themselves.

Civil and Criminal Actions for Fraud

Fraud may be prosecuted criminally, civilly, or both, in sequence or simultaneously, but there are a number of differences between criminal and civil actions with which the Certified Fraud Examiner should be familiar. The following is a brief overview of the civil and criminal actions as they relate to fraud.

Criminal Actions

A *criminal action* is a complaint brought by the government, acting on behalf of citizens and the interest of the jurisdiction, against a person accused of violating a law. Increasingly, most criminal offenses are codified in statutes or regulations.

Typically, to be guilty of a crime, a defendant must be found to have committed an offending act (called the *actus reus*) and to have the requisite culpable mental state when he committed the act (called the *mens rea*). The actus reus may involve the full act of committing a crime or merely the initial steps for crimes of attempt. Different offenses require different levels of mens rea, such as actual intent, recklessness, or, in some circumstances, no more than gross negligence.

Some criminal offenses, however, are strict liability offenses, which are offenses in which the government does not have to prove the defendant's intent.

Criminal cases are punished by outcomes such as imprisonment, fines, orders of restitution, probation, and community service.

Civil Actions

A *civil action*, as opposed to a criminal action, is an action for wrongdoing that does not result in a criminal fine or incarceration. In contrast to criminal actions, which are brought by the government, civil actions may be brought by private individuals or organization, usually without the involvement or permission of the government or court. However, government entities may also bring civil actions to pursue noncriminal remedies against other parties. Civil actions, if successful, result in an award of civil remedies.

There are a variety of substantive civil causes of action, but the two main causes that fraud examiners are likely to come across are contract actions and civil wrongs (or delicts).

Contract Actions

Contract actions are civil actions based on contract obligations. A *contract* is an oral or written mutual agreement between two or more individuals or entities that the law will enforce in some way.

Most contract actions are breach of contract lawsuits. A *breach of contract* occurs when one or both parties fail to perform, or announce that they do not intend to perform, without just cause. If a party breaches, the other party may sue for damages—the loss caused by the other party's failure to perform—or, in some instances, for specific performance (i.e., an order from the court compelling the defaulting party to perform).

Civil Wrong and Delict Actions

In common law jurisdictions, a *civil wrong* is a private wrong, such as fraud, that does not arise out of contractual obligations.

In civil law jurisdictions, the equivalent of a civil wrong is often called a delict. A *delict* is a culpable, wrongful act that causes injuries and results in liability for the person who committed the act.

To successfully bring a civil wrong or delict action, there are generally three requirements:

- A party must owe a duty to another party.
- The party that owes the duty breaches that duty.
- The breach results in losses.

A person who suffers a civil wrong is entitled to receive compensation for damages from the party responsible for the act.

THE LAW RELATED TO FRAUD

Definition of *Fraud*

Black's Law Dictionary defines *fraud* as:

> *all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprise, trick, cunning or dissembling, and any unfair way by which another is cheated.*

Put more succinctly, fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.

Principal Types of Fraud

The principal categories of fraud (also known as *white-collar crime*) are:

- Fraudulent misrepresentation of material facts (or false pretenses)
- Negligent misrepresentation
- Concealment of material facts
- Bribery
- Illegal gratuity
- Economic extortion
- Conflicts of interest
- Forgery
- Theft of money or property
- Breach of contract
- Breach of fiduciary duty
- Gross negligence
- Conspiracy
- Obstruction of justice
- Perjury
- False claims and statements to government agencies

Fraudulent Misrepresentation of Material Facts

Fraudulent misrepresentation of material facts is most often thought of when the term *fraud* is used. Misrepresentation cases can be prosecuted criminally or civilly. The gist of the

offense is the deliberate making of false statements to induce the intended victim to part with money or property.

The specific elements of proof required to establish a misrepresentation claim vary somewhat according to where the fraud occurred and whether the case is brought as a criminal or civil action, but the elements normally include:

- The defendant made a false statement (i.e., a misrepresentation of fact).
- The false statement was *material* (i.e., the statement was sufficiently important or relevant to influence the making of a decision).
- The defendant knew the representation was false.
- The victim relied on the misrepresentation.
- The victim suffered damages as a result of the misrepresentation.

Although it might be necessary to prove that the victim relied upon the false statements and actually suffered a loss in a civil case, these elements of proof might not be necessary in a criminal prosecution. In addition, in some statutes, materiality is assumed and need not be proved.

Normally, only material false statements may serve as the basis for a misrepresentation of material facts case. *Materiality* usually refers to statements sufficiently important or relevant to a reasonable person in acting or making a decision. For example, a claim that a company enjoyed a 50 percent growth in profits would probably be material to a prospective investor, whereas a statement that the company was considering moving its headquarters from Toronto to New York City might not be. The materiality of allegedly false statements often is a central issue in security fraud cases.

Moreover, in most instances, only false representations of "presently existing facts" can establish liability for misrepresentation claims. That is, opinions by nonexperts, speculative statements about future events, and other general assertions, even if made with the intent to mislead, may not provide the basis for a misrepresentation claim because such statements are not material facts. For example, a used car salesperson who assures a customer that a 20-year-old car, which was towed into the lot, will give the customer "years of driving pleasure" probably cannot be held liable for misrepresentation. The salesperson, however, could be liable if he tells the customer that the car has been driven only 15,000 miles but knows that it has been driven 150,000 miles.

The general rule that opinions or speculative statements cannot give rise to a successful misrepresentation claim is often applied to prevent fraud claims in contract disputes. A party to a contract who promises to perform certain services by a particular date but fails to do so generally may not be prosecuted for fraud unless the plaintiff can demonstrate that the defendant had the intent not to perform the promised services when the contract was made. Of course, the other party may file an action for breach of contract.

Also, the general rule precluding fraud actions based on opinions or speculative statements is subject to certain exceptions, principally cases involving opinions provided by professional advisers such as Certified Public Accountants. That is, a person who holds himself out as having special expertise on which another party reasonably relies may be liable for a false opinion that is within that area of special expertise. For example, an independent accountant may be liable for misrepresentation if he does any of the following:

- Certifies that a financial statement fairly presents the financial condition of the audited company when he knows it does not
- Falsely states that the audit was conducted in accordance with generally accepted accounting principles
- Deliberately distorts the audit results

In almost all fraud cases, the party alleging fraud must prove that a false statement was intentional and part of a deliberate scheme to defraud. A person intentionally makes a false statement if it is his desire to cause the social harm, or if he acts with knowledge that the social harm will almost certainly result from his actions. In some instances, particularly those involving civil actions for fraud and securities cases, the intent requirement is met if the party alleging fraud is able to show that the false statements were made *recklessly*; that is, with complete disregard for truth or falsity.

Moreover, there is no such thing as an accidental or negligent fraud. For example, mistakenly entering incorrect numbers on a financial statement is not fraud; however, knowingly entering incorrect numbers with the intent that someone will take action in reliance on them is fraud if the other elements are present.

Negligent Misrepresentation

Although a misrepresentation fraud case may not be based on negligent or accidental misrepresentations, in some instances, civil liability may arise from negligent misrepresentation. Negligent misrepresentation occurs in situations where there is a special

relationship that imposes a duty on the defendant to provide correct information to the plaintiff.

Generally, the specific elements required to establish a negligent misrepresentation claim are as follows:

- The defendant made a misrepresentation of a material fact.
- The misrepresentation was made pursuant to a special relationship that imposed a duty on the defendant to provide correct information.
- The defendant had no reasonable basis to believe the misrepresentation to be true.
- The victim relied on the misrepresentation, and the reliance was reasonable.
- The victim suffered damages as a result.

The main difference between fraudulent misrepresentation and negligent misrepresentation is that fraudulent misrepresentation requires that the statements be made intentionally and as a part of a deliberate scheme to defraud, whereas negligent misrepresentation only requires that the statement was made while having no reasonable basis to believe it to be true.

This civil action is appropriate if a party suffered a loss because of the carelessness or negligence of another party upon which the first party was entitled to rely. For example, a false statement regarding the value of a closely held company's stock that is negligently made to a prospective purchaser could give rise to a misrepresentation claim. Similarly, a false statement regarding the accuracy of a company's financial statements that is negligently made to a prospective purchaser could also give rise to this type of claim.

Concealment of Material Facts

An action for fraud may be based on the concealment of material facts, but only if the defendant had a duty in the circumstances to disclose. The essential elements of fraud based on failure to disclose material facts are:

- The defendant had knowledge of a material fact.
- The defendant had a duty to disclose the material fact.
- The defendant failed to disclose the material fact.
- The defendant acted with intent to mislead or deceive the victim(s).

The duty to disclose usually depends on the relationship between the parties. Those people who occupy a special relationship of trust, such as the officers or directors of a corporation, a lawyer, accountant, trustee, stockbroker, or other agent, may be found to have a duty to

completely disclose material facts to the parties who rely upon them. Statutes might expand the duty to disclose to areas in which traditionally there was no such duty, such as to the sellers of personal or real property or to the purchasers or sellers of securities.

Proof that the concealed fact was material is probably the most important element in a concealment case; there can be no liability if the withheld information was not material (i.e., the information would not have affected the other party's actions or decisions).

Also, it is not necessary to prove that the defendant knew for certain that the victim would be harmed. It is only necessary to prove that he intended to mislead or deceive the victim.

In addition to being liable for fraudulent concealment, a defendant might be liable for negligent failure to discover and disclose material facts. An accountant, for example, might be liable for failure to discover or report material facts in a financial statement or audit. Of course, as with negligent misrepresentation, the penalties are less severe for negligent concealment than fraudulent concealment, and there is no criminal liability for negligent concealment.

Bribery

Bribery is a form of corruption that may be defined as the offering, giving, receiving, or soliciting of anything of value to influence an act or a decision.

Types of Bribery Schemes

Bribery schemes are classified into two types: official bribery and commercial bribery.

OFFICIAL BRIBERY

Official bribery refers to the corruption of a public official to influence an official act of government. Illegal payments to public officials can be prosecuted as official bribery, and they can give rise to stiff penalties. The elements of official bribery vary by jurisdiction, but generally include:

- The defendant gave or received (offered or solicited) a thing of value.
- The recipient was (or was selected to be) a public official.
- The defendant acted with corrupt intent.
- The defendant's scheme was designed to influence an official act or duty of the recipient.

COMMERCIAL BRIBERY

In contrast, *commercial bribery* refers to the corruption of a private individual to gain a commercial or business advantage. That is, in commercial bribery schemes, something of value is offered to influence a business decision rather than an official act. In some countries, commercial bribery might be referred to as *secret commissions*.

Commercial bribery may not be a crime in every jurisdiction. For example, in the United States, there is no federal statute that prohibits commercial bribery, but many states outlaw the practice. Canada and the United Kingdom, however, do criminalize commercial bribery. If a jurisdiction does not have a commercial bribery statute, it may still prosecute commercial bribery schemes under other fraud statutes on the theory that the payment of a commercial bribe defrauds the business owner of the right to an employee's unbiased and loyal services.

The elements of commercial bribery vary by jurisdiction, but typically include:

- The defendant gave or received a thing of value.
- The defendant acted with corrupt intent.
- The defendant's scheme was designed to influence the recipient's action in a business decision.
- The defendant acted without the victim's knowledge or consent.

Commercial bribery requires a lack of knowledge or consent on the principal's part, and the "without the knowledge or consent of the principal" element is included on the theory that a private business owner is not defrauded if the owner knows of or allows employees to accept gifts, favors, or other payments from vendors or other business contacts.

Methods of Making Corrupt Payments

To establish a bribery claim, the party bringing the action must prove that the defendant offered a thing of value, and generally, the item of value element necessary to establish a bribery scheme is defined broadly. That is, in bribery schemes, the *thing of value* is not limited to cash or money. Any tangible benefit given or received with the intent to corruptly influence the recipient may constitute an illegal payment. Courts have held that such things as lavish gifts and entertainment, payment of vacation travel and lodging expenses, payment of credit card bills, loans, promises of future employment, and interests in businesses, can be bribes if they were given or received with the intent to influence or be influenced.

Corrupt Influence

To establish a bribery claim, the party bringing the action must prove that the defendant acted with corrupt influence. Proof of corrupt influence often involves demonstrating that the person receiving the bribe favored the bribe-payer in some improper or unusual way. For example, corrupt influence often is established by showing that the person receiving the bribe:

- Provided preferential treatment to the bribe-payer
- Bent or broke the rules
- Took extraordinary steps to assist the bribe-payer
- Allowed the bribe-payer to defraud the agency or company

Although, to prove corrupt influence, it is not necessary that the prosecution or plaintiff demonstrate that the bribe-taker acted improperly; a bribe might be paid to induce an official to perform an act that otherwise would be legal, or an act that the official might have performed without a bribe. Bribery schemes involving these circumstances, however, are difficult to prove and lack appeal for prosecution.

Illegal Gratuity

Illegal gratuities are items of value given to reward a decision, often after the recipient has made the decision. Illegal gratuities are similar to official bribery schemes, and most illegal gratuity laws outlaw gratuities in the public sector.

In general, the elements of an illegal gratuity are:

- A thing of value
- Given, offered, or promised to (or demanded, sought, received, or accepted by)
- A (present, former, or future) public official
- For or because of any official act performed or to be performed by such public official

The major difference between an official bribe and an illegal gratuity is that an illegal gratuity charge does not require proof that the gratuity was given for the purpose of influencing an official act. That is, an illegal gratuity charge only requires that the gratuity be given for, or because of, an official act.

In the typical illegal gratuities scenario, a decision is made that happens to benefit a certain person or company. The party who benefited from the decision then gives a gift to the

person who made the decision. The gifts are merely offered as a "thank you" for something that has been done.

Economic Extortion

An extortion case is often the flip side of a bribery case. *Extortion* is defined as the obtaining of property from another with the other party's "consent" having been induced by wrongful use of actual or threatened force or fear. Fear might include the apprehension of possible economic damage or loss. A demand for a bribe or kickback, coupled with a threat of adverse action if the payment is not paid, also might constitute extortion.

Generally, extortion is not a defense to bribery. That is, a person who makes a bribe payment upon demand of the recipient still is culpable for bribery. In New York, however, extortion may be a defense in certain circumstances.

Conflicts of Interest

A *conflict of interest* occurs when an employee or *agent*—someone who is authorized to act on behalf of a principal—has an undisclosed personal or economic interest in a matter that could influence his professional role. It encompasses a conflict between the professional duties and the private interest of an employee or agent, in which the employee or agent's private interest could improperly influence the performance of his professional duties and responsibilities.

Conflicts of interest involve a state of opposition between an individual's personal and professional interests, and they can occur in various ways. For example, a conflict may occur when a procurement employee accepts inappropriate gifts, favors, or kickbacks from vendors, or when an employee engages in unapproved employment discussions with current or prospective contractors or suppliers.

Statutes (in some cases) or common law prohibit people from engaging in conduct that involves a conflict of interest.

Elements of a typical civil claim for conflict of interest include:

- The defendant is an agent of a principal or employer.
- The agent takes an interest in a transaction.

- The agent's interest is actually or potentially adverse to the principal (i.e., the interest is one that could cause the agent or employee to place his personal interests ahead of the principal or employer).
- The agent did not disclose the interest and obtain approval by the principal.

Conflicts of interest do not necessarily constitute legal violations, as long as they are properly disclosed. Thus, for a conflict of interest claim to be actionable, the conflict must be undisclosed.

Conflicts of interest occur in principal-agent relationships. A principal-agent relationship is an arrangement in which one person (the "agent") is authorized to make decisions on behalf of another person or entity (the "principal"). Common principal-agent relationships include principal and agent, employer and employee, principal and independent contractor, client and attorney, client and accountant, property owner and real estate agent, and the public and government official.

Trust is central to the principal-agent relationship, and conflicts of interest exist when there is an incompatibility between an agent's personal interest and his duties and responsibilities in serving his principal.

An *agent* is any person who, under the law, owes a duty of loyalty to another. Officers, directors, employees, public officials, trustees, brokers, independent contractors, lawyers, and accountants all function as agents. People who do not occupy positions of trust with another party, such as arm's-length commercial parties, are not subject to conflict of interest restrictions.

A *principal* is an entity that authorizes an agent to act on its behalf. In a principal-agent relationship, the agent acts on behalf of the principal, and the agent should not have a conflict of interest in carrying out the act on behalf of the principal.

All of the following situations might give rise to a conflict of interest claim:

- An employer's interests are directly or indirectly affected or likely to be affected in some negative way by the private actions of an employee.
- The private actions of employees impair their ability to pursue the interests of their employers.
- The private actions of employees compromise their employer's business interests.

- The private actions of employees leave them in a position of gain or potential gain at the expense of their employer.
- Employees use knowledge or information learned through their employment to pursue their own private interests.

If the defendant in a civil conflict of interest case is found liable, he may be ordered to repay any losses that the conflict caused and "disgorge" any profits he earned because of the conflict, even if there was no actual loss to the principal. The "disloyal" party also might be required to forfeit all compensation received during the period of disloyalty. The victim of a conflict of interest also may void any contracts entered into on its behalf that were the result of or influenced by the conflict.

Forgery

A *forgery* is any writing prepared with the intent to deceive or defraud. The crime of forgery occurs when an individual, with intent to defraud, makes or alters a document apparently capable of defrauding another.

A document is not a forgery just because it contains a false representation. To constitute a forgery, the writing as a whole must have apparent legal significance. In addition, forgery occurs not only when an entire writing or instrument is created, but also when there is any material alteration that affects the legal significance of the document or whenever a signature on a writing is fraudulently procured from a person who does not know what he is signing. Furthermore, the forgery is committed even if no one is actually defrauded.

Theft of Money or Property

Theft is a term often used to describe a wide variety of fraudulent conduct that encompasses many forms of deceitful taking of property belonging to others. As used here, however, the term *theft* is limited to embezzlement, larceny, and misappropriation of trade secrets and proprietary information.

Embezzlement

Embezzlement is the wrongful appropriation of money or property by a person to whom it has been lawfully entrusted (or to whom lawful possession was given). Embezzlement involves a breach of trust, although it is not necessary to show a *fiduciary relationship*—a relationship of

confidence, trust, or good faith—between the parties. The elements of embezzlement vary somewhat by jurisdiction, but generally are:

- The defendant took or converted
- Without the knowledge or consent of the owner
- Money or property of another
- That was entrusted to the defendant (the defendant had lawful possession of the property)

Larceny

Larceny is defined as the wrongful taking of money or property of another with the intent to convert or to deprive the owner of its possession and use. Unlike in embezzlement schemes, in larceny, the defendant never has lawful possession of the property to establish a larceny claim. The elements of larceny typically include:

- Unlawfully taking or carrying away
- Money or property of another
- Without the consent of the owner
- With the intent to permanently deprive the owner of its use or possession

Larceny differs from embezzlement, and the difference centers on who has legal custody over the stolen articles. A larcenist takes something from its rightful owner without ever having had legal custody of the item stolen. The embezzler, conversely, takes something in which he has lawful possession. Thus, the major distinction between larceny and embezzlement lies in the issue of whether the thief had been lawfully entrusted with the stolen articles.

Although larceny was an offense under the common law of England, it has been abolished in England and Wales, Northern Ireland, and the Republic of Ireland. In England and Wales, larceny was replaced by the broader offense of theft under the Theft Act 1968, and in Northern Ireland, larceny was replaced by the offense of theft under the Theft Act (Northern Ireland) 1969. (Scotland has a separate criminal law framework that differs from the one in England and Wales.) Accordingly, the terms *theft* and *larceny* are sometimes used synonymously. Larceny does, however, remain an offense in the United States and New South Wales, Australia.

Misappropriation of Trade Secrets

Misappropriation is the intentional, illegal use of the property, funds, or ideas of another person for an unauthorized purpose. In the fraud context, misappropriation claims generally involve trade secrets or other proprietary information.

Trade secrets include not only secret formulas and processes, but the term also refers to more mundane proprietary information, such as customer lists, sales figures, business plans, vendor contracts, blueprints and construction plans, bidding systems, computer programs, test data, pricing information, recipes, marketing plans, manufacturing processes, business forms, or any other confidential information that has a value to the business and would be potentially harmful if disclosed.

The definition of what constitutes a trade secret depends on the organization, industry, and jurisdiction, but the following three characteristics are common to most definitions:

- The information is not generally known to the relevant portion of the public.
- The information confers some sort of economic benefit on its holder (where this benefit must derive specifically from its not being generally known, not just from the value of the information itself).
- The information is the subject of reasonable efforts to maintain its secrecy.

The elements of a typical claim for misappropriation of trade secrets are:

- The defendant possessed information of value.
- The information was treated confidentially.
- The defendant took or used the information by breach of an agreement, confidential relationship, or other improper means.

Organizations and individuals can maintain legal protection over trade secrets by taking reasonable steps to keep the information secret. Safeguarding trade secrets should include measures such as security policies and procedures that protect sensitive information and mitigate risks associated with information security breaches, awareness training, physically securing the information to prevent unauthorized access and use, and strict limitations on distribution of the information.

The owners of the information also should enforce restrictive agreements and act promptly to remedy any inadvertent disclosures. Failure to do so might be construed as a waiver of confidentiality and make it impossible to prevent future use or disclosures.

Also, employers should consider requiring that all employees sign nondisclosure and noncompetition agreements upon the commencement and termination of employment. Such agreement can provide employers with legal recourse against those who misappropriate proprietary information.

Generally, a *nondisclosure agreement* is a written agreement providing that signatory employees must keep all trade secrets and proprietary information learned during their employment confidential. Nondisclosure agreements serve the following functions:

- They delineate the confidentiality expectations the employer has for its employees.
- They demonstrate that the employer is serious about protecting trade secrets and proprietary information.
- They show the reasonable efforts that the employer takes to maintain the secrecy of its confidential information.

A *noncompetition agreement* is an agreement whereby one party (usually an employee) agrees not to work for or start a company in competition against another party (usually the employer) within a certain period. Such agreements usually take effect after the employer-employee relationship has ended.

While noncompetition agreements can be useful for a variety of reasons, such as protecting trade secrets or goodwill, there are a number of legal issues that limit their effectiveness. For example, courts in some jurisdictions have held that such agreements are against public policy because they limit the future employment of a person; therefore, in these jurisdictions, noncompetition agreements are unenforceable. Moreover, even in jurisdictions that uphold these agreements, they will only do so if the agreements satisfy the following three elements:

- The agreement is supported by consideration at the time it is signed. If the employment agreement and the noncompetition agreement are signed at the same time (or if the noncompetition agreement is signed before the employee begins employment), the employment itself will be sufficient consideration for the promise not to compete. If, however, an employee signs the noncompetition agreement after beginning employment, the agreement generally will be invalid unless the employee receives something of value (besides the promise of continued employment) in exchange for the promise (e.g., a promotion or additional benefit that was not part of the original employment agreement).
- The agreement protects a legitimate business interest of the employer (e.g., confidential information and goodwill developed by an employer in terms of customer relations).

- The agreement is reasonable in scope, geography, and duration. Courts generally only enforce noncompetition agreements to the extent necessary to protect the employer. Thus, to be enforceable, such agreements must contain reasonable limitations to the scope, geographical area, and time in which a party may not compete.

Additionally, any noncompetition signed by an at-will employee who is not covered by an employment agreement would be unenforceable. Therefore, before instituting a noncompetition agreement, management should consult with legal counsel to make sure the agreement is valid and enforceable under the applicable law.

Furthermore, a person accused of misappropriating trade secrets might raise several defenses. The most typical defense is that the accused developed the information independently. The accused also might defend a misappropriation claim by showing that the information was not in fact a secret, that he was authorized to use the information, or that the owner had abandoned the trade secret.

CIVIL ACTION FOR MISAPPROPRIATION OF TRADE SECRETS

In most jurisdictions, a victim of trade secret theft may file a civil action for damages or request an *injunction*—a court order by which a party is required to perform, or is restrained from performing, a specific act—under various types of laws. Civil damages for misappropriation of trade secrets might include reimbursement for actual losses caused by the defendant, such as lost profits, reimbursement of development expenses and overhead costs, and the cost of efforts to protect the secret or recover damages, as well as for reduction in the value of business. Damages also can be measured by the defendant's profits, which may be ordered to be paid to the plaintiff. Punitive damages and attorney's fees also may be awarded.

In addition to or in lieu of monetary damages, the plaintiff in a civil action for misappropriation of trade secrets also may obtain an injunction prohibiting further use of the information. But injunctions are difficult to obtain. To obtain an injunction, the plaintiff must establish that an injunction is warranted. Generally, to demonstrate that an injunction is warranted, the plaintiff must establish that:

- It is the proper owner of the trade secret.
- An unauthorized person has taken or used the trade secret.
- There is a high probability of improper disclosure.

- The injunction is necessary to prevent the plaintiff from suffering immediate and irreparable harm that cannot be adequately compensated by monetary damages.
- The plaintiff probably will win the underlying case for misappropriation of trade secrets.

Injunctions have been issued in trade secret cases to:

- Prevent the use of stolen information.
- Prohibit an employee in possession of a trade secret from accepting employment with a competitor.
- Order the wrongdoer to return the misappropriated information.

Breach of Contract

If the fraudster has any kind of a contractual relationship with the victim, there may be a breach of contract claim. A *breach of contract* occurs when one party to a contract fails to perform, or announces that it does not intend to perform, his contractual obligations without just cause. A breach of contract claim can arise under an oral or written contract. Many jurisdictions have recognized certain implied or unwritten duties as a part of almost every contract. For instance, some courts have held that it is an implicit part of a contract that each party will use their best efforts to fulfill their duties under the contract. A similar duty that has been recognized in some jurisdictions is the duty imposed on each party to deal with each other in good faith. If a party to a contract, including employment contracts, breaches the duty of good faith, the non-breaching party may have a civil claim for breach of contract.

Breach of Fiduciary Duty

People in a position of trust or *fiduciary relationship*—such as officers, directors, high-level employees of a corporation or business, and agents and brokers—owe certain duties to their principals or employers, and any action that runs afoul of such fiduciary duties constitutes a breach.

Establishing a breach of fiduciary duty claim is easier than establishing a claim for fraud because a breach of fiduciary duty claim does not require proof of wrongful intent. In fact, to state a claim for breach of fiduciary duty, the plaintiff must show only that the defendant:

- Occupied a position of trust or fiduciary responsibility with respect to the plaintiff (e.g., was an employee or agent)
- Breached that duty to advance a personal interest

The principal fiduciary duties are loyalty and care.

Duty of Loyalty

The *duty of loyalty* requires that the employee/agent act solely in the best interest of the employer/principal, free of any self-dealing, conflicts of interest, or other abuse of the principal for personal advantage. Employees/agents who owe a duty of loyalty must act solely in the best interest of their principal and may not seek to advance their personal interests to the detriment of their principal. Accordingly, corporate directors, officers, and employees are barred from using corporate property or assets for their personal pursuits or taking corporate opportunities for themselves.

Additionally, if an employee/agent commits a more traditional form of fraudulent conduct, such as embezzlement, theft, acceptance of a kickback, and conflict of interest, the conduct also violates the employee/agent's duty of loyalty and may be redressed as such in addition to or instead of the underlying offense.

Duty of Care

The *duty of care* means that people in a fiduciary relationship must act with such care as an ordinarily prudent person would employ in similar positions. Corporate officers, directors, or high-level employees, as well as other people in a fiduciary relationship, must conduct their business affairs prudently with the skill and attention normally exercised by people in similar positions. Fiduciaries who act carelessly or recklessly are responsible for any resulting loss to the corporate shareholders or other principals. Damages may be recovered in a civil action for negligence, mismanagement, or waste of corporate assets.

People in a fiduciary relationship, however, are not guarantors against all business reverses or errors in judgment. In many countries, the *business judgment rule* protects corporate officers and directors from liability for judgments that were made in good faith (e.g., free of self-dealings or conflicts) and appeared to be prudent based on the then-known circumstances. Corporate defendants in such cases might raise the business judgment rule in defense by showing that they had no reasonable grounds to suspect such conduct or that the cost of prevention or recovery was too high compared to the anticipated returns.

Corporate officers breach their duty of loyalty if they accept kickbacks, engage in a conflict of interest, or are otherwise disloyal, but corporate officers who carelessly fail to prevent such conduct, enforce controls, or pursue recovery of losses might breach their duty of care.

Breach of Fiduciary Duty Claims

Generally, a breach of fiduciary duty claim is a civil wrong that is redressible by a civil action for recovery of damages. Typically, a plaintiff who brings a successful breach of fiduciary duty claim may receive damages for lost profits and recover profits that the disloyal employee/agent earned—in some instances even the salary paid to the employee or agent during the period of disloyalty. The plaintiff may recover profits earned by the disloyal agent even if the principal did not suffer an actual loss. The plaintiff also may void any contracts entered into on its behalf that were the result of or were influenced by the employee or agent's disloyalty.

Gross Negligence

Gross negligence is a civil cause of action, and it can be generally defined as the intentional failure to perform a duty in reckless disregard of the consequences to the victim. Although the exact definition varies by jurisdiction, the basic elements of this civil cause of action are that the defendant committed an intentional act, knowing that it was at least substantially likely to cause harm to the victim.

In the employment context, employees have a duty to act in the best interests of their employers. So, if an employee consciously steals from his employer, the employee has breached his duty to act in the best interest of his employer and caused harm to his employer. Further, if the employee knew that the harm resulting from his wrongful act was likely to occur when he committed the act, his actions may rise to the level of gross negligence.

Generally, punitive or exemplary damages are available if the defendant is found liable for gross negligence.

Conspiracy

Conspiracy refers to a situation in which two or more people agree to commit an illegal act. In most jurisdictions, the crime of conspiracy is actually a separate criminal offense from the underlying crime, meaning that the underlying crime (e.g., bank fraud, bribery, securities fraud, etc.) and the conspiracy to commit it are two separate offenses.

The essential elements that must be shown to prove a conspiracy are as follows:

- The defendant entered an agreement with at least one person to commit an illegal act.
- The defendant knew the purpose of the agreement and intentionally joined in the agreement.
- At least one of the conspirators knowingly committed at least one overt act in furtherance of the conspiracy.

Under the first element, the government must prove that the defendant reached an agreement or understanding to commit an illegal act with at least one other person. The conspirators must agree about the precise illegal act.

Under the second element, the government must establish that the defendant knew of the conspiracy's existence and its objective. The government, however, does not have to establish that the defendant knew all the details or objectives of the conspiracy, and it does not have to prove that the defendant knew the identity of all the participants in the conspiracy.

Finally, the purpose of the conspiracy need not be accomplished for a violation to occur, but at least one of the co-conspirators must have carried out at least one overt act in furtherance of the conspiracy. The overt act must be an independent act that comes after the agreement to commit the illegal act and that is performed for the purpose of carrying out the conspiracy's objective. The overt act, however, need not be criminal and could be as innocuous as making a phone call or writing a letter.

Conspiracy counts are favored by prosecutors because they provide evidentiary and pleading advantages. If a conspiracy is shown, the acts and statements of one co-conspirator may be admitted into evidence against all, and each co-conspirator may be convicted for the underlying substantive offense (e.g., destroying government property) committed by any one of its members.

A corporation cannot conspire with one of its own employees to commit an offense because the employee and employer are legally viewed as one. A corporation, however, can conspire with other business entities or third parties to commit conspiracy.

Obstruction of Justice

Obstruction of justice occurs when an individual engages in an act designed to impede or obstruct the investigation or trial of other substantive offenses. Prosecutors usually are pleased to discover such violations by defendants because they add a more sinister flavor to what might be colorless white-collar charges, and such actions can help to prove criminal intent.

Jurisdictions might have several criminal obstruction statutes. Some common types of obstruction statutes are those that prohibit:

- Influencing or injuring any officer of the court or juror by force, threats of force, intimidating communications, or corrupt influence
- Influencing a juror through a writing
- Stealing or altering records or processes by parties that are not privy to the records
- Using force or threats of force to obstruct or interfere with a court order
- Destroying documents related to a future proceeding
- Tampering with a witness, victim, or an informant (e.g., killing or attempting to kill, using force or threats of force, intimidating, influencing with bribes or other corrupt means, misleading, or harassing the protected parties)
- Influencing, obstructing, or impeding a government auditor in the performance of his official duties
- Obstructing the examination of a financial institution

Perjury

Perjury is an intentional false statement given under oath on a material point at issue. The basic elements for the crime of perjury are as follows:

- The defendant made a false statement.
- The defendant made the false statement while under oath.
- The false statement was material or relevant to the proceeding.
- The defendant made the statement with knowledge of its falsity.

Laws that criminalize perjury, however, do not require that the false statement be given in a court of law. Generally, the forum for a perjurious statement includes any court, depositions in connection with litigation, bail hearings, venue hearings, suppression hearings, and so on. Thus, an individual can commit perjury for false statements made somewhere other than a court of law.

Also, for a statement to be perjurious, it must be material. Generally, a statement is material if it tends to influence, or is capable of influencing, the decision of the decision-making body to whom it is addressed.

False Claims and Statements to Government Agencies

Laws prohibiting false claims and statements to government agencies make it illegal for a person to lie to, or conceal material information from, a government agency. A *false claim* is an assertion of a right to government money, property, or services that contains a misrepresentation. A *false statement* is an oral or written communication, declaration, or assertion that is factually untrue.

Elements of False Claim or Statement Violations

Generally, to prove a violation, the government must show that the defendant:

- Knowingly and willfully (or with reckless disregard for truth or falsity)
- Made a false claim or statement (or used a false document)
- That was *material* (i.e., sufficiently important or relevant to influence decision making)
- Regarding a matter within the jurisdiction of a government agency
- With knowledge of its falsity

An act is done knowingly and willfully if it is done voluntarily and intentionally, and not by mistake or another innocent reason. Thus, an individual can be found guilty for making a false statement or claim only if the individual knew the statement or claim was false at the time it was made.

Also, the following are general rules with regard to laws criminalizing false claims and statements to government agencies:

- An individual can be found guilty for making a false claim or statement even if the claim or statement is not made directly to a governmental department or agency. That is, a false claim or statement can be made to a third party as long as it involves a matter within the jurisdiction of a governmental department or agency.
- An individual can be found guilty for making a false claim or statement even if the government was not deceived by the falsity.
- An individual can be found guilty for making a false claim or statement even if the government did not rely on the falsity.

- An individual can be found guilty for making a false claim or statement even if the government did not suffer a loss in reliance on the falsity.
- For an individual to be found guilty of making a false claim or statement, the claim or statement at issue must have been capable of influencing the government entity involved.

Often, countries have various related laws that criminalize false or fraudulent statements to government agencies. Common types of false claims and statement laws of greatest importance to fraud examiners include:

- Laws that prohibit the making of fraudulent demands for money against the government
- Laws that prohibit false statements or reports on credit applications or related document submitted to a bank or credit institution
- Laws that prohibit schemes to obtain money or property from governments by means of false or fraudulent pretenses involving government contracts

International Initiatives Against Fraud and Corruption

Introduction

There are a range of different international instruments designed to combat fraud and corruption, including international treaties, European Union (EU) instruments for member countries, domestic laws, and non-legally binding instruments. This section introduces some of the major international tools, including those related to anti-corruption, anti-money laundering, and banking and financial system regulation and supervision.

International Anti-Corruption Instruments

The international effort to combat corruption gained significant momentum in the 1990s. Until that time, only the United States had criminalized the bribery of foreign public officials with the passage of its Foreign Corrupt Practices Act (FCPA) in 1977. The FCPA effectively put companies operating within the United States at a competitive disadvantage, leading business groups to petition for a weakening of the FCPA's provisions.

Previous attempts to establish multinational initiatives against corruption had failed largely as a result of security concerns related to the Cold War. However, the end of that conflict and the growing trend toward economic integration created a far more receptive political climate. Simultaneously, increased media coverage of financial matters, facilitated in part by the

emergent Internet, brought greater public attention to bribery and corrupt trade practices. In addition, contemporary campaigns to promote democratic principles throughout the world had targeted corruption as an inherent obstacle to good governance.

Recognizing the limited impact unilateral efforts can have on a global issue like corruption, international organizations developed strategies to combat corruption through coordinated domestic measures. Starting with the work of the Organisation for Economic Co-operation and Development (OECD), this movement has continued to grow and has produced increasingly ambitious endeavors. Despite the progress already made, however, corruption remains a serious concern.

This section introduces the major international anti-corruption instruments, beginning with those concerning the OECD. An overview of the more recent UN Convention and several regional conventions follows. And because the FCPA and the UK Bribery Act 2010 have an extraterritorial effect on multinational companies, this section contains a brief discussion of each of these laws.

The Organisation for Economic Co-operation and Development

Formed in 1961, the Organisation for Economic Co-operation and Development (OECD) is an intergovernmental institution dedicated to democracy and the market economy. It operates as a forum for governments to cultivate and advance social and economic policies that expand world trade, promote sustainable economic development, and improve living standards. Members compare policy experiences to identify sound practices for the resolution of common problems.

The OECD coordinates domestic and international policy through either soft law or legally binding agreements. *Soft law* refers to guidelines, resolutions, codes of conduct, and other quasi-legal instruments that are not directly enforceable. The OECD Recommendations discussed below are examples of soft law. In contrast, the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions is a legally binding agreement.

At present, the OECD consists of 34 member countries: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, South Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain,

Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Joining the OECD fully in 2010, Chile, Estonia, Israel, and Slovenia are the most recent members. The OECD suspended membership talks with Russia in 2014 due to its role in the Crimean crisis.

THE OECD'S RECOMMENDATION ON COMBATING BRIBERY IN INTERNATIONAL BUSINESS

The OECD formed an ad hoc working group in 1989 to explore corruption in international trade. After conducting a comparative review of member countries' laws and regulations, the group published the *Recommendation on Combating Bribery in International Business* (Recommendation) in 1994.

The Recommendation was designed to combat corruption in international business by urging member states to adopt effective measures to detect, prevent, and combat bribery of foreign public officials in international business. Thus, it targets only acts of bribery aimed at public-sector officials, and it is silent regarding bribery confined to the private sector.

The Recommendation defines *bribery* as the act of offering and giving any undue benefit to obtain or retain business.

As a result, the Recommendation targets the *supply side* of bribery—the offering side of the bribery bargain. It does not address the *demand side*—the solicitation and receipt of bribes. In doing so, the Recommendation avoids complicated jurisdictional issues and interference with the sovereignty of non-member countries.

The Recommendation urges member states to deter and penalize the bribery of foreign public officials by taking "concrete and meaningful steps" to improve the following areas within their respective infrastructures:

- Criminal, civil, commercial, and administrative laws
- Tax systems and regulations
- Banking and accounting requirements and practices
- Laws and regulations related to public subsidies, licenses, and contract procurement

In 1994, the OECD Working Group on Bribery in International Business Transactions (Working Group) was formalized and began to develop substantive provisions to be implemented in the four identified areas.

THE OECD'S TAX RECOMMENDATION AND REVISED RECOMMENDATION

In 1996, the Working Group responded to tax-related concerns by releasing the *Recommendation on Tax Deductibility of Bribes of Foreign Officials* (Tax Recommendation). Bribery had become so entrenched in international business that some countries provided tax deductions for bribes paid to foreign officials. The Tax Recommendation calls on members to prohibit this practice.

In 1995, measures to address the remaining areas of concern were presented in the *Revised Recommendation on Combating Bribery in International Business* (Revised Recommendation). To strengthen banking and accounting standards, the Revised Recommendation advocates that OECD members take the following steps:

- Prohibit off-book transactions and accounts.
- Require companies to maintain adequate records of income and expenditures and to disclose material contingent liabilities in financial statements.
- Establish and maintain standards to ensure independence when financial statements are audited externally.
- Encourage companies to adopt internal controls and standards of conduct that provide protection and channels for reporting violations.
- Suspend companies that have bribed foreign officials from competing for public contracts.
- Incorporate anti-corruption provisions into bilateral aid-funded procurements and international development institutions.
- Cooperate fully with other countries and international bodies in the investigation and prosecution of bribery cases.

The Working Group's main objective in creating the Revised Recommendation was the criminalization of bribery of foreign public officials, yet this goal presented substantial challenges. Fundamental differences in national legal systems prevented the formulation of provisions that could be implemented uniformly. In addition, many OECD members were not content to address such a critical matter through soft law alone, while others feared that negotiating a legally binding convention would result in considerable delays.

Ultimately, the working group used the Revised Recommendation to advise members to criminalize the bribery of foreign public officials and announce the commencement of negotiations for a binding convention.

THE OECD CONVENTION ON COMBATING BRIBERY OF FOREIGN PUBLIC OFFICIALS IN INTERNATIONAL BUSINESS TRANSACTIONS

The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Anti-Bribery Convention) is a legally binding agreement that sets a uniform, minimum standard that signatory countries must implement through national legislation. Of course, countries may adopt laws that exceed that standard; the following section provides several examples of such legislation.

Signatory countries commit themselves to criminalizing the bribery of foreign public officials through domestic legislation, and any differences in such laws are accepted if they produce equivalent results (i.e., effective prosecution or sanctions).

The OECD Anti-Bribery Convention defines *bribery* as intentionally offering, promising, or giving an undue benefit, either directly or through an intermediary, in order to obtain business or an improper advantage in the course of international trade.

Like the Recommendation on Combating Bribery in International Business, the OECD Anti-Bribery Convention applies only to the supply side of bribery and only to acts aimed at foreign public officials (i.e., public-sector officials).

The OECD Anti-Bribery Convention defines a *foreign public official* as any person who:

- Holds a legislative, administrative, or judicial office in a foreign country either by election or appointment
- Exercises a public function for a foreign country, public agency, or public enterprise
- Acts as an official or agent for a public international organization

The OECD Anti-Bribery Convention specifies that bribes involve any form of undue benefit or advantage, including both pecuniary gains—money, membership to a club, or the promise of a scholarship—and non-pecuniary gains, like favorable publicity.

Additionally, signatory countries are required to establish jurisdiction over acts of foreign bribery that occur, either in whole or in part, within their respective territories. Countries that exercise jurisdiction to prosecute nationals for offenses committed abroad must likewise establish jurisdiction over acts of foreign bribery. Furthermore, the OECD Anti-Bribery Convention requires enhanced mutual legal assistance between countries in the investigation and prosecution of foreign bribery, including the extradition of nationals.

Moreover, signatory countries must establish effective, proportionate, and dissuasive criminal penalties for the offense of foreign bribery. The OECD Anti-Bribery Convention stipulates that such penalties must be comparable to the respective penalties each country enforces for domestic bribery. Countries that do not apply criminal penalties to legal persons for domestic bribery must impose non-criminal sanctions for acts of foreign bribery. Parties to the OECD Anti-Bribery Convention must also take reasonable steps to assure the seizure and confiscation of bribes and the assets derived from bribery. Finally, where domestic bribery qualifies as a predicate act for money laundering, foreign bribery must also constitute a predicate act.

The Working Group monitors the implementation of the OECD Anti-Bribery Convention through a rigorous peer review process conducted over the course of multiple phases.

OECD'S RECOMMENDATIONS FOR FURTHER COMBATING BRIBERY OF FOREIGN OFFICIALS

In 2009, the Working Group issued two additional recommendations for further combating bribery of foreign public officials in international business transactions. For the most past, these instruments merely reinforce the earlier Recommendations and OECD Anti-Bribery Convention. They encourage member countries to review, evaluate, and, where necessary, strengthen the laws and regulations relevant to the fight against foreign bribery. Members are specifically advised to re-examine standards pertaining to:

- The adequacy of accounting requirements
- The independence of external audits
- Corporate internal controls and compliance programs
- The suspension of public advantages for enterprises that have engaged in foreign bribery

The 2009 recommendations introduced several new provisions as well. The 2009 recommendations encouraged member countries to launch initiatives to raise awareness within both the public and private sectors of the fight against foreign bribery, and they call for measures to improve reporting acts of foreign bribery. According to the 2009 recommendations, easily accessible channels should exist to report suspected acts of bribery to the appropriate authorities, and safeguards should be in place to protect individuals who, in good faith, file a report from discrimination or disciplinary actions.

OECD'S GUIDELINES FOR MULTINATIONAL ENTERPRISES

The OECD Guidelines for Multinational Enterprises (OECD Guidelines) are a form of soft law, and they contain principles and standards designed to engage corporations in the fight against corruption.

The OECD Guidelines seek to combat corruption in a number of ways. They discourage all forms of bribery, including illegal contributions to political parties and candidates, and they recommend the adoption of self-regulatory practices and compliance programs to maintain high standards for accounting, auditing, and disclosing financial statements.

Furthermore, the OECD Guidelines encourage companies' management to enhance the transparency of their anti-corruption activities to raise greater awareness within their communities, and they propose principles to halt anti-competitive activities such as price fixing and bid rigging.

Finally, the OECD Guidelines include provisions intended to protect consumer, employee, and environmental interests.

OECD'S GOOD PRACTICE GUIDANCE ON INTERNAL CONTROLS, ETHICS, AND COMPLIANCE

On February 18, 2010, the OECD Council, which exercises the decision-making power of the OECD, adopted the Good Practice Guidance on Internal Controls, Ethics, and Compliance (Good Practice Guidance). The Guidance, which can be downloaded from the OECD website, sets forth certain best practices for establishing an anti-corruption compliance program.

The OECD's Good Practice Guidance identifies key features for effective compliance programs to detect and prevent the bribery of foreign officials. Businesses are encouraged to adapt such features to suit their unique circumstances and incorporate the identified practices to complement their overall compliance framework. In addition, professional organizations and associations may be consulted for further information and resources.

In general, the OECD's Good Practice Guidance recommends that organizational management adhere to the following measures when establishing compliance programs:

- Establish a clear and unambiguous policy prohibiting the bribery of foreign officials.

- Create an ethical environment, and ensure that the anti-corruption policy has strong, explicit support from senior management.
- Provide that compliance with anti-bribery program is the duty of every employee.
- Make senior management responsible for implementation and oversight of the anti-corruption policies, standards, and procedures.
- Design the compliance program to detect and prevent corruption, and it should include policies covering gifts; hospitality, entertainment, and expenses; customer travel; political contributions; charitable donations and sponsorships; facilitation payments; and solicitation and extortion.
- Make the program applicable to third party business partners (e.g., agents and other intermediaries, consultants, representatives, distributors, contractors, suppliers, consortia, and joint venture partners).
- Create an internal controls system designed to ensure compliance with the prohibition of bribing foreign officials.
- Implement mechanisms to ensure that anti-corruption policies, standards, and procedures are communicated effectively to all employees and, where appropriate, agents and business partners.
- Implement appropriate measures to encourage and provide support for employees to comply with the compliance program.
- Institute appropriate disciplinary measures for violations of anti-corruption laws, policies, and procedures, as well as remedial actions to prevent recurrences of such misconduct.
- Install a system that provides guidance and advice to employees regarding anti-corruption issues.
- Conduct periodic testing of the anti-corruption program to evaluate and improve its effectiveness.

The OECD Working Group began to monitor countries' progress in encouraging their companies to implement the provisions contained in the guidance in March 2010.

United Nations Convention Against Corruption

The United Nations, an international organization with a membership that includes almost every nation, also produces initiatives against bribery and corruption. The United Nations' *Convention Against Corruption* (UN Convention) is an important instrument in the international fight against corruption, and it represents the significant progress that has been made over the past few decades. The UN Convention was concluded in 2003 and went into force in

2005. It remains open to accession by any country or regional economic integration organization and, at present, has been signed by 140 members. Of the 41 nations party to the OECD Convention, only two have yet to ratify the UN Convention—Japan and New Zealand.

The UN Convention is considerably broader in scope than the OECD Convention. It establishes a framework to combat all forms of corruption, including bribery, extortion, embezzlement, trading in official influence, and general abuses of power. The UN Convention introduces standards for member states to incorporate into national legislation to address corruption in both the private and public sectors. The measures and provisions contained therein are intended to respect the fundamental principles of members' respective legal systems while focusing on four specific areas of concern:

- Prevention
- Criminalization
- Asset recovery
- International cooperation

PREVENTION

The UN Convention devotes its first chapter to preventive measures aimed at both the public and private sectors. Member states must ensure the existence of independent anti-corruption bodies that oversee implementation of the UN Convention policies and disseminate relevant information. Such policies include the development of safeguards to ensure civil servants are hired, retained, and promoted based on objective criteria. Once recruited, civil servants must be subject to codes of conduct and reporting requirements to enhance transparency and accountability in the management of public finances. Member states must also take the necessary steps to ensure the independence of the judiciary and prosecution services.

Regarding the private sector, member states must improve accounting and auditing standards to require the maintenance of books and records and the disclosure of financial statements. The UN Convention also mandates regulations to deter and detect all forms of money laundering by any bank or financial institution. Additional measures call for professional codes of conduct, rules to prevent conflicts of interest, and greater cooperation between law enforcement agencies and private entities. Finally, member states are encouraged to engage civil society, including community groups and non-governmental organization, in the fight against corruption.

CRIMINALIZATION

As noted above, the UN Convention addresses all forms of corruption, not bribery alone. The UN Convention lists specific acts of corruption, but it does not require member states to criminalize every one of them. Instead, it requires member states to criminalize only certain acts of corruption, and to merely consider criminalizing others. Specifically, members to the UN Convention must establish a criminal offense for the following acts of corruption:

- The supply and demand of bribes to domestic public officials
- The supply of bribes to foreign public officials
- Money laundering
- The embezzlement, misappropriation, or diversion of public property by domestic officials

Member states are encouraged, but not obligated, to criminalize the following acts of corruption:

- The demand of bribes by foreign public officials
- The supply and demand of bribes by private sector actors
- Trading in influence
- The abuse of official functions or position
- Illicit enrichment
- Embezzlement by private sector actors
- The concealment or retention of proceeds of a crime
- The obstruction of justice

Similar to the OECD Convention, the UN Convention requires member states to establish liability for legal persons and to exercise jurisdiction over acts of corruption committed within their territories or by their nationals. In addition, any legislation criminalizing an act of corruption must include knowledge or specific intent as an element of the offense.

ASSET RECOVERY

Perhaps the most significant achievement of the UN Convention, and a major influence in many countries' decision to ratify, is the agreement on asset recovery. Stated as a fundamental principle, asset recovery is particularly important to developing countries, which are vulnerable to corruption and in need of resources for reconstruction and rehabilitation programs. Reaching consensus on the issue required intensive negotiations to balance the needs of countries seeking recovery against the legal and procedural safeguards of countries providing assistance. Effective implementation of the asset recovery provisions

will both remedy one of the worst effects of corruption and send a message that illegal assets cannot be hidden anywhere.

Member states must implement the necessary mechanisms to detect and prevent the transfer of assets obtained through illicit activities. Authorities must have competence to confiscate, seize, or freeze any such assets. All parties to the UN Convention must permit one another to initiate legal action in their respective courts. Generally, a requesting state will recover the contested assets if it is able to prove ownership, and in certain circumstances the assets will be returned directly to the victims.

INTERNATIONAL COOPERATION

Parties to the UN Convention agree to cooperate with one another in the fight against corruption, including the prevention, investigation, and prosecution of any offense. Cooperation is mandatory in criminal matters, but only encouraged in civil and administrative issues. Countries must assist one another in gathering and sharing evidence, returning the proceeds of illicit activity, and extraditing offenders for effective prosecution.

Major Regional Initiatives Against Corruption

This discussion provides an overview of several regional anti-corruption conventions, including the:

- Inter-American Convention Against Corruption
- European Union Convention on the Fight Against Corruption Involving Officials of the European Communities or Officials of Member States
- Council of Europe Criminal Law Convention on Corruption
- African Union Convention on Preventing and Combating Corruption

INTER-AMERICAN CONVENTION AGAINST CORRUPTION

While the OECD is generally credited with setting the international trend against corruption, the *Inter-American Convention Against Corruption* (IACAC) was actually the first legally binding convention to address the issue. It went into effect in March 1997 and has been ratified by all 35 members of the Organization of American States.

The stated purpose of the Inter-American Convention Against Corruption (IACAC) is to promote and regulate cooperation among members to prevent, detect, punish, and eradicate corruption.

The IACAC requires signatories to:

- Consider preventive measures, such as codes of conduct, transparent systems for the hiring of public servants and expenditure of public funds, and the encouragement of active participation by civil society in the fight against corruption.
- Establish a criminal offense for both the supply and demand of bribes aimed at domestic and foreign officials.
- Provide legal and technical assistance to one another for the effective prosecution of acts of bribery, including the extradition of nationals and the freezing, seizure, and forfeiture of identified property and assets.

EUROPEAN UNION CONVENTION ON THE FIGHT AGAINST CORRUPTION INVOLVING OFFICIALS OF THE EUROPEAN COMMUNITIES OR OFFICIALS OF MEMBER STATES

The EU Convention on the Fight Against Corruption came into effect in May 1997. Its scope is narrowly tailored to prevent the supply and demand of bribes aimed only at officials of the EU and EU member states. Such officials may include ministers, members of national parliaments, members of the judiciary and the courts of auditors, and members of the EU Commission, European Parliament, and the Court of Justice. EU member states are to cooperate fully in the prosecution and extradition of offenders. The Convention does require national legislation to incorporate the principle of *ne bis in idem*. The principle, which translates from Latin as "not twice for the same", prohibits prosecution in two member states based on the same underlying facts.

COUNCIL OF EUROPE CRIMINAL LAW CONVENTION ON CORRUPTION

The Council of Europe is distinct from the EU and focuses its efforts on human rights, the rule of law, democratic development, and cultural cooperation. It is currently comprised of 47 nations and membership is open to any European state. Other countries, including the United States and Japan, have observer status and may participate in the Council of Europe committees, and several conventions are open to accession by non-member countries.

The Council of Europe Convention was concluded in January 1999 and contains measures to address a wide range of corrupt behavior and encourage mutual assistance. Signatory countries must establish a criminal offense for:

- The supply and demand of bribes involving domestic and foreign public officials, members of domestic and foreign public assemblies, officials of international organizations, and judges and officials of international courts

- The supply and demand of bribes within the private sector
- Trading in influences or influence peddling (i.e., using one's influence in government or connections with people in authority to obtain preferential treatment)
- Money laundering and fraudulent recordkeeping and accounting practices

Liability must apply to corporate entities as well as individuals. The Convention also calls for cooperation between national authorities for gathering evidence, confiscating corrupt proceeds, protecting witnesses, and extraditing offenders.

AFRICAN UNION CONVENTION ON PREVENTING AND COMBATING CORRUPTION

The Convention on Preventing and Combating Corruption was adopted in 2003 by the African Union and went into effect in 2006.[1] Forty-eight nations have signed the AU Convention, and 35 of those signatories have ratified it. It is a comprehensive instrument based on the promotion of democratic principles and social justice, transparency in governance, and respect for human rights. In addition to criminalizing acts of corruption, member states agree to adopt preventive measures, increase public access to information, and involve the media and civil society in the fight against corruption.

Members must adopt national legislation necessary to establish criminal offenses for a wide range of corrupt activity, including:

- The supply and demand of bribes aimed at both the public and private sectors
- Embezzlement of public funds
- Illicit enrichment
- Money laundering

The Convention requires cooperation among members, extradition of offenders, and confiscation and seizure of illegal proceeds. All offenders must receive a fair trial conducted in accordance with the minimum guarantees set forth in the African Charter on Human and People's Rights.

The U.S. Foreign Corrupt Practices Act

The United States Congress originally enacted the Foreign Corrupt Practices Act (FCPA) in 1977 to prohibit making corrupt payments to foreign officials or political organizations. Since its enactment, the FCPA has had an enormous impact on the way organizations

[1] Every African nation is a member of the African Union, with the exception of the Kingdom of Morocco.

around the world conduct business. While only enforced by the United States, the FCPA is a law with international reach because businesses within its scope may violate the statute anywhere in the world.

The FCPA has two principal components: the anti-bribery provisions and the accounting provisions. In short, the anti-bribery provisions make it unlawful to bribe foreign government officials to obtain or retain business, and the accounting provisions require publicly traded companies subject to the FCPA's jurisdiction to keep accurate books and records and adopt internal controls to prevent improper use of corporate funds.

FCPA'S ANTI-BRIBERY PROVISIONS (15 U.S.C. § 78dd)

The FCPA's anti-bribery provisions make it unlawful for regulated parties (i.e., any citizen, national, or resident of the United States; any U.S. business entity; any company that has securities registered in the United States or is required to file reports with the Securities and Exchange Commission (SEC); and foreign nationals and businesses taking action in the United States) to bribe foreign government officials to obtain or retain business. Specifically, the provisions prohibit corrupt offers or payments to foreign government officials, political parties, political party officials or candidates, or to any person for payment to such foreign officials for an improper advantage.

ELEMENTS OF A BRIBERY VIOLATION

With respect to the basic prohibition of bribery, there are five elements that must be met to constitute a violation:

- A regulated party
- Makes a payment or offer
- To a foreign official
- With corrupt intent
- For the purposes of influencing a business purpose

First, under the FCPA, U.S. jurisdiction over corrupt payments to foreign officials depends on whether the violator is a regulated party. That is, only regulated parties, such as issuers, domestic concerns, and foreign nationals or businesses, are subject to FCPA jurisdiction. An *issuer* is a corporation that has issued securities that have been registered in the United States or that is required to file periodic reports with the SEC.

A *domestic concern* is any citizen, national, or resident of the United States, or any business entity that has its principal place of business in the United States or that is organized under the laws of a state, territory, possession, or commonwealth of the United States. Moreover, the FCPA applies extraterritorially to U.S. citizens working for foreign subsidiaries of domestic companies.

Also, a foreign national or business is subject to the FCPA if it takes any act in furtherance of a corrupt payment within U.S. territory.

Additionally, the agents, subsidiaries, or other third-party representatives who act on behalf of an issuer, a domestic concern, or a foreign national or business are liable under the same conditions as the issuer, domestic concern, or foreign national or business.

Finally, U.S. parent companies (issuers or domestic concerns) may be held liable for the acts of foreign subsidiaries where they authorized, directed, or controlled the activity in question.

Second, the FCPA prohibits paying, offering, promising to pay, or authorizing to pay or offer money or anything of value to obtain or retain business. Thus, an offer or promise of a corrupt payment can violate the FCPA.

Under the FCPA, *anything of value* is broadly defined and can include any of the following:

- Money, cash, and cash equivalent
- Travel expenses and non-monetary gifts
- Charitable contributions or donations
- In-kind service
- Benefit to third persons with connection to government officials (e.g., scholarship to foreign official's relative)
- Overpayments for shares
- Loans at favorable interest rate

Third, the prohibition extends only to corrupt payments to a foreign official. The term *foreign official* means any officer or employee of a foreign government, a public international organization or any department or agency thereof, or any person acting in an official capacity. Foreign officials include:

- Members of any branch of a foreign government
- Employees of any entity substantially owned or controlled by a foreign government

- Consultants who hold government positions
- Any official or candidate of a foreign political party
- Officials of public international organizations

Fourth, to constitute a prohibited payment under the FCPA, the person making or authorizing it must have a corrupt intent. That is, it must be intended that the payment induce its recipient to misuse his official position to provide an improper business advantage.

Moreover, the government does not need to show that the defendant knew his conduct violated the FCPA, and corrupt intent can be inferred from the evidence.

Fifth, to constitute a violation, the payment must be made for a business purpose. That is, the payment must be made to assist the payer "in obtaining or retaining business for or with, or directing business to, any person." The U.S. government interprets this requirement broadly, and it covers payments made to secure a large variety of unfair business advantages, including obtaining or retaining contracts, influencing the procurement process, reducing or eliminating customs duties, securing favorable tax treatment, obtaining government action to prevent competitors from entering a market, influencing the adjudication of lawsuits or enforcement actions, obtaining exceptions to regulations, and circumventing a licensing or permit requirement.[2] The business to be obtained, however, does not need to be with a foreign government or foreign government instrumentality.

EXCEPTION FOR FACILITATING PAYMENTS

The FCPA does not prohibit all payments to foreign officials; it contains an explicit exception for certain types of payments, known as facilitating payments, or *grease payments,* made to expedite or secure performance of a routine governmental action by a foreign official, political party, or party official that relates to the performance of their ordinary and routine functions.

This exception is designed to allow companies to avoid liability where small amounts are paid to expedite certain routine, non-discretionary government acts. According to the DOJ and SEC's *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, examples of facilitating

[2] U.S. Department of Justice and U.S. Securities and Exchange Commission, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (Nov. 14, 2012).

payments include actions that are ordinarily and commonly performed by a foreign official in:

- Obtaining permits, licenses, or other official documents to qualify a person to do business in a foreign country
- Processing governmental papers, such as visas and work orders
- Providing police protection, mail pickup and delivery, or scheduling inspections associated with contract performance or inspections related to transit of goods across the country
- Providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products or commodities from deterioration

CRIMINAL ENFORCEMENT OF FCPA'S ANTI-BRIBERY PROVISIONS

The Department of Justice (DOJ) is responsible for all criminal enforcement of the FCPA. Under the anti-bribery provisions, corporations and other business entities are subject to a fine of up to $2 million per violation, while officers, directors, stockholders, employees, and agents are subject to a fine of up to $100,000 and imprisonment for up to five years. Fines imposed on individuals may not be paid by their employer or principal.

Furthermore, violators of the bribery provisions may be prohibited from participating in future federal contracts.

CIVIL ENFORCEMENT OF FCPA'S ANTI-BRIBERY PROVISIONS

Civil enforcement of the anti-bribery provisions of the FCPA is shared by the SEC and the DOJ. The primary civil enforcement tool is an injunction, though the FCPA also provides for monetary penalties. The maximum civil penalty for a violation by any firm, as well as by any officer, director, employee, or agent, is $10,000 per occurrence. In addition, in an SEC enforcement action, the court may impose an additional fine not to exceed the greater of (1) the gross amount of the pecuniary gain to the defendant as a result of the violation, or (2) a specified dollar limitation based on the flagrancy of the violation.

FCPA ACCOUNTING PROVISIONS (15 U.S.C. § 78m)

In addition to outlawing bribery payments, the FCPA contains separate accounting provisions for certain entities already subject to the FCPA provisions. The U.S. Congress enacted the FCPA's accounting provisions as an additional deterrent to bribery based on its conclusion that U.S. companies concealed most bribes in their corporate books. Essentially,

the accounting provisions are designed to compel corporate transparency to prevent publicly traded entities from disguising bribes as legitimate commercial transactions.

The accounting provisions, however, are more limited in scope than the anti-bribery provisions; they apply to all issuers (companies with securities listed in the U.S. trading markets) and their subsidiaries.

The FCPA imposes two requirements with respect to the accounting provisions. Issuers must maintain accurate books and records, and they must adopt internal controls to prevent the improper use of corporate funds.

In addition, the FCPA requires that a covered entity make a good-faith effort to ensure that any company, including joint ventures, in which the U.S. company or one of its subsidiaries holds 50 percent or less of the voting power comply with the FCPA accounting provisions.

BOOKS AND RECORDS (RECORDKEEPING) PROVISION

The first major requirement of the accounting provisions is that all issuers must accurately record all transactions, keep receipts and other support for transactions, and keep records in a manner consistent with overall document retention and recordkeeping policies.

In practice, the books and records provisions are used to prevent three types of improprieties:

- The failure to record improper transactions
- The falsification of records to conceal improper transactions
- The creation of records that are quantitatively correct, but fail to specify the qualitative aspects of a transaction that might reveal the true purpose of a particular payment

INTERNAL CONTROLS PROVISION

The internal controls provision is designed to prevent unauthorized or unrecorded transactions. Under the internal controls provision, a company must maintain robust compliance policies and must take reasonable steps to ensure that its affiliates maintain suitable internal controls.

The SEC has considered several factors to determine the adequacy of a system of internal controls. The factors include:

- The role of the board of directors
- Communication of corporate procedures and policies
- Assignment of authority and responsibility
- Competence and integrity of personnel
- Accountability for performance and compliance with policies and procedures
- Objectivity and effectiveness of the internal audit function

SEC REGULATIONS REGARDING THE ACCOUNTING PROVISIONS

The SEC, which has rulemaking authority over the accounting provisions, has adopted two regulations enforcing the accounting provisions. First, Rule 13b2-1 makes it unlawful to falsify accounts, providing that "[n]o person shall, directly or indirectly, falsify or cause to be falsified, any book, record or account" required to be kept under the accounting provisions of the FCPA. Second, the SEC established Rule 13b2-2, which makes it unlawful for directors and officers to omit material facts or supply false information to auditors in connection with any audit or document required to be filed with the SEC.

ENFORCEMENT OF THE ACCOUNTING PROVISIONS

The FCPA's accounting provisions are enforced by both the SEC and the DOJ. The SEC has authority to initiate civil enforcement actions and can impose civil fines and disgorgement on the company and individuals. The SEC has brought enforcement actions of the accounting provisions both in cases involving actual foreign bribes and in domestic transactions. The SEC can seek civil penalties of up to $500,000 for covered entities and $100,000 for individuals.

The DOJ is responsible for criminal prosecution of "willful" violations of the accounting provisions, and criminal penalties can include large fines and imprisonment. A willful violation of the accounting and controls provision is punishable by a fine up to $25 million against entities, and a fine up to $5 million and imprisonment up to 20 years against individuals.

Also, the FCPA provides that an individual may be held criminally liable for "knowingly" falsifying any book, records, or account, or circumventing or failing to implement a system of internal accounting controls. Knowing may include willful blindness or conscious attempts not to know. But no criminal liability is imposed for technical or insignificant accounting errors.

In addition, administrative and civil relief also is available for violations of the accounting provisions. A corporation or individual found in violation of the FCPA may be subject to debarment before many government agencies, and an indictment under the FCPA can also lead to the suspension of one's right to do business with the government or the immediate suspension of export licenses for military defense equipment.

It is common for FCPA enforcement actions to involve a series of prohibited payments, making the total amount of penalties very large. For example, the DOJ's enforcement action against the German conglomerate Siemens for violating the FCPA's accounting provisions led to a settlement of $800 million—$450 million in penalties and $350 million in profit disgorgement.

ANTI-CORRUPTION COMPLIANCE PROGRAMS

The FCPA encourages regulated organizations to implement effective compliance programs that are designed to prevent and detect criminal conduct. An *effective compliance program* is one that is reasonably designed, implemented, and enforced so that it will generally be effective in preventing and detecting criminal conduct. These programs are important because an organization that violates the FCPA is eligible for a reduced sentence if it has an effective compliance program.

In November 2012, the DOJ and SEC, which are responsible for enforcing the FCPA, jointly issued *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, which contains guidance on the FCPA. Among other things, the *Resource Guide* details the hallmarks of an effective corporate compliance program.

The *Resource Guide* states that the hallmarks of effective compliance programs are as follows:

- *Commitment from senior management and a clearly articulated policy against corruption*: Business managers must establish an ethical tone for the companies they lead, and organizations should have an anti-corruption policy that is clear.
- *Code of conduct and compliance policies and procedures*: Organizations should have a code of conduct and anti-corruption policies and procedures that are clear, practical, accessible, and enforceable.
- *Oversight, autonomy, and resources*: Organizations must develop a compliance infrastructure that includes designated responsibility to one or more senior corporate executives for implementing and overseeing the company's anti-corruption policies, standards, and

procedures, and those assigned responsibility for the program should be granted the autonomy, authority, and resources to manage the program, enforce the program's requirements, and react to issues that arise under the program.

- *Risk assessment*: Organizations should conduct a risk assessment addressing the nature and extent of the risks relating to bribery and corruption to which they are exposed and develop their anti-corruption standards and procedures based on the assessments.
- *Training and continuing advice*: Management must periodically and appropriately train all employees and third parties (agents, contractors, subcontractors, vendors, distributors, partners, etc.) about the program's compliance requirements and procedures.
- *Incentives and disciplinary measures*: Organizations establish and adhere to a system of disciplinary measures for rule breakers and incentives for those who demonstrate good behavior.
- *Third-party due diligence and payments*: To the extent that an organization uses third parties, including agents, consultants, and distributors, it must implement appropriate due diligence and compliance requirements for the retention of such agents and business partners.
- *Confidential reporting and internal investigation*: Organizations should establish and communicate a reporting system whereby employees and other agents can confidentially report actual or potential criminal conduct without fear of retribution.
- *Continuous improvement*: Organizations should review and improve their compliance program's standards and procedures, including internal controls, ethics, and compliance programs, on a regular basis.

The United Kingdom Bribery Act

Parliament passed the UK Bribery Act in May 2010, updating the nation's anti-corruption laws for the first time in more than a century. The Bill received Royal Assent on April 8, 2010, and went into effect on July 1, 2011.

The Bribery Act is the United Kingdom's analogue of the FCPA, although with several distinctions. Both the UK Bribery Act and the FCPA make it a crime to offer foreign public officials bribes or to accept bribes from them in connection with international business transactions, and their prohibitions on bribing foreign government officials are broadly comparable. Thus, like the FCPA, the Bribery Act seeks to punish corruption on a global level, but the Bribery Act has an even broader application than the FCPA.

Also, the FCPA and the UK Bribery Act encourage regulated organizations to implement effective anti-corruption programs that are designed to prevent and detect corrupt conduct. But again, the Bribery Act is broader than the FCPA; even if an organization's anti-corruption program is sufficiently robust for the purpose of complying with the FCPA, it might not be sufficient for the purpose of complying with the UK Bribery Act. Therefore, it is important for international organizations to be aware of the differences between the FCPA and the Bribery Act.

In short, the Bribery Act contains a specific offense for the bribery of foreign public officials; it contains a general commercial bribery offense; and it creates a corporate offense of failure to prevent bribery.

SCOPE

Like the FCPA, the Bribery Act exercises broad jurisdiction over all individuals and corporate entities for acts of corruption when any part of the offense occurs in the UK. Furthermore, liability exists for acts committed outside the UK by individuals and entities with a close connection to the UK, including:

- British citizens, overseas citizens, overseas territories' citizens, and any person declared a British subject under the 1981 British Nationality Act
- Individuals who normally reside in the UK
- An entity incorporated under the law of any part of the UK

More specifically, foreign companies that have offices in the UK, employ UK citizens, or provide any services to a UK organization are responsible for complying with the UK Bribery Act. A listing on the London Stock Exchange will not, in itself, subject a company to the Act.

Therefore, any organization with any connection with the UK should assess and revise their anti-corruption programs with the Bribery Act's new standards and guidance in mind.

THREE CATEGORIES OF OFFENSES

The Bribery Act creates three categories of offenses:

- Bribing a foreign public official
- General commercial bribery offenses
- A corporate offense of failure to prevent bribery

BRIBERY OF FOREIGN OFFICIALS

Like the FCPA, the UK Bribery Act makes it an offense to bribe a foreign public official for the purpose of obtaining or retaining business or an advantage in the course of business. A *foreign public official,* as defined by the Act, is anyone who:

- Holds a legislative, administrative, or judicial position, either by election or appointment, in a country or territory outside the UK
- Exercises a public function for a country or territory outside the UK
- Acts as an official or agent for a public international organization

GENERAL COMMERCIAL BRIBERY

One way in which the Bribery Act has a broader application than the FCPA is that it covers bribery on a private level. That is, the Bribery Act, unlike the FCPA, has a commercial bribery offense. Whereas the FCPA only prohibits bribes involving foreign government officials, the Bribery Act goes further by making commercial bribery—bribes paid to people working in the private sector—a crime. Additionally, a person who improperly performs a relevant function in anticipation of receiving a benefit commits a general commercial bribery offense.

FAILURE TO PREVENT BRIBERY

The UK Bribery Act also creates an offense for the failure of a corporate entity to prevent bribery committed by associated persons. The term *associated persons* refers to any individual who performs services for or on behalf of the company, such as an employee, agent, or subsidiary.

A company can be liable for failing to prevent bribery offenses committed by associated persons if the corrupt act was for the purpose of securing or retaining business or some advantage for the company.

This is a *strict liability offense*, which means that no criminal intent is required (the government must prove only that the defendant performed the act; it does not have to prove that the defendant performed the conduct with any particular mental state).

The failure to prevent bribery is subject to a defense of having adequate procedures in place to prevent acts of bribery by associated persons. Unfortunately, the Bribery Act does not define *adequate procedures*, but the UK government provided guidance on what constitutes adequate procedures.

The UK's Ministry of Justice published final guidance for consultation as to what might constitute *adequate procedures*. In short, to be adequate, the procedures should be reasonably designed, implemented, and enforced so that they will generally be effective in preventing and detecting criminal conduct.

Specifically, the Ministry of Justice provided six principles to guide organizations to access the defense:

- *Proportionality*: Procedures in place should be proportional to the risk and size of the business; large businesses in industries with high risks of corruption need relatively higher measures than small companies with lower risks.
- *Top-level commitment*: High-level management should take an active role in demonstrating that the organization does not tolerate bribery.
- *Risk assessment*: Management accessed research in the organization's industry and places of business to determine the level of risk for bribery.
- *Due diligence*: The organization's management should know who it does business with, which might require gathering background information on trade partners (the focus is on trade partners that perform services on behalf of the organization).
- *Communication*: This includes communicating policies not only to employees, but to others who perform services for the organization; it also includes continued training
- *Monitoring and review*: There should be periodic reviews of anti-bribery measures to keep them modern and reviews when entering new markets or other new forms of risk.

NO FACILITATION PAYMENTS EXCEPTION

Another way that the UK Bribery Act has broader application than the FCPA concerns facilitating payments. The FCPA does not prohibit all payments to foreign officials; it contains an explicit exception for facilitating payments made to expedite or secure performance of a routine governmental action. The Bribery Act, however, makes no such exception.

ENFORCEMENT

The Serious Fraud Office (SFO) is responsible for enforcement of the Act. SFO enforcement is limited, but it has stated that one of its primary purposes is to level the playing field for UK companies that are complying with the law.

The Bribery Act establishes severe penalties for violations. An individual convicted of either general bribery or the bribery of a foreign public official faces a penalty of up to 10 years'

imprisonment and a fine. A company convicted of either general bribery or the bribery of a foreign public official faces a fine. The failure to prevent an act of bribery by an associate party is also punishable by a fine. Note that the Bribery Act does not establish any upper limits on the fines that may be imposed.

FCPA VERSUS UK BRIBERY ACT

The chart below compares key provisions of FCPA with the UK Bribery Act.

	FCPA	Bribery Act
Bribery of Private Entities	Applies to bribery of foreign government officials	Prohibits bribes paid to any person (not limited to foreign officials)
Corrupt Intent	Requires corrupt intent	Does not require corrupt intent
Corporate Strict Liability	Bribery charges must prove intent or negligence	Strict corporate liability offense for the failure to prevent bribery
Facilitating Payments	Exception for facilitating payments	No exception for facilitating payments

International Anti-Money Laundering Instruments

There are a number of international instruments related to money laundering. These include:

- Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering
- FATF's Nine Special Recommendations on Combating Terrorist Financing
- UN Convention Against Transnational Organized Crime
- Instruments developed by the Egmont Group of Financial Intelligence Units
- Instruments developed by the International Monetary Fund/World Bank

For more information on the various international instruments related to money laundering, see the "Money Laundering" chapter in this section of the *Fraud Examiners Manual*.

International Banking and Financial Systems

There are international instruments in the area of banking and financial system regulation and supervision, including:

- International Organization of Securities Commissions' (IOSCO) Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information

- Basel Committee on Banking Supervision Core Principles for Effective Banking Supervision
- Basel Committee on Banking Supervision Core Principles Methodology

Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information

In 2002, the International Organization of Securities Commissions (IOSCO), an international organization comprising securities commissioners and administrators responsible for securities regulation and the administration of securities laws in their respective countries, approved a multilateral agreement on cooperation and global information exchange within the international community of securities regulators.

The agreement, known as the Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (IOSCO MMoU), was the first international standard for cooperation in dealing with breaches of stock exchange regulations.

IOSCO MMoU represents a common understanding amongst the signatory parties about how they will confer, collaborate, and exchange information for securities regulatory enforcement purposes. That is, IOSCO MMoU was designed to facilitate cross-border enforcement and exchange of information amongst stock exchange supervisory authorities.

IOSCO MMoU provides for different forms of co-operation, including assistance in obtaining statements, exchange of information upon request, and spontaneous exchange of information.

Core Principles for Effective Banking Supervision

The Core Principles for Effective Banking Supervision is a set of supervisory guidelines the Basel Committee on Banking Supervision developed to provide a general framework for effective banking supervision. That is, they were designed to help countries assess their banking supervisory systems and identify areas for improvement and to promote more consistent and effective bank supervision in all countries. The Core Principles for Effective Banking Supervision also serve as a reference document for national supervisors and international institutions.

Core Principles Methodology

The Core Principles Methodology, which the Basel Committee on Banking Supervision developed along with the Core Principles for Effective Banking Supervision, serves as a tool for assessing compliance with the Core Principles for Effective Banking Supervision.

BANKRUPTCY (INSOLVENCY) FRAUD

Introduction

If a party, such as a person or business, cannot repay the debts it owes to creditors, it may file for bankruptcy to initiate a process whereby it can resolve its debts. While the types of parties that may file for bankruptcy vary by jurisdictions, it is common for individuals, corporations, limited liability companies, partnerships, and other entities to be able to file for bankruptcy. For debtors, the biggest benefit of filing for bankruptcy is the discharge of debts. When a debt is discharged, the debtor is no longer required to pay it, and creditors cannot collect on it.

Bankruptcy fraud occurs when an individual or organization makes false or misleading representations in the course of petitioning for debt relief. Bankruptcies are governed by legislation, and illegal conduct related to bankruptcies is almost always a criminal offense.

Bankruptcy proceedings often play a substantial role in fraud examinations for two reasons. First, there are many fraud schemes that are perpetrated using the bankruptcy system. Additionally, for any investigation into financial crimes, fraud examiners need to be able to consider the role that bankruptcy might play if attempting to recover the victim's assets.

Key Parties in the Bankruptcy System

Debtors

A *debtor* is an individual, partnership, corporation, or municipality who is the subject of a bankruptcy filing. *Municipality* refers to a political subdivision, public agency, or instrumentality of a state.

Debtors might have different goals in seeking bankruptcy. For example, a debtor seeks a liquidation bankruptcy (e.g., Chapter 7 bankruptcy in the United States) to be relieved of all dischargeable debts and allowed to start over with a clean slate. But a debtor files for a reorganization bankruptcy (e.g., Chapter 11 bankruptcy in the United States) if, despite its financial problems, it wants to reorganize and continue operating as a business. (Liquidation and reorganization bankruptcies are discussed in more detail below.)

Creditors

A *creditor* is a person to whom money is owed by a debtor.

Many jurisdictions, including the United States, recognize a distinction between secured and unsecured creditors during bankruptcy proceedings.

Secured Creditors

A *secured creditor* is one who has a secured interest in some of the debtor's property, meaning that if the debtor defaults on payments to the creditor, the creditor may possess or liquidate the secured property to satisfy the debt.

Creditors typically prefer to have secured interests because such claims have priority over unsecured claims and normally get paid first in the distributions to creditors made by the trustee or debtor-in-possession. The most common example of a secured interest occurs when a lender finances a debtor's purchase of a particular property (e.g., a home or vehicle) and, as part of the debt agreement, takes a collateral interest in the financed property.

The method of establishing oneself as a secured creditor varies from jurisdiction to jurisdiction. There might be a filing requirement to register a financing statement with a public registry or a government agency.

A secured creditor's claim is secured to the extent of the property's value. When the debt is undersecured (the debt is secured by property that is worth less than the amount of the debt), the debt will be considered both unsecured and secured. For example, if a note for $500 is secured by property having a value of $400, there will be a secured claim for $400 and an unsecured claim for $100.

Unsecured Creditors

An *unsecured creditor* is one that does not have any secured interests in the debtor's assets. If the debtor goes into bankruptcy, secured creditors receive payment before unsecured creditors. That is, in jurisdictions that recognize a distinction between secured and unsecured creditors, the secured creditors are entitled to payment before unsecured creditors in bankruptcy proceedings.

Courts

In many countries, bankruptcy is a court process. For example, in the United States, the United Kingdom, and Australia, bankruptcy is a formal, court-governed process available to eliminate and reorganize debt.

U.S. Bankruptcy Courts

Bankruptcy is a federal court process in the United States. All bankruptcy cases are filed in federal court, and almost all are filed in the local district of the U.S. bankruptcy court. U.S. district courts have jurisdiction over bankruptcy proceedings, but in practice, virtually all cases are deferred to the U.S. bankruptcy courts. Although bankruptcy courts are federal courts, they do not derive their power from Article III of the Constitution. Article III courts include the U.S. district courts, the U.S. Circuit Courts of Appeal, and the U.S. Supreme Court. Instead, bankruptcy courts derive their power from Article I (congressional powers). Article III states that judicial power of the United States rests with the Supreme Court and in inferior courts established by Congress.

Bankruptcy courts are not contemplated within this scheme as "inferior" courts, but they are considered as an adjunct to "inferior" U.S. district courts.

Bankruptcy judges hear all cases involving debtors' and creditors' rights, approve plans of reorganization, award fees to professionals, and conduct hearings and trials when necessary to resolve disputes.

United Kingdom

In the United Kingdom, bankruptcy petitions are usually presented in the High Court in London or in a county court near to where the filing party lives or trades.

Australia

In Australia, bankruptcy cases may be heard by the Federal Court or the Federal Circuit Court.

Bankruptcy Agencies

Some countries have government agencies that are responsible for overseeing bankruptcies. For example, in the United States, the Office of the United States Trustee (UST) is responsible for administering bankruptcy cases. In Canada, the Office of the Superintendent

of Bankruptcy (OSB) is a federal agency tasked with ensuring that bankruptcies are administered in a fair and orderly manner.

The Office of the United States Trustee

The Office of the United States Trustee (UST) is a Department of Justice (DOJ) agency that is responsible for administering bankruptcy cases; appointing trustees, examiners, and Chapter 11 committees; overseeing and monitoring trustees; reviewing employment and fee applications; and appearing in court on matters of interest to the estate and creditors.

The Office of the UST is subdivided into 21 regions, each made up of one or more federal districts. Each region consists of a U.S. Trustee (or an Assistant Trustee in several regions). The Office of the UST in each region principally is comprised of staff attorneys, bankruptcy analysts (including accountants), and, in some instances, special investigative units. *Staff attorneys* review pleadings (e.g., fee applications and motions to appoint trustees and examiners) and represent the UST on these matters.

Bankruptcy analysts analyze and review operating reports and other relevant financial information and, in general, oversee the debtor's case to ensure compliance with the Bankruptcy Code and to protect the assets of the estate.

Special investigative units investigate criminal referrals (complaints) in bankruptcy cases. In some cases, they work with criminal investigative agencies, such as the Federal Bureau of Investigation and the Internal Revenue Service Criminal Investigative Division.

The Office of the Superintendent of Bankruptcy in Canada

The Office of the Superintendent of Bankruptcy (OSB) is a federal agency that seeks to protect the integrity of Canada's bankruptcy and insolvency system. It engages in the following activities:

- Supervises the administration of estates in bankruptcy, commercial reorganizations, and receiverships under bankruptcy and insolvency legislation
- Maintains public records of bankruptcy and insolvency proceedings
- Licenses private-sector trustees to administer estates in bankruptcy
- Records and investigates complaints regarding possible wrongdoing by someone involved in the bankruptcy or insolvency processes
- Sets and enforces professional standards for the administration of estates in bankruptcy

- Promotes awareness of the rights and responsibilities of those involved in the bankruptcy and insolvency system

Bankruptcy Trustees

Some countries, such as the United States, the United Kingdom, and Canada, use trustees to administer bankruptcy estates. A *trustee* is an entity that holds property, authority, or a position of trust for the benefit of another entity. A *bankruptcy trustee* is neutral professional assigned to administer an estate in bankruptcy.

Panel Trustees in the U.S. Bankruptcy System

The U.S. bankruptcy system maintains a list of private, individual professionals (usually attorneys) that act as bankruptcy trustees (often called panel trustees) in Chapter 7 bankruptcies. Trustees also might serve in Chapter 11 cases where operation of the debtor's business is considered appropriate. (Chapter 7 and Chapter 11 bankruptcy cases are discussed in more detail below.) Trustees or others might develop a plan of reorganization to conclude the Chapter 11 proceedings, but if the business in a Chapter 11 bankruptcy cannot be reorganized, the trustee might petition the presiding court to convert the case to Chapter 7 or develop a plan of liquidation under Chapter 11.

The duties of a trustee are specifically enumerated in Title 11, U.S.C., Section 704 (in Chapter 7 cases) and Title 11, U.S.C., Section 1106 (in Chapter 11 cases). The duties of a trustee are as follows: administer assets of the estate; liquidate assets; pay creditors; litigate matters where necessary; have the right to sue and be sued; conduct hearings; conduct investigations of financial affairs of the debtor; file reports as required by the Office of the UST; and, where appropriate, file criminal referrals with the U.S. Attorney's Office.

A trustee's compensation is statutorily defined under the Bankruptcy Code.

Bankruptcy Trustees in the Canadian Bankruptcy System

In Canada, bankruptcy trustees are licensed and regulated by the Office of the Superintendent of Bankruptcy. Some of the duties of trustees in a bankruptcy include:

- Arranging mandatory counseling for the debtor
- Presiding over meetings of creditors
- Selling nonexempt assets
- Objecting to the debtor's discharge
- Distributing the debtor's property among the creditors

Official Receivers in UK Bankruptcy Proceedings

In the United Kingdom, Official Receivers are trustees appointed by the courts in bankruptcy proceedings who are charged with overseeing liquidation and using any proceeds to pay outstanding debts on the bankrupt party's behalf. An Official Receiver is also typically responsible for:

- Investigating the bankrupt party's financial affairs and conduct and reporting findings from such investigatory efforts to the court
- Protecting the bankrupt party's estate
- Obtaining custody of the bankrupt party's property and assets of worth

Types of Bankruptcy Filings

The structure of bankruptcy proceedings varies by jurisdiction, so it is important to study the rules of the relevant jurisdiction when dealing with potential bankruptcy fraud. However, there are common types of bankruptcy filings, and most countries have adopted a similar version of at least one. The particular terms might change, but three common types of bankruptcy designed to deal with different debt situations are liquidation, reorganization, and debt adjustment.

Liquidation

Liquidation is the most basic type of bankruptcy proceeding and involves accounting for all dischargeable debts the subject owes, identifying all of the subject's assets, and liquidating nonexempt assets to pay off creditors. This process allows the debtor to get a court or administrative order under which some or all of his debts may be eliminated.

Each jurisdiction determines what exceptions there are in terms of debts that may not be discharged and assets that may not be liquidated. Some debts, like taxes owed or child support payments, might be non-dischargeable, meaning the bankruptcy will not wipe these debts away. Typical items that may not be liquidated include the debtor's primary residence, items of nominal value, or assets deemed necessary for the debtor to maintain employment.

However, there might be exceptions to protected assets that allow creditors to reach them. Frequently, bankruptcy laws will not protect assets that were obtained through fraudulent means, even if they are normally subject to protection. The laws might also only protect assets up to a certain amount (e.g., a debtor's luxury home is liquidated in bankruptcy and he is only entitled to 20 percent of the sale price).

Reorganization

Unlike liquidation, which seeks to give the debtor a fresh start, the purpose of *reorganization* bankruptcies is to allow the debtor breathing room from creditors so that the debtor can reorganize its financial affairs and continue as a going concern. The hope is that the debtor will be able to pay the creditors back more of the debt in the long run by staying in business than if the entire business was ended and liquidated. However, debt is often restructured and reduced to some extent. Some reorganization proceedings involve putting the debtor's business under receivership for a certain period to ensure as much debt is paid back as possible.

Reorganization bankruptcies are growing more popular, with many countries allowing business entities to declare bankruptcy using this method. Some countries also allow individuals to use reorganization.

Debt Adjustment

Debt adjustment is another alternative to liquidation that allows a debtor pay off his debts over time in accordance with a court-approved plan. Under this type of case, the debtor may keep certain property that he would not be allowed to retain in a liquidation bankruptcy. Typically, the court reviews the debtor's financial situation and comes up with a plan to repay creditors. This type of bankruptcy, if available, is primarily for individuals.

Bankruptcy Schemes

Bankruptcy fraud can take on many forms. But generally, bankruptcy fraud occurs when an individual knowingly engages in prohibited conduct during the pendency of a bankruptcy proceeding with a fraudulent intent to defeat the bankruptcy laws.

The following are some common bankruptcy schemes.

Concealed Assets

The most common type of bankruptcy fraud scheme involves the concealment of assets rightfully belonging to the debtor's estate to avoid forfeiting the assets in bankruptcy. In these schemes, concealed assets might include cash, consumer property, houses, and interests in partnerships and corporations, as well as lawsuits in which the debtor is a plaintiff. Concealed assets might also include the debtor's books and records.

The Planned Bustout

A *bustout* is a planned and fraudulent bankruptcy. It can take many different forms, but the basic approach is for an apparently legitimate business to order large quantities of goods on credit, and then dispose of those goods through legitimate or illegitimate channels. Since the point of the bustout scheme is to quickly resell the goods for cash, the fraudster is much more likely to purchase more liquid items like inventory than real estate, insurance policies, or services. The perpetrator then closes shop, absconding with the proceeds and leaving the suppliers unpaid. The debtor might then go into bankruptcy. Often, by this point the debtor has already made false accounting entries or taken other steps to conceal the assets or make the sales look legitimate. Other times, debtors simply flee the jurisdiction or do not show up at the proceedings.

Bustout schemes are planned and perpetrated by individuals both before and after the formation of the new business entity. Other characteristics of bustout schemes include:

- They are planned from the beginning.
- Sometimes organized crime is involved.
- Credit is established with numerous vendors; prompt payments are made to all vendors; and vendors feel comfortable in dealings, thereby extending existing credit lines.
- Perpetrators build inventory by ordering everything they can from vendors; they promise to pay soon and order more merchandise.
- Perpetrators sell out inventory at deep discount or move it before vendors can take possession of it.
- The business fails or closes up, files bankruptcy, or creditors beat them to it with involuntary bankruptcy.

Detection

Some red flags that signal that a bustout scheme might be in process include:

- A business relationship based principally on trust: Creditors are willing to offer extended terms for payment, hold checks, or take post-dated checks. This makes them vulnerable.
- Buyers with a history of purchasing goods for an unreasonable discount
- A large number of bank accounts, indicating a possible kiting scheme: The perpetrator occasionally pays some of his creditors with funds generated by floating checks between bank accounts.
- Inexplicably large purchases of inventory or goods (e.g., perishable goods that could not likely be sold to customers before going bad)

Prevention

To help prevent this type of bankruptcy fraud, lenders and suppliers should evaluate potential customers carefully before extending credit by performing due diligence and obtaining detailed background information. Lenders and suppliers should at times visit their customers' locations to verify the legitimacy of the businesses.

Multiple Filings

Multiple filing schemes occur when the same debtor files for bankruptcy several times, using either false information or real information in several different jurisdictions. Generally, debtors will make multiple filings to obtain an automatic stay, which occurs at the beginning of a bankruptcy proceeding and prevents creditors from continuing attempts to collect debts from the petitioner. The automatic stay occurs once the bankruptcy case has been commenced. Usually, in these schemes, the petitions are dismissed for failure to file the required statements or to appear for examination. False statements on petitions are common, including a denial that the debtor has filed any previous petition.

Credit Card Bustout

In a credit card bustout scheme, the debtor intentionally runs up a number of credit cards to their limit and files bankruptcy with no intent to repay. The credit card debts might include purchases for jewelry, luxury items, or other personal property that are not disclosed on the schedules. Credit card debt also might include large cash advances taken prior to filing the bankruptcy petition.

Forged Filings

Bankruptcy petitions are sometimes filed using forged documents, and often, the filings are made using stolen identities, usually as part of a larger scheme using an assumed identity. If someone files for bankruptcy using a stolen identity, it can take years to correct the credit records of the person whose identity was stolen. Alternatively, a debtor might file for bankruptcy using a name obtained from obituary notices.

Typing Services or Petition Mills

These schemes involve companies that file bankruptcy petitions on behalf of others. Typically, these entities target low-income and unsuspecting clients, and to obtain cooperation, they might promise to erase the person's poor credit record or offer some other bogus financial service. Often, in these schemes, the filing entity has held itself out to be a renter's rights group and has not told the client how it will accomplish what it has

promised. And, in some cases, the debtor is not even aware of the filing or the effect that a bankruptcy will have on his credit rating.

Additionally, to carry out these schemes, the petition mill might file false documents for debtors with deliberately wrong government identification numbers or other incorrect information. The petitions filed in these schemes often contain numerous false statements.

Cross-Border Insolvency Regimes

Many of the world's major economies are subject to some form of cross-border insolvency regime for handling cross-border insolvencies. A *cross-border insolvency* is an insolvency in which the insolvent debtor has assets in more than one country or where some of the insolvent debtor's creditors are from different countries. *Cross-border insolvency regimes* are legal frameworks designed to address cross-border insolvency proceedings, and the lack of such regimes often results in cross-border insolvencies being dealt with through inadequate and unorganized approaches that are unpredictable and time-consuming.

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Cross-Border Insolvency is a model law that established the international standard for cross-border insolvency frameworks. Twenty-three jurisdictions have adopted legislation based on the Model Law, including the United States, Japan, the United Kingdom, Australia, Canada, and South Korea. The Model Law was designed to assist countries in equipping their insolvency laws with a legal framework that can effectively address cross-border insolvency proceedings.

In addition, all member states of the European Union are bound by the EU Insolvency Regulation, which establishes a regional cross-border insolvency regime for insolvency cases arising within the EU.

There is, however, an absence of cross-border insolvency regimes in major emerging economies. In particular, none of the BRIC countries (Brazil, Russia, India and China) have adopted any regimes for handling cross-border insolvencies.

The World Bank Principles

Introduction

To improve the stability of the international financial system, the World Bank developed the *Principles and Guidelines for Effective Insolvency and Creditor Rights Systems* (the World Bank Principles) to assist countries in developing sound insolvency systems.

Effective insolvency systems are important to a financial system's stability because they promote economic expansion and competition by cultivating robust credit cultures and permit economies to take timely efforts in cases of default and delinquency.

The World Bank Principles provide fundamentals applicable to national insolvency systems and are a distillation of international best practice on design aspects of these systems, emphasizing contextual, integrated solutions, and the policy choices involved in developing those solutions.

Before the World Bank Principles were published, the United Nations Commission on International Trade Law (UNCITRAL), an international organization established to harmonize laws and reduce barriers to international trade, approved a proposal to adopt the Legislative Guide on Insolvency Law (UNCITRAL Guide). The UNCITRAL Guide, which the United Nations General Assembly later endorsed in 2004, explains the key elements of effective insolvency law and provides recommendations on the content of such law. UNCITRAL's Guide is designed to help government establish new laws and assess the effectiveness of existing laws and regulations.

The World Bank Principles and the UNCITRAL Guide are complementary in nature, and it was therefore proposed to incorporate UNCITRAL's Guide into the standards and codes that are used to evaluate national insolvency systems. The result is the Creditor Rights and Insolvency Standard, revised in 2011.

Objectives and Scope of the World Bank Principles

The World Bank Principles were designed to assist countries in evaluating and improving core aspects of their commercial law systems that are fundamental to a sound investment climate, and to promote commerce and economic growth.

National systems depend on a range of structural, institutional, social, and human foundations to make a modern market economy work. There are as many combinations of these variables as there are countries, though regional similarities have created common customs and legal traditions. The World Bank Principles embody several fundamental propositions, including:

- *Effective systems respond to national needs and problems*. These systems must be rooted in the country's broader cultural, economic, legal, and social context.
- *Transparency, accountability, and predictability are fundamental to sound credit relationships*. Capital and credit, in their myriad forms, are the lifeblood of modern commerce. Investment and availability of credit are predicated on both perceptions and the reality of risks. Competition in credit delivery is handicapped by lack of access to accurate information on credit risk and by unpredictable legal mechanisms for debt enforcement, recovery, and restructuring.
- *Legal and institutional mechanisms must align incentives and disincentives across a broad spectrum of market-based systems—commercial, corporate, financial, and social*. This calls for an integrated approach to reform, taking into account a wide range of laws and policies in the design of insolvency and creditor rights systems.

The World Bank Principles emphasize contextual, integrated solutions, and the policy choices involved in developing those solutions. Adapting international best practices to the realities of countries requires an understanding of the market environments in which these systems operate. This is particularly apparent in the context of developing countries, which are exposed to many challenges, including weak or unclear social protection mechanisms, weak financial institutions and capital markets, ineffective corporate governance and uncompetitive businesses, ineffective and weak laws, institutions and regulation, and a shortage of capacity and resources.

These obstacles pose enormous challenges to the adoption of systems that address the needs of developing countries while keeping pace with global trends and good practices. The application of the World Bank Principles at the country level will be influenced by domestic policy choices and by the comparative strengths (or weaknesses) of applicable laws, institutions, and regulations, as well as by capacity and resources.

The World Bank Principles also highlight the relationship between the cost and flow of credit (including secured credit) and the laws and institutions that recognize and enforce credit agreements, and they outline key features and policy choices relating to the legal

framework for risk management and informal corporate workout systems, formal commercial insolvency law frameworks, and the implementation of these systems through sound institutional and regulatory frameworks.

Additionally, the World Bank Principles embrace practices that have been widely recognized and accepted as good practices internationally. As markets evolve and competition increases globally, countries must adopt and evolve to maximize their own advantages for commerce and to attract investment by adopting laws and systems that create strong and attractive investment climates.

Following is a brief summary of the key elements of the World Bank Principles.

Legal Framework for Creditor Rights

Compatible Credit and Enforcement Systems

A regularized system of credit should be supported by mechanisms that provide efficient, transparent, and reliable methods for recovering debt. These methods can include seizure and sale of immovable and movable assets and sale or collection of intangible assets, such as debt owed to the debtor by third parties. An efficient system for enforcing debt claims is crucial to a functioning credit system, especially for unsecured credit.

A creditor's ability to take possession of a debtor's property and to sell it to satisfy the debt is the simplest, most effective means of ensuring prompt payment. It is far more effective than the threat of an insolvency proceeding, which often requires a level of proof and a prospect of procedural delay that make it not credible to debtors as leverage for payment.

While much credit is unsecured and requires an effective enforcement system, an effective system for secured rights is especially important in developing countries. Secured credit plays an important role in industrial countries, notwithstanding the range of sources and types of financing available through both debt and equity markets. In some cases equity markets can provide cheaper and more attractive financing. But developing countries offer fewer options, and equity markets are typically less mature than debt markets. As a result most financing is in the form of debt. In markets with fewer options and higher risks, lenders routinely require security to reduce the risk of non-performance and insolvency.

Collateral Systems

One of the pillars of a modern credit economy is the ability to own and freely transfer ownership interests in property. Granting a security interest to credit providers, with respect to such interests and rights, provides access to credit at more affordable prices. For instance, a bank that provides a loan to someone for the purpose of buying a home typically takes a security interest in the home, making the transaction less risky for the bank and, therefore, less expensive for the homebuyer. Secured transactions play an enormously important role in a well-functioning market economy.

Laws on secured credit mitigate lenders' risks of default and as a result increase the flow of capital and facilitate low cost financing. Discrepancies and uncertainties in the legal framework governing security interests are the main reasons for high costs and unavailability of credit, especially in developing countries.

The legal framework for secured lending addresses the fundamental features and elements for the creation, recognition, and enforcement of security interests, including both possessory and non-possessory interests, in all types of assets on a global basis. This includes movable and immovable assets, as well as those that are tangible and intangible (including inventories, receivables, proceeds, and future property). The law should encompass any or all of a debtor's obligations to a creditor, present or future, and between all types of persons. In addition, it should provide for effective notice and registration rules that can be adapted to all types of property, and clear rules of priority on competing claims or interests in the same assets. For security rights and notice to third parties to be effective, they must be capable of being publicized at reasonable costs and be easily accessible to stakeholders. A reliable and affordable public registry system is essential to promote optimal conditions for asset-based lending. Where several registries exist, the registration system should be integrated to the maximum extent possible so that all notices recorded under the secured transactions legislation can be easily retrieved.

Enforcement Systems

A modern, credit-based economy requires predictable, transparent, and affordable enforcement of both unsecured and secured credit claims by efficient mechanisms outside of insolvency, as well as a sound insolvency system. These systems must work in harmony. Commerce is a system of commercial relationships predicated on express or implied contractual agreements between an enterprise and a wide range of creditors and constituencies. Although commercial transactions have become increasingly complex as

more sophisticated techniques are developed for pricing and managing risks, the basic rights governing these relationships and the procedures for enforcing these rights have not changed much. These rights enable parties to rely on contractual agreements, fostering confidence that fuels investment, lending, and commerce. Conversely, uncertainty about the enforceability of contractual rights increases the cost of credit to compensate for the increased risk of non-performance or, in severe cases, leads to credit tightening.

Legal Framework for Insolvency

Though approaches vary, effective insolvency systems have a number of aims and objectives. Systems should aspire to the following:

- Integrate with a country's broader legal and commercial systems
- Maximize the value of a firm's assets and recoveries by creditors
- Provide for both efficient liquidation of nonviable businesses and those where liquidation is likely to produce a greater return to creditors and reorganization of viable businesses
- Strike a careful balance between liquidation and reorganization, allowing for easy conversion of proceedings from one proceeding to another
- Provide for equitable treatment of similarly situated creditors, including similarly situated foreign and domestic creditors
- Provide for timely, efficient, and impartial resolution of insolvencies
- Prevent the improper use of the insolvency system
- Prevent the premature dismemberment of a debtor's assets by individual creditors seeking quick judgments
- Provide a transparent procedure that contains, and consistently applies, clear risk allocation rules and incentives for gathering and dispensing information
- Recognize existing creditor rights and respect the priority of claims with a predictable and established process
- Establish a framework for cross-border insolvencies, with recognition of foreign proceedings

Where an enterprise is not viable, the main thrust of the law should be swift and efficient liquidation to maximize recoveries for the benefit of creditors. Liquidations can include the preservation and sale of the business, as distinct from the legal entity. On the other hand, where an enterprise is viable, meaning it can be rehabilitated, its assets are often more valuable if retained in a rehabilitated business than if sold in a liquidation. The rescue of a business preserves jobs, provides creditors with a greater return based on higher going

concern values of the enterprise, potentially produces a return for owners, and obtains for the country the fruits of the rehabilitated enterprise. The rescue of a business should be promoted through formal and informal procedures. Rehabilitation should permit quick and easy access to the process, protect all those involved, permit the negotiation of a commercial plan, enable a majority of creditors in favor of a plan or other course of action to bind all other creditors (subject to appropriate protections), and provide for supervision to ensure that the process is not subject to abuse. Modern rescue procedures typically address a wide range of commercial expectations in dynamic markets.

Though insolvency laws may not be susceptible to fixed formulas, modern systems generally rely on design features to achieve the objectives outlined above.

Selected Anti-Fraud Requirements

Under the World Bank Principles, countries should adopt the following anti-fraud policies.

Administrative Powers

Most bankruptcy processes, whether through a court or otherwise, involve granting a person or group administrative powers to oversee the processes. The name of this appointee varies among jurisdictions, but often is called the *administrator*, *trustee*, *receiver*, *examiner*, or *supervisor*. The World Bank Principles recommend that the administrator have broad powers, including:

- Right to cancel fraudulent contracts or transactions entered into by the debtor
- Powers to collect, preserve, and dispose of the debtor's property
- Ability to interfere with contracts to meet the objectives of the insolvency process
- Powers to examine the debtor, the debtor's agents, or other people with knowledge of the debtor's affairs and compel them to provide relevant information

Governance and Management

In liquidation proceedings, management should be replaced by an independent insolvency representative with authority to administer the estate in the interest of creditors. Control of the estate should be surrendered immediately to the insolvency representative. In creditor-initiated filings, where circumstances warrant, an interim administrator with limited functions should be appointed to monitor the business to ensure that creditor interests are protected.

There are typically three preferred approaches in reorganization proceedings:

- Exclusive control of the proceeding is entrusted to an independent insolvency representative

- Governance responsibilities remain invested in management
- Supervision of management is undertaken by an impartial and independent insolvency representative or supervisor.

Under the second and third approaches, complete administration power should be shifted to the insolvency representative if management proves incompetent, negligent, or has engaged in fraud or other misbehavior.

Avoidable Transactions

After the commencement of an insolvency proceeding, transactions by the debtor that are not consistent with the debtor's ordinary course of business or engaged in as part of an approved administration should be avoided (canceled), with narrow exceptions protecting parties who lacked notice.

Certain transactions prior to the application for or the date of commencement of the insolvency proceeding should be avoidable (cancellable), including fraudulent and preferential transfers made when the enterprise was insolvent or that rendered the enterprise insolvent.

The suspect period, during which payments are presumed to be preferential and may be set aside, should be reasonably short in respect to general creditors to avoid disrupting normal commercial and credit relations, but may be longer in the case of gifts or where the person receiving the transfer is closely related to the debtor or its owners.

Integrity of the System

The system must have integrity, which requires that it have certain characteristics. First, the system should guarantee security of tenure and adequate remuneration of judges, and personal security for judicial officers and court buildings. Court operations and decisions should be based on firm rules and regulations to avoid corruption and undue influence.

Second, the court must be free of conflicts of interest, bias, and lapses in judicial ethics, objectivity, and impartiality.

Third, the persons involved in a proceeding must be subject to rules and court orders designed to prevent fraud, other illegal activity, and abuse of the insolvency and creditor rights system. In addition, the court must be vested with appropriate powers to enforce its

orders and address matters of improper or illegal activity by parties or persons appearing before the court with respect to court proceedings.

Competence and Integrity of Insolvency Representatives

The system should ensure that:

- Criteria as to who may be an insolvency representative should be objective, clearly established, and publicly available.
- Insolvency representatives be competent to undertake the work to which they are appointed and to exercise the powers given to them.
- Insolvency representatives act with integrity, impartiality, and independence.
- Insolvency representatives, where acting as managers, be held to director and officer standards of accountability, and be subject to removal for incompetence, negligence, fraud, or other wrongful conduct.

Reorganization Proceedings

The system should promote quick and easy access to the reorganization proceeding, assure timely and efficient administration of the proceeding, afford sufficient protection for all those involved in the proceeding, provide a structure that encourages fair negotiation of a commercial plan, and provide for approval of the plan by an appropriate majority of creditors. Key features and principles of a modern reorganization proceeding includes the following:

- *Plan formulation and consideration.* A flexible approach for developing a plan consistent with fundamental requirements designed to promote fairness and prevent commercial abuse.
- *Plan voting and approval.* For voting purposes, classes of creditors may be provided with voting rights weighted according to the amount of a creditor's claim. Claims and voting rights of insiders should be subject to special scrutiny and treated in a manner that will ensure fairness. Plan approval should be based on clear criteria aimed at achieving fairness among similar creditors, recognition of relative priorities and majority acceptance, while offering opposing creditors or classes a dividend equal to or greater than they would likely receive in a liquidation proceeding. Where court confirmation is required, the court should normally defer to the decision of the creditors based on a majority vote. Failure to approve a plan within the stated time period, or any extended periods, is typically grounds for placing the debtor into a liquidation proceeding.
- *Plan implementation and amendment.* Effective implementation of the plan should be independently supervised. A plan should be capable of amendment (by vote of the creditors) if it is in the interests of the creditors. Where a debtor fails or is incapable of

implementing the plan, this should be grounds for terminating the plan and liquidating the insolvency estate.

- *Discharge and binding effects.* The system should provide for plan effects to be binding with respect to forgiveness, cancellation, or alteration of debts. The effect of approval of the plan by a majority vote should bind all creditors, including dissenting minorities.
- *Plan revocation and closure.* Where approval of the plan has been procured by fraud, the plan should be reconsidered or set aside. Upon consummation and completion of the plan, provision should be made to swiftly close the proceedings and enable the enterprise to carry on its business under normal conditions and governance.

Implementation: Institutional and Regulatory Frameworks

Strong institutions and regulations are crucial to an effective insolvency system. The institutional framework has three main elements:

- The institutions responsible for insolvency proceedings
- The operational system through which cases and decisions are processed
- The requirements needed to preserve the integrity of those institutions.

A number of fundamental principles influence the design and maintenance of the institutions and participants with authority over insolvency proceedings.

Transparency and Corporate Governance

Transparency and good corporate governance are the cornerstones of a strong lending system and corporate sector. Transparency exists when information is assembled and made readily available to other parties and, when combined with the good behavior of "corporate citizens," creates an informed and communicative environment conducive to greater cooperation among all parties. Transparency and corporate governance are especially important in emerging markets, which are more sensitive to volatility from external factors. Without transparency, there is a greater likelihood that loan pricing will not reflect underlying risks, leading to higher interest rates and other charges.

Another effect of implementing minimum standards of transparency and corporate governance is fostered communication and cooperation. Disclosure of basic information—including financial statements, operating statistics, and detailed cash flows—is recommended for sound risk assessment. Accounting and auditing standards should be compatible with international best practices so that creditors can assess credit risk and monitor a debtor's financial viability.

Transparency and strong corporate governance are needed in both domestic and cross-border transactions and at all phases of investment—at the inception when making a loan, when managing exposure while the loan is outstanding, and especially once a borrower's financial difficulties become apparent and the lender is seeking to exit the loan. Lenders require confidence in their investment, and confidence can be provided only through ongoing monitoring, whether before or during a restructuring or after a reorganization plan has been implemented.

From a borrower's perspective, the continuous evolution in financial markets is evidenced by changes in participants, financial instruments, and the complexity of the corporate environment. Besides traditional commercial banks, today's creditor (including foreign creditors) is as likely to be a lessor, an investment bank, a hedge fund, an institutional investor (such as an insurance company or pension fund), an investor in distressed debt, or a provider of treasury services or capital markets products. In addition, sophisticated financial instruments such as interest rate, currency, and credit derivatives have become more common. Although such instruments are intended to reduce risk, in times of market volatility they may increase a borrower's risk profile, adding intricate issues of netting and monitoring of settlement risk exposure. Complex financial structures and financing techniques may enable a borrower to leverage in the early stages of a loan. But sensitivity to external factors, such as the interest rate environment in a developing economy, may be magnified by leverage and translate into greater overall risk.

From a lender's perspective, once it is apparent that a firm is experiencing financial difficulties and approaching insolvency, a creditor's primary goal is to maximize the value of the borrower's assets to obtain the highest debt repayment. A lender's support of an exit plan, whether through reorganization and rehabilitation or liquidation, depends on the quality of the information flow. To restructure a company's statement of financial position, the lender must be in a position to prudently determine the feasibility of extending final maturity, extending the amortization schedule, deferring interest, refinancing, or converting debt to equity, while alternatively or concurrently encouraging the sale of non-core assets and closing unprofitable operations. The enterprise's indicative value should be determined to assess the practicality of its sale, divestiture, or sale of controlling equity interest. Values must be established on both a going-concern (i.e., a plan that does not require liquidation) and liquidation basis to confirm the best route to recovering the investment. And asset disposal plans, whether for liquidity replenishment or debt reduction, need to be substantiated through valuations of encumbered or unencumbered assets, taking into

account where the assets are located and the ease and cost of access. All these efforts and the maximization of value depend on and are enhanced by transparency.

Transparency increases confidence in decision making and so encourages the use of out-of-court restructuring options. Such options are preferable because they often provide higher returns to lenders than straight liquidation through the legal process—and because they avoid the costs, complexities, and uncertainties of the legal process. In many developing countries it is hard to obtain reliable data for a thorough risk assessment. Indeed, it may be too costly to obtain the quantity and quality of information required in industrial countries. Still, efforts should be made to increase transparency.

Predictability

A predictable, reliable legal framework and judicial process are needed to implement reforms, ensure fair treatment of all parties, and deter unacceptable practices. Corporate laws and regulations should guide the conduct of the borrower's shareholders. A corporation's board of directors should be responsible, accountable, and independent of management, subject to best practices on corporate governance. The law should be imposed impartially and consistently. Creditor rights and insolvency systems interact with and are affected by these additional systems, and are most effective when good practices are adopted in other relevant parts of the legal system, especially the commercial law.

Investment in emerging markets is discouraged by the lack of well-defined and predictable risk allocation rules and by the inconsistent application of written laws. Moreover, during systemic crises investors often demand uncertainty risk premiums too onerous to permit markets to clear. Some investors may avoid emerging markets entirely despite expected returns that far outweigh known risks. Rational lenders will demand risk premiums to compensate for systemic uncertainty in making, managing and collecting investments in emerging markets.

The likelihood that creditors will have to rely on risk allocation rules increases as fundamental factors supporting investment deteriorate. That is because risk allocation rules set minimum standards that have considerable application in limiting downside uncertainty, but that usually do not enhance returns in non-distressed markets (particularly for fixed-income investors). During actual or perceived systemic crises, lenders tend to concentrate on reducing risk, and risk premiums soar. At these times the inability to predict downside risk

can cripple markets. The effect can impinge on other risks in the country, causing lender reluctance even toward untroubled borrowers.

Lenders in emerging markets demand compensation for a number of procedural uncertainties. First, information on local rules and enforcement is often asymmetrically known. There is a widespread perception among lenders that indigenous stakeholders can manipulate procedures to their advantage, and often benefit from fraud and favoritism. Second, the absence or perceived ineffectiveness of corporate governance raises concerns about the diversion of capital, the undermining of security interests, or waste. Third, the extent to which non-insolvency laws recognize contractual rights can be unpredictable, leaving foreign creditors in the sorry state of not having bought what they thought they bought. Fourth, the enforcement of creditor rights may be disproportionately demanding of time and money.

Many creditors simply are not willing (or do not have the mandate) to try to improve returns if the enforcement process has an unpredictable outcome. In the end, a procedure unfriendly to investors but consistently applied may be preferred by lenders to uncertainty, because it provides a framework for managing risk through price adjustment. Moreover, emerging markets appear to be particularly susceptible to rapid changes in the direction and magnitude of capital flows. The withdrawal of funds can overwhelm fundamental factors supporting valuation, and creditors may race to sell assets to preserve value and reduce leverage. As secondary market liquidity disappears and leverage is unwound, valuation falls further in a self-reinforcing spiral.

In industrial countries there is usually a class of creditor willing to make speculative investments in distressed assets and provide a floor to valuation. In theory such creditors also exist in emerging markets. But in practice, dedicated distressed players are scarce and tend to have neither the funds nor the inclination to replace capital withdrawn by more ordinary creditors. Non-dedicated creditors often fail to redirect capital and make up the investment deficit, partly because the learning curve in emerging markets is so steep, but also because of uncertainty about risk allocation rules. The result? Markets fail because there are no buyers for the price at which sellers not forced to liquidate simply hold and hope.

If risk allocation rules were more certain, both dedicated and non-dedicated emerging market creditors would feel more comfortable injecting fresh capital in times of stress. In

addition, sellers would feel more comfortable that they were not leaving money on the table by selling.

Relative to industrial countries, developing countries typically have weaker legal, institutional, and regulatory safeguards to give lenders (domestic and foreign) confidence that investments can be monitored or creditors' rights will be enforced, particularly for debt collection. In general, a borrower's operational, financial, and investment activities are not transparent to creditors. Substantial uncertainty exists on the substance and practical application of contract law, insolvency law, and corporate governance rules. And creditors perceive that they lack sufficient information and control over the process used to enforce obligations and collect debts. The lack of transparency and certainty erodes confidence among foreign creditors and undermines their willingness to extend credit.

In the absence of sufficient and predictable laws and procedures, creditors tend to extend funds only in return for unnecessarily high risk premiums. In times of crisis they may withdraw financial support altogether. Countries would benefit substantially if creditor rights and insolvency systems were clarified and applied in a consistent and fully disclosed manner.

SECURITIES FRAUD

Introduction

Securities fraud refers to deceptive practices in the purchase or sale of securities, and the term covers a broad range of illegal activities. *Securities* are fungible, negotiable financial instruments that represent an interest or a right in something else.

Securities are not inherently valuable. Their value stems from various factors, including the issuer's financial condition, markets, and competitive and regulatory climates. Thus, securities are not a commodity to be consumed; they more closely resemble currency being traded.

Many financial products and opportunities can be classified as securities, but what actually constitutes a security is often far from obvious to an untrained observer.

Most countries have laws that prohibit false statements and other fraudulent activity in connection with securities transactions, and although such laws vary by jurisdiction, most jurisdictions typically define securities fraud violations to include the following elements:

- The defendant made a material misstatement (false statement) or omission.
- The misstatement or omission was in connection with the purchase or sale of a security.
- The defendant acted with a specific intent to defraud.
- The victim relied on the misrepresentation or omission.
- The victim suffered economic loss caused by the misrepresentation or omission.

This section helps provide fraud examiners with the tools necessary to recognize a security and conduct a successful securities fraud investigation.

What Constitutes a Security?

In basic terms, a *security* is a fungible, negotiable financial instrument that represents an interest or a right in something else. This is a broad definition under which many types of instruments may be classified as securities.

The term *security*, however, is not a straightforward legal concept, and there is no standard definition. Moreover, countries define the term differently; therefore, what is considered a security varies from country to country. In addition, countries also vary in their use of the

term itself. For example, the U.S. definition of a security is substitutable with *securities* in India and South Africa, *investments* in the UK, and *financial product* in Australia.

Accordingly, determining whether something is a security can be difficult. Nevertheless, establishing whether a financial instrument is a security is often necessary, because once a financial instrument is found to be a security, it will be governed by extensive rules and regulations. (In most cases involving allegations of securities fraud, however, the exact nature of the investment does not need to be determined.)

The various definitions for the term *security* also vary in scope. A narrow construction of the term might provide that a security refers only to stocks and bonds, but there are also various other instruments that may or may not be classified as securities.

One of the most elaborate definitions of *security* is set forth in the two main pieces of federal securities law in the United States: the U.S. Securities Act of 1933 and the U.S. Exchange Act of 1934. The two laws present definitions that are functionally indistinguishable. Section 2(1) of the U.S. Securities Act of 1933 provides: "The term 'security' means any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, . . . investment contract, . . . or, in general, any interest or instrument commonly known as a 'security', . . . or any . . . guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing."

By including *investment contracts* within this definition of a *security*, U.S. lawmakers allowed this definition to include classes of financial instruments that are not specifically listed in it. Accordingly, under U.S. federal law, the default definition of a *security* is the term *investment contract,* which was defined in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). In *Howey*, the Supreme Court defined an investment contract as "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of" someone other than the investor. Thus, in *Howey*, the Supreme Court established a four-factor test, which is known as the *Howey* test, to determine whether a financial instrument is an investment contract. All four factors must be present for an investment contract to exist.

But in the United States, the *Howey* test is not definitive. Each state has its own set of securities laws, and although a majority of the states use the *Howey* test, many states use the risk capital test as an alternative to the *Howey* test. This "test" allows the investor to play a

more active role if the funds he contributes are part of the "risk capital" of the business. A person entrusts money or other capital to another with the expectation of deriving a profit. The success or failure of the venture is dependent upon the managerial efforts of the other person. Several states have formally adopted this test, sometimes known as the Hawaii Market Test, as an alternative definition of *investment contract*. However, the Supreme Court has expressly declined to decide if this test should be used.

There is, however, a certain level of uniformity in how the term *security* is defined among European countries because EU policymakers have made considerable efforts to harmonize securities law. In the United Kingdom, the Financial Services and Markets Act 2000 (FSMA), which is the primary legislation regulating securities markets in the UK, defines *investment* in terms similar to the U.S. *securities* definition. Under FSMA, an *investment* is a regulated activity that is specified in the classes of activity and categories of investment in Part II of Schedule 2 to the FSMA, which include:

- Securities
- Instruments creating or acknowledging indebtedness
- Government and public securities
- Instruments giving entitlement to investments
- Certificates representing securities
- Units in collective investment schemes
- Options
- Futures
- Contracts for differences
- Contracts of insurance
- Participation in Lloyd's syndicates
- Deposits
- Loans secured on land
- Rights in investments

The principal Australian securities laws—the Corporations Act of 2001 (Corporations Act)—contains several definitions of a *security* and *securities*, but these definitions are aggregated, defined, and regulated as *financial products* in the context of financial market and services regulation.

India's definition of *securities* is akin to the U.S. definition, and its sole definition of *securities* is contained in Section 2(h) of the Securities Contracts (Regulation) Act 1956 (SCR Act).

Section 2(h) defines *securities* as:

> *(i) shares, scrips, stocks, bonds, debentures, debenture stock or other marketable securities of a like nature in or of any incorporated company or other body corporate; (ia) derivative; (ib) units or any other instrument issued by any collective investment scheme to the investors in such schemes; (ic) security receipt as defined in clause (zg) of section 2 of the Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002; (id) units or any other such instrument issued to the investors under any mutual fund scheme; (ie) any certificate or instrument (by whatever name called), issued to an investor by any issuer being a special purpose distinct entity which possesses any debt or receivable, including mortgage debt, assigned to such entity, and acknowledging beneficial interest of such investor in such debt or receivable, including mortgage debt, as the case may be; (ii) Government securities; (iia) such other instruments as may be declared by the Central Government to be securities; (iii) rights or interest in securities.*

In the Republic of South Africa, the definition of *securities* is found in the Securities Services Act, which provides:

> *(i) shares, stocks and depository receipts in public companies and other equivalent equities, other than shares in a share block company as defined in the Share Blocks Control Act, 1980 (Act No. 59 of 1980); (ii) notes; (iii) derivative instruments; (iv) bonds; (v) debentures; (vi) participatory interests in a collective investment scheme as defined in the Collective Investment Schemes Control Act, No. 45 of 2002, and units or any other form of participation in a foreign collective investment scheme approved by the Registrar of Collective Investment Schemes in terms of section 65 of that Act; (vii) units or any other form of participation in a collective investment scheme licensed or registered in a foreign country; (viii) instruments based on an index; (ix) the securities contemplated in subparagraphs (i) to (viii) that are listed on an external exchange; and (x) an instrument similar to one or more of the securities contemplated in subparagraphs (i) to (ix) declared by the registrar by notice in the Gazette to be a security for the purposes of this Act; (xi) rights in the securities referred to in subparagraphs (i) to (x); (b) excludes- (i) money market instruments except for the purposes of Chapter IV; and (ii) any security contemplated in paragraph (a) specified by the registrar by notice in the Gazette.*

These definitions are important for numerous reasons. For one thing, investments classified as securities are subject to the rules and procedures set up by regulatory bodies like the UK's

Financial Services Authority, which impose a host of reporting and compliance obligations for securities. For another thing, whether an international transaction is classified as a security affects the jurisdictions under which it falls.

Although the definition of *securities* varies among jurisdictions, most of these definitions cover instruments that can easily be identified as securities. These more traditional securities are usually easy to spot.

Traditional Securities

Types of investments most commonly recognized as securities include: stocks, bonds, and certificates of deposit (CDs).

Stocks

A *stock* is an instrument that represents an ownership interest in a corporation and a claim on a proportional share in the corporation's assets and profits. Corporations raise capital through the sale of shares of stock, which entitle the lawful holder to dividends and other rights of ownership. There are many different classes of stock, including common, preferred, non-voting, and restricted.

Bonds

A *bond* is a debt instrument; it is a certificate of debt issued by a government or corporation guaranteeing payment, plus interest, on the original investment by a specified future date. A bond, like a loan, obligates the issuer to pay the bondholder a specified sum of money, usually at specified intervals, and to repay the amount of the loan at maturity. There are many types of bonds, including treasury bills, corporate bonds, municipal bonds, and junk bonds. Although the term *junk bonds* has a negative connotation, these instruments are simply high-risk, below-investment-grade, commercial bonds.

Certificates of Deposit

Certificates of deposit (CDs) are interest-bearing investment products that provide limited access to the money invested and a modest rate of interest. Put differently, CDs are certificates of debt that are issued by financial institutions and that guarantee payment on the original investment, plus interest, by a specified future date. In these documents, banks acknowledge the receipt of money and promise to repay the money with interest.

CDs are intended to be held until maturity, at which time the money may be withdrawn together with the accrued interest. Many banks impose penalties on money that is withdrawn from a CD before maturity.

Futures and Options

Numerous securities fraud schemes involve futures contracts, option contracts, and over-the-counter (OTC) options (i.e., an option that does not trade on a major exchange). Futures and options are the main types of derivative instruments. *Derivatives* are financial instruments whose value is based on an underlying asset or economic factor.

There are two main types of financial markets for derivatives: exchange-traded and over-the-counter (OTC). Thus, the contracts traded on these markets derive their values from an underlying asset or economic factor.

Futures and options are essentially methods of managing price risk, often called *hedging*. Futures and options can be used, for example, by farmers or international manufacturing companies as a form of insurance against adverse price or currency exchange rate changes. Many esoteric types of investment vehicles have been created, often using complex mathematical models, and these derivative products allow trading to take place in various indices known as *strips*, *collateralized mortgage obligations*, and *leaps*.

Trading derivatives is risky and, consequently, internal controls must be airtight in a firm that engages in hedging or trading activities using exchange-traded or OTC derivatives.

Futures Contracts

A *futures contract*, or *future*, is an agreement between buyers and sellers to make delivery (i.e., sell) or to take delivery of (i.e., buy) a given quantity and quality of a commodity at a specified price and on a specified future date.

Often, the underlying asset to a futures contract is commodities, and generally, futures contracts are bought and sold on commodities exchanges, which are similar to stock exchanges in that they function as a central marketplace and provide facilities to buy and sell commodities. A *commodity* is anything that can be turned to commercial advantage. Goods commonly sold on the commodities market include such items as soybeans, wheat, corn, pork bellies, rice, gold, and silver. In the commodities market, the basic instrument of exchange is the futures contract.

Futures contracts are a valuable tool that certain businesses (e.g., a rancher who is dependent on corn for feeding his cattle) rely on to reduce their exposure to price fluctuations of commodities. Prices of commodities are highly volatile, as they are affected by factors including, but not limited to, weather, industry, economy, employment, technology, and political and global events. Investors, who have no intention of taking delivery of the actual physical commodities, trade in commodity futures contracts with the goal of profiting from price fluctuations in the underlying commodity.

Futures contracts are standardized and contain terms with specifications such as the contract size, delivery months, commodity grade, location of delivery, and so on. Price and quantity are the only things negotiated by the counterparties to a trade. In the United States, agricultural, industrial, and financial futures are traded on organized exchanges known as contract markets.

Futures contracts are either physically delivered or cash settled. When futures contracts are physically delivered, the holder must either produce the underlying commodity or take delivery from the exchange. The possibility of delivery keeps futures contracts in line with their underlying cash markets. If a contract rises too high in price relative to the cash market, traders might sell futures with the intent of making delivery. This forces the futures price down and is the reason futures markets reflect the price of their underlying cash market.

Cash settlement is a method of settling futures contracts by cash rather than by physical delivery. The value of these contracts is derived from an underlying index value. When a futures contract is cash settled, traders will often use a calculated "fair value" to determine if the futures are high or low compared to the underlying index. If fair value indicates that futures are too high, a trader might sell futures, expecting the difference to narrow.

Futures contracts do not have any intrinsic value in and of themselves; their value is derived from the underlying commodity, index, or security. Because futures contracts "derive" their price from their underlying cash market, they are called derivatives.

THE PRINCIPLE OF OFFSET

One of the features of commodity futures markets that make them so liquid and cost effective is the principle of offset. In a futures contract, the delivery or sale of the product is assumed, and the investor has an obligation to fulfill the contract; therefore, buying or selling a futures contract does not necessarily mean that the investor will accept or make delivery of

the actual commodity itself. But the obligation of the buyer (to accept future delivery) and the obligation of the seller (to make future delivery) is not with each other; it is with the central clearing function of the exchange (exchanges may have a separate clearing corporation or the clearing may be a part of the exchange itself).

The primary means of fulfilling one's obligation under a future's contract is to enter into an off-setting contract. An *off-setting contract* is one in which a purchase (sale) of futures contracts is liquidated through the sale (purchase) of an equal number of futures contracts with the same delivery month, thus closing out a position. This legally cancels the outstanding obligation.

Each futures exchange has its own clearing organization that provides clearing services with respect to futures contracts. *Clearing* is the process by which a clearing organization acts as a third-party intermediary to futures contracts and assumes the role of the buyer and seller in such contracts so that it can reconcile the orders between the transacting parties.

That is, the clearing organization matches futures transactions and becomes counterparty to both sides of the trade, eliminating counterparty credit risk by guarantying both sides of the transaction. As a result, traders can liquidate their positions (obligations) by merely executing an equal and opposite offsetting transaction (selling out a long position or buying back a short one). Clearing also transfers funds between transacting parties when futures trades are marked to market at the end of each day.

TRADING ON MARGIN

Futures are traded on margin, which is the initial amount of money that is invested by both buyers and sellers of futures contracts to ensure performance on the terms of the contract (the making or taking delivery of the commodity or the cancellation of the contract by a subsequent offsetting trade). A margin in futures is not a down payment, as in securities, but rather a performance bond. A buyer puts up an initial margin at the time a futures market contact is established to act as security for a guarantee of contract fulfillment. Only a small percentage, usually about 5 percent of the contract's notional value, is required to establish a position (long or short) in a futures market (notional value is the contract size in units multiplied by the price per unit).

Margins are set by the exchange for each commodity and are raised or lowered from time to time to reflect changing market volatility and notional contract values. Brokerage firms may

require greater margin of their customers but may not require less than what the exchange has set. Each exchange will have a margin committee made up of exchange members and support personnel that monitors and evaluates the markets and makes margin changes as appropriate.

There are two types of margin: initial margin and maintenance margin. The *initial margin* is the amount of money per contract that must be present in the account when the position is initiated. That is, to buy securities on margin, an investor must deposit enough assets with a broker to meet the initial margin requirement for that purchase. The *maintenance (variation) margin* is the minimum amount of money per contract that must be maintained in the account while the position is open. That is, the maintenance margin is the amount investors must have in their account to maintain an open position. For example, a December corn contract had a closing price of $2.84 1/4 per bushel. The notional value of this contract is $14,212 (5,000 bushels x $2.84 1/4). The initial margin requirement is $810 per contract, which is 5.69 percent of the notional contract value, while maintenance margin is set at $625 per contract, which is 4.39 percent of the notional contract value. Positions can be liquidated without customer authorization in accounts that violate margin requirements.

TRADING BASICS

A trader who buys futures contracts (assuming this is not an offsetting transaction) is long in the market and will profit if prices rise (e.g., if you bought a December corn contract at $2.70 per bushel and the price rose to $2.80 per bushel, you would have an unrealized profit of $500 (.10 cents x 5,000 bushels)). Because open commodity positions (transactions that are not offset) are marked to market at the end of the trading day, this $500 profit will be credited to your trading account and is available as margin for additional contract purchases. This transfer of funds occurs through the clearing corporation of the exchange.

The transaction counterpart of the long buyer is the short seller. Using the previous example, if you sold a December corn contract at $2.70 per bushel and the price rose to $2.80 per bushel, you would have an unrealized loss of $500 (.10 cents x 5,000 bushels). Again, open commodity positions are marked to market at the end of the trading day, meaning that this $500 loss will be debited from your trading account.

Options

Options (or *option contracts*) are like futures contracts, but unlike futures, options do not impose obligations on the buyer and seller to make or take physical delivery of the commodity. An

option contract confers a right—not an obligation—to the option buyer to take delivery of (i.e., buy) the underlying asset and imposes obligations on the option seller.

Options can be traded on exchanges, over-the-counter (OTC), between individual business entities, or between individuals. Option contracts have widespread appeal and application, and they are used and abused. Businesses and individuals commonly use options in real estate, personal property, and interest rate transactions.

The main difference between option contracts and futures contracts is that options confer rights and impose obligations, whereas futures impose obligations. More specifically, an option contract confers a right—not an obligation—to the option buyer to take delivery of (i.e., buy) the underlying asset and imposes obligations on the option seller. Futures impose obligations on both the buyer and the seller to either make or take physical delivery of the commodity or to agree to cash settlement at contract expiration.

If an option is not exercised, it expires unexercised (most exchange-traded options expire worthless). In contrast, if a commodity contract is held to expiration, the investor who has the long position takes delivery of the commodity, and the investor in the short position makes delivery.

Again, the buyer of an option contract purchases the right, not the obligation, to buy or sell something at a specified price (exercise or strike price) by the expiration date of the option contract.

The object of the option contract (what the option is written on) is called the *underlying*. The value of the underlying is the main (but not only) factor from which the option contract derives its value.

Also, options are a zero-sum transaction, meaning that one investor must suffer a loss for another investor to gain.

Option trading, however, has conservative and speculative aspects. On the one hand, option contracts can be used to hedge other security positions or assets. On the other hand, option contracts enable a speculator to control large quantities of securities with a small amount of capital.

There are two kinds of options: calls and puts. A *call option* is the right, but not the obligation, to purchase the underlying security at the strike (exercise) price by the option's expiration date. A *put option* is the right, but not the obligation, to sell the underlying security at the strike (exercise) price by the option's expiration date.

In options transactions, the seller of a call option is the *call writer*, while the seller of the put option is the *put writer*. Option buyers pay a premium to option writers for the options they buy. Option writers (sellers) collect this premium for the options they write and are obligated to deliver the underlying security if the option is exercised.

Options come in various styles such as:

- *Plain vanilla option*: This is the most standard version of an option. Plain vanilla options have simple expiration dates and strike prices and no additional features.
- *Exotic option*: This option has more complex features than plain vanilla.
- *American option*: This option may be exercised on any trading day on or before expiration.
- *European option*: This option may only be exercised on expiration.

RELATIONSHIP OF THE UNDERLYING SECURITY TO AN OPTION

Options are derivatives; therefore, their value is derived primarily from the value of their underlying instruments. For example, XYZ common stock closed today at $88.29 per share and the strike prices of the October 2008 XYZ calls ranged from $65 per share to $135 per share. The more that the share price of XYZ is above a particular strike price, the greater the value of that option. The stock price of $88 per share is about $23 over the strike price of the XYZ $65 calls. The current premium for XYZ $65 calls is $22.90 per share. A trader who had previously bought this call option could sell it back into the market for about $2,290 ($22.90 x 100 shares) or could exercise the option and buy the stock at $65 with the market at $88.

Options can be *in the money*, *out of the money*, or *at the money*. A call option is in the money when the price of the underlying security exceeds its strike price. Likewise, a put option is in the money when the price of the underlying security is less than its strike price. Options are at the money when the price of the underlying security is about the same as the strike price. All other options are out of the money.

OPTION VALUES AND PREMIUMS

There are two values that make up option premiums: intrinsic value and time value. To have any intrinsic value, an option must be in the money. Out of the money options have only time value. Returning to the previous example, the XYZ $85 call closed today at a premium of $5.70 per share. This call option is $3 in the money because the underlying XYZ stock closed above the strike price at $88 per share. The premium has $3 intrinsic value, while the remaining $2.70 is time value.

While the concept of *intrinsic value*—the difference between the underlying stock's price and the strike price—is rather straightforward, the concept of time value is complex and beyond the scope of this writing. It is worth noting, however, that the mathematical formula for pricing option time value was first introduced by Fischer Black and Myron S. Scholes in 1973. The formula takes six factors into account: underlying price, strike price, time to expiration, volatility of the underlying, dividends, and interest rates.

OVER-THE-COUNTER OPTIONS

Again, options can be traded over-the-counter. A security that does not trade on a major exchange is said to trade over-the-counter (OTC). Unlike the floor trading in physical exchanges, OTC trading is conducted electronically, through direct contact with a market maker, or through communication among professional buyers and sellers. Banks, large brokerage firms, insurance companies, and many other businesses are active in the OTC options markets.

OTC options are not centrally cleared or standardized. These options are usually customized by the option writer to fit the needs of the option buyer. Because OTC options are not centrally cleared, counterparty credit risk can be a major concern and risk factor. The option is worthless if the option writer cannot perform.

OTC options can be plain vanilla or exotic. When traded OTC, exotic forms can be problematic for market participants, accountants, and auditors, but such problems are beyond the scope of this writing.

Investment Contracts

In many countries, such as in the United States, the term *security* includes investment contracts. The leading global definition of *investment contract* parallels the *Howey* test

established by the U.S. Supreme Court, and it provides that a contract, transaction, or scheme is an investment contract if all of the following four elements are met:

- *There is an investment of money or other asset.*
- *The investment is in a common enterprise.* In very general terms, the common enterprise requirement means the success of the investor is dependent on the efforts and success of those seeking the investment of third parties (typically the promoter). The third party, who provides the entrepreneurial skill, shares in the profits (or losses) with the investor.
- *The investment was made with expectations of making a profit. Profit* is generally defined as either money received for the use of capital or capital appreciation.
- *The profits are to come solely from the efforts of people other than the investor.* To qualify as a security under this definition of investment contract, the essential managerial efforts, which affect the success or failure of the enterprise, must come from someone other than the investor. As a general rule, the more actively involved an investor is in the enterprise, the less likely it is that an investment contract will be found to exist. Thus, if the investor's efforts are significant to the enterprise's success, an investment contract will not be found to exist.

Under this definition, the term *investment contract* is broad enough to cover obscure, deceitful, new, uncommon, or irregular devices. Thus, some of the less obvious types of investments that are recognized as securities fall under the catch-all category of an investment contract. Many fraudulent schemes involving exotic investments can be argued to constitute the offer or sale of investment contracts.

The following are types of investments that frequently qualify as investment contracts:

- Ponzi schemes
- Illegal pyramid schemes
- Prime-bank note schemes
- Investment schemes involving precious metals or stones
- Viaticals
- Partnerships
- Joint ventures
- Oil, gas, and mineral interests
- Hedge funds
- Promissory notes

Ponzi Schemes

Ponzi schemes refer to illegal operations that use financial instruments of some sort to extract money from victims, and these schemes constitute securities fraud. In countries like the United States, in which the term *security* includes investment contracts, Ponzi schemes fall under securities laws and regulations because they qualify as investment contracts.

A Ponzi scheme is generally defined as an illegal business practice in which new investors' money is used to make payments to earlier investors. In a Ponzi scheme, there are few or no actual investments being made, just funds passing up a ladder.

The term *Ponzi scheme* is named after Charles Ponzi who, in the early 1920s, persuaded tens of thousands of Bostonians to invest over $10 million. He created an entity, aptly named the Securities and Exchange Company, and issued investors a promissory note guaranteeing a 50 percent return in 90 days on every $1,000 invested.

Illegal Pyramid Schemes

An *illegal pyramid* is a scheme in which a buyer or participant is promised a payment for each additional buyer or participant he recruits. Typically, these schemes involve a strategy whereby the fees or dues a member pays to join the organization are paid to another member, and in many cases, these schemes contain a provision for increasing membership through a process of new members bringing in other new members.

In these schemes, the members make money not by earning a commission on the bona fide retail sale of a legitimate product, but by recruiting new people. Illegal pyramids pay participants commissions for recruiting new members, and the schemes generate revenue by recruiting new members.

Illegal pyramids have unsustainable organizational structures that, like Ponzi schemes, rely on bringing in new people. Although illegal pyramid schemes are fraudulent, not all pyramid schemes are investment contracts.

Prime-Bank Note Schemes

Prime-bank note schemes involve the issuance and purported trading of so-called prime bank notes or other high-yield investment opportunities. In these schemes, investors are often told that they can obtain returns exceeding several hundred percent per year when their funds are placed in an offshore trading program.

These programs are generally characterized by a number of factors. They are often excessively complex and secret. Investors are usually told that the investment opportunity is only available to a select few and the signing of nondisclosure agreements is mandatory. Typically, the explanation of how the program actually works is full of obscure terminology, and it makes reference to legitimate banks or organizations, such as the International Monetary Fund (IMF), to lend credibility. Often, to promote these schemes, investors are told that there is little or no risk of losing their principal.

While prime-bank note schemes were once an effective type of fraud, these schemes have died out for three key reasons. First, consumers are better informed. Second, investigative agencies have effectively prosecuted these schemes. Third, fraudsters have moved on to faster and more productive opportunities to commit fraud.

Schemes Involving Precious Stones and Metals

Often, investment schemes involve precious metals or stones. Scams involving precious stones and metals usually commence with an offer to purchase assets of a long-term nature that is made by a high-pressure salesperson over the phone or on the Internet. Consumers respond to questions that enable the salesperson to determine their financial potential to make substantial investments. These investments are often promoted as low risk with a high rate of return. Typically, these involve the purchase of interests in gold or silver coins, bullion, diamonds, and other precious or semi-precious stones.

Viaticals

Insurance companies have historically offered policies with an accelerated death benefit option. This option allows the insured to receive up to 80 percent of the death benefit or face value of the policy within the last year of the insured's projected life. The remaining 20 percent is paid upon death to the insured's estate.

In a *viatical settlement*, a terminally-ill policy holder sells the death benefit under his insurance policy at a discount to a third party. In this type of settlement, the owner of the insurance policy receives cash, and the buyer becomes the new owner, or beneficiary, of the life insurance policy. The new owner pays all future premiums on the policy and receives the entire death benefit upon the insured's death. If the new owner does not pay the insurance premiums, the insurance policy will be voided, and the end payment will not be paid out. Moreover, in a viatical settlement, the third party who purchases the policy can resell the policy—along with the insured's medical and personal history.

In and of itself, a viatical settlement does not constitute the offer or sale of a security. But an industry has evolved to buy these rights and then sell fractional interests in them to investors. Frequently, these policy rights are pooled, and the investors are sold an interest in the pool. Investor returns increase according to how deeply the policy is discounted and are inversely related to how long the beneficiary survives.

Whether viatical investments constitute securities is unclear and can vary in different jurisdictions.

Partnerships

A partnership is a business structure that is used to separate a business from its owners. According to *Barron's Dictionary of Finance*, a partnership is a "contract between two or more people in a joint business who agree to pool their funds and talent and share in the profits and losses of the enterprise."[1] Put differently, a partnership is an association of two or more persons acting as co-owners in a business for profit.

There are various partnership forms, including general partnerships and limited partnerships. *General partnerships* are associations of two or more persons acting as co-owners in a business for profit. In a general partnership, each general partner can incur obligations on behalf of the partnership, and each partner assumes unlimited liability for the partnership's debts. Thus, a general partner has unlimited personal liability. Also, in a general partnership, the partners take an active role in the operation of the business (i.e., they have management responsibilities).

Typically, however, general partnerships are not considered securities because the profits derived from such structures are generated from the efforts of the investors, not from the efforts of others. Thus, because the partners take an active role in the operations of general partnerships, these arrangements do not qualify as securities.

Be warned, however, that some promoters will try to disguise an investment contract as a general partnership. Therefore, it is important to look beyond the surface and determine if the partners really take an active role in operating the entity.

[1] *Barron's Dictionary of Finance and Investment Terms,* 2006.

The unlimited liability risk of general partnerships makes limited partnerships an attractive alternative to general partnerships. A limited partnership is similar to a general partnership, except that in addition to one or more general partners, limited partnerships also have one or more limited partners. In contrast to a general partner, who has unlimited personal liability, a limited partner is a passive investor whose liability is limited to the amount of his investment in the company. Thus, in a limited partnership, the general partners manage the enterprise's activities, and the limited partners supply the funding. Limited partners do not manage the enterprise's activities. Simply put, limited partnerships facilitate commercial investments by those who want a financial interest but do not want the responsibilities or liabilities of general partnerships.

Unlike general partnership interests, interests in limited partnerships generally constitute investment contracts.

To determine if a partnership is an investment contract, determine if the partners truly take an active role in operating the entity.

Joint Ventures

Joint ventures are associations of two or more people or entities that form an alliance to pursue a common business objective. Interests in a joint venture will often be found to be securities. As with partnership interests, to determine if a joint venture is a security, pay careful attention to the extent to which the investor actively participates in the management or operation of the business.

Oil, Gas, and Mineral Interests

Usually, the sale of fractional ownership of oil and gas wells or mineral rights constitutes the sale of a security. The misrepresentations and omissions found in oil and gas scams are often repeated in other mineral mining schemes, such as gold or coal. Investors have a right to be advised of the risks inherent in a securities investment, and oil/gas opportunities are traditionally high-risk investments. A red flag should arise if investors have been assured or guaranteed of success in striking oil, gas, or mineral deposits. Naturally, when examining investments involving oil, gas, and mineral interests, examiners should look for discrepancies in promoters' credentials, business history, and commission.

The following types of misrepresentations and omissions are often encountered in these investments:

- *Inflated drilling and completion costs*: Costs are often inflated to bilk the investor.
- *Invalid lease*: Promoters frequently do not have a valid *mineral rights lease*—a lease conveying property rights to exploit an area for the minerals it holds.
- *Misinformation on discovery and production potential*: The investor might be misled regarding the likelihood of striking oil, gas, or mineral deposit and the amount produced. This information is usually contained in the geologist's report.
- *Exaggeration about the wells*: The promoter might exaggerate the number and depth of wells, thus inflating the operating costs paid by investors.
- *Self-dealing*: Often, promoters of such interests engage in self-dealing. The promoter might, for example, declare a good well dry to reap the benefits of a productive well later when the investors have given up.
- *Dry holes*: Often, the promoter completes *dry holes*—wells drilled for oil or gas but yielding none—solely to improve his completion record and collect completion funds from investors.
- *Disproportionate royalties*: Insiders might be assigned the majority of royalties while investors receive only a small portion.
- *Unreasonable number of partners*: Promoters are likely to oversell the well (e.g., 99/64ths).

Occasionally, an oil, gas, or mineral investment might be a complete fabrication. This is even more likely in overseas mineral investments. To carry out such schemes, the perpetrators might falsify geologists' reports or the promoters might rely on investors' reluctance to travel to remote spots to see their well or mine for themselves.

EXAMPLE

The Bre-X gold scandal, which occurred in the spring of 1997, provides a good example of a scheme involving international mineral investments.

In the 1990s, Bre-X, a Canadian mining company, announced that it had found a large gold deposit in Busang, Indonesia. As rumors of the tremendous discovery circulated, share prices of the penny-stock company skyrocketed.

Optimistic investors largely ignored the red flags that began to emerge. The initial concern with the announcement was that the mine was located in Indonesia, creating potential difficulties due to poor Canadian and U.S. relations with that country.

Undeterred by the red flags, investors continued to acquire stock in the mining company. Moreover, the company's geological reports claimed that there were as many as 5.68 grams of gold per ton of ore.

The rise in stock price, however, came to an end once a number of problems began to arise. Notably, the accuracy of the sampling came into question. Typically, when performing geological samples, companies preserve part of the core samples for verification. Bre-X, however, did not preserve parts of the core samples; instead, the company allowed the core samples to be crushed.

Additionally, a fire destroyed the records of the Bre-X geologists, further casting the discovery into doubt. Accordingly, insiders began surreptitiously selling off large amounts of their shares.

Moreover, news that the Indonesian government had withheld key permits was concealed from investors.

Bre-X's exploration manager then suffered a mysterious death (he supposedly committed suicide by jumping out of a helicopter), and following his death, share prices plunged from approximately $100 to around $2. Ultimately, Bre-X's market value declined by 90 percent.

It was later revealed that the core samples had been "salted" (i.e., gold had been added to the ore samples to change the ore's value).

The most disturbing aspect of this case is the severe handicap investigators faced because of jurisdictional questions. "This could be a monumental scam that will be nearly impossible to prosecute," said a private investigator working on the case. "No one really has jurisdiction. The salting [of the gold samples] took place in Indonesia, but what laws were really broken in that country? The law against salting? There is none. The law against deceiving shareholders? That happened in Canada and the U.S. Most of the main suspects probably disappeared in the Philippines. But what law did they break in the Philippines? Are they fugitives? No. Can a prosecutor in Canada get a warrant for those guys in the Philippines for what they did in Indonesia? Very tricky."

> *In Indonesia, no extradition or law-enforcement cooperation agreements exist with Canada or the United States. Consequently, the criminal investigation was handled by the Indonesians themselves. Likewise, though Washington asked the U.S. Embassy in Jakarta to look into the fraud, the United States and Indonesia have a poor record of cooperating in criminal matters.*

Investors in ventures like the one described in the Bre-X example can easily find themselves with no legal recourse if things go wrong. Obviously, different countries have varying laws regarding investor rights. Naturally, this makes it difficult to investigate such cases.

The principals of Bre-X claimed that they did not know about the sample salting. They portrayed themselves as victims and blamed the geologists for the fraudulent samples. The geologists, however, were Philippine nationals and retreated to their homeland, further complicating the investigation. The Philippine government suspected foul play in the death of the head geologist, Michael de Guzman, and was more concerned with its inquiry into his death than with turning over their countrymen for questioning.

When examining the case from a "follow the money" standpoint, the trail seems to lead to Bre-X insiders. Insiders concealed news of permits being withheld by the Indonesian government, and they secretly sold off huge amounts of stock at great profit. According to the *Wall Street Journal,* Bre-X Chairman David Walsh, Vice Chairman and Chief Geologist John Felderhof, and two other executives sold nearly C$38 million of stock.

Hedge Funds

In general, *hedge funds* refer to private pooled investment vehicles managed by advisors who generally have a very large financial interest in the funds based on a management fee that includes a percentage of the fund's performance. Put differently, hedge funds pool investors' money and invest it in financial instruments with the goal of earning a positive return.

Hedge funds employ various speculative and aggressive strategies. For example, they often combine traditional investments with short sales, leveraging, and arbitrage strategies to maximize returns. In addition, hedge funds are often complex and lack transparency, and they are not as heavily regulated as other types of funds.

Certain factors make hedge funds vulnerable to fraud. For one thing, hedge funds have become an increasingly popular form of investment, causing some managers to become more aggressive and less meticulous in their transactions. For another thing, hedge fund managers typically charge a performance fee of 20 percent of a hedge fund's profits, on top of an asset management fee of 1 to 2 percent of assets managed. Such lofty fees can motivate hedge fund managers to take greater risks with the hope of generating greater returns.

Typical hedge fund frauds committed by hedge fund managers include:

- Theft of investor assets
- Late trading
- Insider trading
- Overvaluation of portfolios
- Entering into inappropriate timing arrangements
- Exploitation of mutual fund investors for private gain
- Entering into inappropriate arrangements with mutual fund advisors in which the mutual fund advisors waive restrictions on market timing in exchange for placement of other assets by the hedge fund advisor in funds managed by a mutual fund advisor
- Conspiring with intermediaries to identify hedge fund from mutual fund personnel

Some red flags of improper hedge fund activities include:

- The fund's manager is resistant to due diligence or is resistant to provide the information necessary to conduct due diligence.
- The fund's manager is not willing to provide information upfront, including verification of employee date of births, Social Security numbers, employment history, education, professional licensing, professional credentials, corporate affiliations, and so on.
- The fund's manager is not willing to provide a signed release to allow the investigator to perform thorough checks.
- The fund's structure is not appropriate.
- The fund does not have verifiable and reputable independent service providers (e.g., independent accountants, attorneys, fund administrators, and prime brokers).
- The fund or its key employees have criminal records and civil litigation issues.
- There are misrepresentations (e.g., misrepresentations of education, employment history, or professional credentials).
- The fund has omitted significant background information (e.g., prior employment, employment terminations, or prior fund closures).

- The fund has experienced relevant or repeated regulatory issues.
- The fund lacks independent or experienced service providers.

Promissory Notes

A *promissory note* is a contract in which one party (the maker or issuer) makes an unconditional promise in writing to pay a sum of money to the other party (the payee), under specific terms, at a stated time, or on demand of the payee. Promissory notes area a form of debt similar to loans or IOUs, and they are investments that typically involve investors loaning money to a company in exchange for a fixed return over a stated period.

Private companies issue promissory notes to raise money and finance some aspect of their business, from launching new products to repaying expensive debt. In return for the loan, companies agree to pay investors a fixed return over a stated period.

A promissory note may be a security, but determining whether a promissory note actually is a security can be difficult. Under certain circumstances, promissory notes are not held to be securities. A note is presumed to be a security unless it bears a strong resemblance to a category of instruments that are not securities. Generally, longer-term commercial paper is similar in many respects to a bond and may be held to be a security unless it relates to such transactions as consumer finance or residential mortgages. For example, in the case of a residential mortgage, the note signed is simply a promise to repay, not a method to raise capital for some business venture.

To determine if a note is a security, it is often helpful to apply the resemblance test and look at three things: motive and expectation, plan of distribution, and regulation.

MOTIVE AND EXPECTATION

First, consider the issuer and buyer's primary motives. If the issuer's primary motive is to raise money for the general use of a business enterprise, then the note may be a security. Is the buyer motivated to make a loan or an investment-type transaction? What is a reasonable investor thinking? What are his expectations?

PLAN OF DISTRIBUTION

Second, consider the plan of distribution. If there is some form of common trading, a security probably exists.

REGULATION

Third, determine if there is some other regulatory system that significantly reduces the risk of the transaction, thereby rendering it unnecessary to apply the securities laws. If the transaction is deemed appropriately regulated in ways other than through the application of the securities laws, then it is less likely that securities laws will apply.

Securities Laws and Regulations

Securities regulation refers to laws, rules, and procedures enacted by a legislative body and administered by dedicated agencies that govern the way in which companies, consumers, and financial professionals behave when trading securities.

Securities regulation serves several purposes, the primary one being to balance the legitimate needs of businesses to raise capital against the need to protect investors. Other purposes served by securities regulation include:

- Fostering an active and competitive market
- Maintaining market confidence
- Reducing financial crime
- Protecting investors
- Discouraging behavior that might harm the market

The power to prescribe and enforce securities laws and regulations is territorial, and most securities markets, which are the markets in which securities are traded, are regulated by laws and regulations enacted and promulgated on a national basis. But because securities transactions have extraterritorial effects, national securities laws and regulations have some extraterritorial reach.

In some countries, however, the securities industry is governed by laws and regulations at different levels of government. For example, in the United States, the securities industry is regulated at both the federal and state levels. And although there is some commonality between federal and state laws, there are also some differences. Consequently, in the United States, there is a complex web of securities laws from the federal and state governments. Each state has its own securities laws, and even where the state law is similar to the federal law, the law's interpretation and rules might differ in state and federal courts.

Additionally, investors in securities face many challenges, especially in the globalized market. Different countries' exchanges have varying methods of regulating transactions. Some European countries, for instance, do not have restrictions against insider trading, while others do. Also, some countries do not have regulatory agencies to protect investor interests, and others make no stringent regulatory efforts to prevent market abuse.

National Securities Regulators

To compete in in the global securities market, a country must have a national regulatory authority to regulate all securities markets and administer securities laws under its jurisdiction. Typically, such authorities supervise the exchanges and the main participants in the securities market (e.g., brokers, dealers, and investment advisors).

Below is a list of selected securities regulators:

- United States: Securities and Exchange Commission (SEC)
- Australia: Securities and Investments Commission
- Canada: Securities Administrators
- European Union: Committee of European Securities Regulators
- European Union: Internal Market and Services Directorate General
- Germany: Bundesanstalt für Finanzdienstleistungsaufsicht
- Japan: Financial Services Agency
- Mexico: Comision Nacional Bancaria y de Valores
- United Kingdom: Financial Services Authority

Exchanges

An *exchange* is a market in which securities, commodities, futures, or options are traded. Several types of exchanges exist, including securities exchanges, commodities exchanges, and futures exchanges.

Securities Exchanges

A *securities exchange* (or *stock exchange*) is a market in which stocks, bonds, and other securities are traded. Securities exchanges host markets where securities are traded. That is, a securities exchange is a market that provides services for brokers and traders to buy and sell stocks, bonds, and other securities. Securities exchanges do not buy or sell securities; they simply provide the location and services for brokers who buy and sell securities.

Securities exchanges provide many essential functions. They provide a mechanism for private enterprises to raise investment funds, supply investors with a forum to liquidate their holdings, help in the valuation of securities, and serve as indicators of economic trends.

Securities exchanges are largely self-regulatory, which means that they regulate themselves. That is, self-regulatory exchanges exercise some degree of authority to create and enforce industry regulations and standards in the markets they organize. Although exchanges have regulatory authority, they are also regulated entities to the extent that they are subject to national control and supervision.

To trade a security on a certain exchange, the security must be listed in the exchange, and securities must meet an exchange's requirements to be listed and traded there.

Some key securities exchanges include:

- New York Stock Exchange (NYSE)
- NASDAQ
- Australian Stock Exchange
- Deutsche Borse (operator of the Frankfurt Stock Exchange)
- Honk Kong Stock Exchange
- London Stock Exchange
- Swiss Exchange
- Tel-Aviv Stock Exchange
- Tokyo Stock Exchange

Commodities Exchanges

A *commodities exchange* is an institution, organization, or association that serves as a market where various commodities and derivatives products are traded.

Futures Exchanges

A *futures exchange* is an institution, organization, or association that serves as a market where futures contracts can be bought and sold. But in practice, futures are usually traded at commodity exchanges.

International Securities Regulatory Institutions

Although securities are regulated on a national level, there are also numerous international bodies involved in the regulation or governance of international securities trading. The most

important of these are the Basel Committee on Banking Supervision (Basel Committee), the International Organization of Securities Commissions (IOSCO), and the International Accounting Standards Board (IASB). Other international securities regulatory organizations include:

- The International Securities Association for Institutional Trade Communication (ISITC)
- The International Capital Market Association (ICMA)
- The World Federation of Exchanges (WFE)
- The International Councils of Securities Associations (ICSA)
- International Swaps and Derivatives Association (ISDA)
- The European Securities and Markets Authority

Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee) provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.

The Basel Committee does not possess any formal supranational supervisory authority, and its conclusions do not, and were never intended to, have legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements—statutory or otherwise—that are best suited to their own national systems. In this way, the committee encourages convergence toward common approaches and common standards without attempting detailed harmonization of member countries' supervisory techniques.

For more information on the Basel Committee, see the "Financial Institution Fraud" chapter in the Financial Transactions and Fraud Schemes section of the *Fraud Examiners Manual*.

The International Organization of Securities Commissions[2]

The International Organization of Securities Commissions (IOSCO) is an international organization comprised of securities commissioners and administrators responsible for securities regulation and the administration of securities laws in their respective countries.

[2] The material in this section is compiled from materials and resources issued by the OICV-IOSCO. For more information on this subject, please refer to their website at www.iosco.org.

IOSCO, which was created in 1983, is currently comprised of regulatory bodies from 115 countries. IOSCO is recognized as the international standard setter for securities markets, and the organization's members regulate more than ninety-five percent of the world's securities markets.

The IOSCO's main objective is to assist its members to:

- Cooperate to promote high standards of regulation in order to maintain just, efficient, and sound markets.
- Exchange information on their respective experiences in order to promote the development of domestic markets.
- Unite their efforts to establish standards and an effective surveillance of international securities transactions.
- Provide mutual assistance to promote the integrity of the markets through a rigorous application of the standards and effective enforcement against offenses.

IOSCO develops, implements, and promotes adherence to recognized standards for securities regulation, and while IOSCO's documents are not binding, IOSCO's work shapes securities regulation worldwide.

In 1998, IOSCO adopted a comprehensive set of *Objectives and Principles of Securities Regulation* (IOSCO Principles), which are recognized as the international regulatory benchmark for all securities markets. Although members pledge to implement the IOSCO Principles in their home countries, the Principles are not binding.

In 2003, IOSCO endorsed a comprehensive methodology (IOSCO Principles Assessment Methodology) that enables an objective assessment of the level of implementation of the IOSCO Principles in the jurisdictions of its members and the development of practical action plans to correct identified deficiencies.

In 2002, IOSCO adopted a multilateral memorandum of understanding (IOSCO MOU) designed to facilitate cross-border enforcement and exchange of information among the international community of securities regulators.

In 2005, the organization endorsed the IOSCO MOU as the benchmark for international cooperation among securities regulators and set out clear strategic objectives to rapidly expand the network of IOSCO MOU signatories. It approved as an unambiguous

operational priority the effective implementation—in particular within its wide membership—of the IOSCO Principles and of the IOSCO MOU, which are considered as primary instruments to facilitate cross-border cooperation, reduce global systemic risk, protect investors, and ensure fair and efficient securities markets. IOSCO also adopted a comprehensive consultation policy designed to facilitate its continuous interaction with the international financial community and in particular with the industry. As of November 2011, the IOSCO MOU has eighty signatories, with 34 additional regulatory authorities seeking the legal authority necessary to enable them to become signatories. The growth of the IOSCO MOU has made it a significant document in combating violations of securities and derivatives laws.

OVERVIEW OF THE IOSCO PRINCIPLES OF SECURITIES REGULATION

The IOSCO Principles are based on the following three objectives:

- The protection of investors
- Ensuring that markets are fair, efficient, and transparent
- The reduction of systemic risk

There are local differences in market structures; however, these objectives form a basis for an effective system of securities regulation.

Although members pledge to implement IOSCO standards in their home countries, the principles are not binding.

THE PROTECTION OF INVESTORS

Investors should be protected from misleading, manipulative, or fraudulent practices, including insider trading, front running or trading ahead of customers, and the misuse of client assets.

Full disclosure of information material to investors' decisions is the most important means for ensuring investor protection. Investors are, therefore, better able to assess the potential risks and rewards of their investments and, as a result, to protect their own interests. As key components of disclosure requirements, accounting and auditing standards should be in place and they should be of a high and internationally acceptable quality.

Only duly licensed or authorized persons should be permitted to hold themselves out to the public as providing investment services, for example, as market intermediaries or the

operators of exchanges. Initial and ongoing capital requirements imposed upon those license holders and authorized persons should be designed to achieve an environment in which a securities firm can meet the current demands of its counter parties and, if necessary, wind down its business without loss to its customers.

Supervision of market intermediaries should achieve investor protection by setting minimum standards for market participants. Investors should be treated in a just and equitable manner by market intermediaries according to standards, which should be set out in rules of business conduct. There should be a comprehensive system of inspection, surveillance, and compliance programs.

Investors in the securities markets are particularly vulnerable to misconduct by intermediaries and others, but the capacity of individual investors to take action may be limited. Further, the complex character of securities transactions and of fraudulent schemes requires strong enforcement of securities laws. Where a breach of law does occur, investors should be protected through the strong enforcement of the law.

Investors should have access to a neutral mechanism (such as courts or other mechanisms of dispute resolution) or means of redress and compensation for improper behavior.

Effective supervision and enforcement depend upon close cooperation between regulators at the domestic and international levels.

ENSURING THAT MARKETS ARE FAIR, EFFICIENT, AND TRANSPARENT

The regulator's approval of exchange and trading system operators and of trading rules helps to ensure fair markets.

The fairness of the markets is closely linked to investor protection and, in particular, to the prevention of improper trading practices. Market structures should not favor some market users over others. Regulation should detect, deter, and penalize market manipulation and other unfair trading practices.

Regulation should aim to ensure that investors are given fair access to market facilities and market or price information. Regulation should also promote market practices that ensure fair treatment of orders and a price formation process that is reliable.

In an efficient market, the dissemination of relevant information is timely and widespread and is reflected in the price formation process. Regulation should promote market efficiency. *Transparency* may be defined as the degree to which information about trading (both for pre-trade and post-trade information) is made publicly available on a real-time basis. Pre-trade information concerns the posting of firm bids and offers as a means to enable investors to know, with some degree of certainty, whether and at what prices they can deal. Post-trade information is related to the prices and the volume of all individual transactions actually concluded. Regulation should ensure the highest levels of transparency.

THE REDUCTION OF SYSTEMIC RISK

Although regulators cannot be expected to prevent the financial failure of market intermediaries, regulation should aim to reduce the risk of failure (including through capital and internal control requirements). Where financial failure nonetheless does occur, regulation should seek to reduce the impact of that failure, and, in particular, attempt to isolate the risk to the failing institution.

Market intermediaries should, therefore, be subject to adequate and ongoing capital and other prudential requirements. If necessary, an intermediary should be able to wind down its business without loss to its customers and counterparties or systemic damage.

Risk taking is essential to an active market, and regulation should not unnecessarily stifle legitimate risk taking. Instead, regulators should promote and allow for the effective management of risk and ensure that capital and other prudential requirements are sufficient to address appropriate risk taking, allow the absorption of some losses, and check excessive risk taking. An efficient and accurate clearing and settlement process that is properly supervised and uses effective risk management tools is essential.

There must be effective and legally secure arrangements for default handling. This is a matter that extends beyond securities law to the insolvency provisions of a jurisdiction. Instability may result from events in another jurisdiction or occur across several jurisdictions, so regulators' responses to market disruptions should seek to facilitate stability domestically and globally through cooperation and information sharing.

THE REVISED PRINCIPLES FOR SECURITIES REGULATIONS

In response to the global financial crisis that began in 2008, IOSCO published a revised version of the principles in 2010. The purpose of the revision was to incorporate the lessons

learned from the crisis and prevent future occurrences. Eight principles were added, bringing the total to 38. The latest principles address hedge funds, credit rating agencies, information service providers, and auditor independence.

The IOSCO Principles need to be practically implemented under the relevant legal framework to achieve the objectives of regulation described above. The principles are grouped into nine categories.

A. Principles Relating to the Regulator

1. The responsibilities of the Regulator should be clear and objectively stated.
2. The Regulator should be operationally independent and accountable in the exercise of its functions and powers.
3. The Regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers.
4. The Regulator should adopt clear and consistent regulatory processes.
5. The staff of the Regulator should observe the highest professional standards, including appropriate standards of confidentiality.
6. The Regulator should have or contribute to a process to monitor, mitigate and manage systemic risk, appropriate to its mandate.
7. The Regulator should have or contribute to a process to review the perimeter of regulation regularly.
8. The Regulator should seek to ensure that conflicts of interest and misalignment of incentives are avoided, eliminated, disclosed or otherwise managed.

B. Principles for Self-Regulation

9. Where the regulatory system makes use of Self-Regulatory Organizations (SROs) that exercise some direct oversight responsibility for their respective areas of competence, such SROs should be subject to the oversight of the Regulator and should observe standards of fairness and confidentiality when exercising powers and delegated responsibilities.

C. Principles for the Enforcement of Securities Regulation

10. The regulator should have comprehensive inspection, investigation, and surveillance powers.
11. The regulator should have comprehensive enforcement powers.

12. The regulatory system should ensure an effective and credible use of inspection, investigation, surveillance, and enforcement powers and implementation of an effective compliance program.

D. Principles for Cooperation in Regulation

13. The regulator should have authority to share both public and nonpublic information with domestic and foreign counterparts.
14. Regulators should establish information sharing mechanisms that set out when and how they will share both public and nonpublic information with their domestic and foreign counterparts.
15. The regulatory system should allow for assistance to be provided to foreign regulators who need to make inquiries in the discharge of their functions and exercise of their powers.

E. Principles for Issuers

16. There should be full, timely, and accurate disclosure of financial results and other information that is material to investors' decisions.
17. Holders of securities in a company should be treated in a fair and equitable manner.
18. Accounting and auditing standards should be of a high and internationally acceptable quality.

F. Principles for Auditors, Credit Ratings Agencies, and Other Information Service Providers

19. Auditors should be subject to adequate levels of oversight.
20. Auditors should be independent of the issuing entity that they audit.
21. Audit standards should be of a high and internationally acceptable quality.
22. Credit rating agencies should be subject to adequate levels of oversight. The regulatory system should ensure that credit rating agencies whose ratings are used for regulatory purposes are subject to registration and ongoing supervision.
23. Other entities that offer investors analytical or evaluative services should be subject to oversight and regulation appropriate to the impact their activities have on the market or the degree to which the regulatory system relies on them.

G. Principles for Collective Investment Schemes

24. The regulatory system should set standards for the eligibility, governance, organization, and operational conduct of those who wish to market or operate a collective investment scheme.
25. The regulatory system should provide for rules governing the legal form and structure of collective investment schemes and the segregation and protection of client assets.
26. Regulation should require disclosure, as set forth under the principles for issuers, which is necessary to evaluate the suitability of a collective investment scheme for a particular investor and the value of the investor's interest in the scheme.
27. Regulation should ensure that there is a proper and disclosed basis for asset valuation and the pricing and the redemption of units in a collective investment scheme.
28. Regulation should ensure that hedge funds and/or hedge funds managers/advisers are subject to appropriate oversight.

H. Principles for Market Intermediaries

29. Regulation should provide for minimum entry standards for market intermediaries.
30. There should be initial and ongoing capital and other prudential requirements for market intermediaries that reflect the risks that the intermediaries undertake.
31. Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, with the aim of protecting the interests of clients and their assets and ensuring proper management of risk, through which management of the intermediary accepts primary responsibility for these matters.
32. There should be procedures for dealing with the failure of a market intermediary in order to minimize damage and loss to investors and to contain systemic risk.

I. Principles for the Secondary Market

33. The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.
34. There should be ongoing regulatory supervision of exchanges and trading systems which should aim to ensure that the integrity of trading is maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.
35. Regulation should promote transparency of trading.
36. Regulation should be designed to detect and deter manipulation and other unfair trading practices.

37. Regulation should aim to ensure the proper management of large exposures, default risk and market disruption.
38. Securities settlement systems and central counterparties should be subject to regulatory and supervisory requirements that are designed to ensure that they are fair, effective and efficient and that they reduce systemic risk.

THE IOSCO FRAUD REPORT

In the late 1990s and early 2000s, the world witnessed a number of high profile financial scandals involving large publicly traded companies. These scandals raised questions about the integrity of global capital markets, and the IOSCO Technical Committee decided to investigate the issues uncovered by these financial scandals and identify any broad trends. It also decided to make recommendations about whether securities regulators needed to undertake any specific actions to ensure that the regulatory framework remains robust and to help guarantee that the international financial system serves to protect the integrity of global capital markets, delivers investor confidence, and combats financial fraud.

Against this background, the Technical Committee published the report *Strengthening Capital Markets Against Financial Fraud* (the Fraud Report). This report identifies seven separate areas that have figured prominently in many high-profile financial scandals:

1. *Corporate governance*, including the role of independent directors on an issuer's corporate board, the protection of minority shareholders, the importance of independent auditor oversight committees, and mechanisms to protect against conflicts of interest presented by related-party transactions
2. *Auditors and audit standards*, including auditor independence, the effectiveness of audit standards and auditor oversight, and issues related to mandatory auditor rotation
3. *Issuer disclosure requirements*, including management's discussion and analysis of material events and factors likely to have an impact on the issuer
4. *Bond market regulation and transparency*, including the types of financial disclosures required of bond issuers and the transparency of bond market price-setting mechanisms
5. *The role and obligations of market intermediaries*, whether they contributed to recent financial scandals, and how these entities can mitigate reputational, legal, and operational risk through adequate controls and procedures, and ensure that material nonpublic information they acquire about an issuer is not misused
6. *The use of complex corporate structures and special purpose entities*, and the circumstances where they may pose particular regulatory issues

7. *The role of private-sector information analysts*, and the ways in which such individuals and entities can protect their analytical integrity and independence

For each of these seven areas the Fraud Report discussed what issues the recent financial scandals raised, and it included an action plan designed to tackle the biggest issues with high priority.

Much progress has been made in the implementation of the IOSCO MOU, and efforts in this field will continue. While much of the work that IOSCO has done can be derived from the seven issues identified in the Fraud Report, and while all this work has had important value, IOSCO drafted separate reports for the following initiatives: corporate governance, transparency and regulation of corporate bond markets, conflicts of interest in initial public offerings (IPOs), and special purpose entities. These reports are briefly discussed below.

CORPORATE GOVERNANCE

In the Fraud Report, IOSCO identified board independence, related-party transactions, and the protection of minority shareholders as crucial elements of corporate governance. These issues have already been addressed by international principles such as those of the Organisation for Economic Cooperation and Development (OECD). However, as these are high-level principles designed to accommodate different legal and regulatory frameworks, IOSCO decided to carry out additional work on how to implement the OECD principles in practice. More specifically, IOSCO set out to undertake, in collaboration with the OECD, additional descriptive and thematic analyses of the definition and role of independent directors on the boards of issuers and the additional protections required in situations where issuers are controlled by a dominant shareholder.

An IOSCO task force carried out an extensive survey to explore these elements, resulting in a consultation document that was published in December 2006. The final report was subsequently published in February 2007. This report, titled *Board Independence of Listed Companies*, contains an overview of the legal and regulatory systems of technical committee jurisdictions regarding specific issues related to board independence and is a comprehensive analysis of current regulations worldwide. The report presents a unique and illustrating overview of existing rules and regulations on board independence in the jurisdiction of a large number of IOSCO members.

CONFLICTS OF INTEREST IN INITIAL PUBLIC OFFERINGS

Another element of the fraud report was the role of intermediaries in initial public offerings (IPOs) with conflicting interests. In 2006, IOSCO began examining this issue. This analysis was performed with the knowledge that the financial scandals involved accusations that underwriters and investment banks were performing substantial roles despite the existence of conflicts of interest. Because no international standards existed on this matter, IOSCO reviewed the role played by intermediaries in the financial standards. IOSCO focused specifically on conflicts of interest within intermediaries when they are involved in an IPO.

After informal discussions with market participants, the technical committee published a discussion paper titled *Market Intermediary Management of Conflicts That Arise in Securities Offerings*. IOSCO intended that the paper would facilitate a dialogue between the financial services industry and regulations on a cross-border basis regarding possible principles that may be used by market intermediaries to guide their management of some of the conflicts that arise from activities related to a securities offering. In November 2007, IOSCO published the final version of the report.

SPECIAL PURPOSE ENTITIES

Special purpose entities (SPEs) are separate legal entities that are corporate in structure and are established (or chartered by) the national, state, or a sub-unit form of government. Because multiple parties often interact with SPEs, it can be difficult to determine, for accounting purposes, which party should consolidate the SPE's assets and liabilities on its statement of financial position. Although SPEs are used for legitimate purposes, SPEs and complex corporate structures were used to perpetrate some major financial frauds. In certain instances, some sponsoring entities provided an incomplete picture of their financial position by not disclosing the transfer of their assets and liabilities to their unconsolidated SPEs.

Since the publication of the fraud report, several IOSCO members have implemented regulatory and legislative changes that are expected to address the concerns raised by the recent financial frauds. Specifically, some IOSCO members have adopted additional nonfinancial statement disclosure requirements to solicit information about unconsolidated SPEs, while others have looked to changes in the relevant accounting standards that were intended to make it more likely that SPEs would be consolidated. The results of the survey and limited review of filings indicate that IOSCO members have only recently taken different approaches in this area and have not yet had an opportunity to evaluate the effectiveness of their initiatives. As a result, the technical committee has concluded that it

would be premature at this time to determine a global approach for addressing the reporting of information to investors regarding unconsolidated SPEs. However, IOSCO will continue to monitor developments with respect to off-statement of financial position financings, including unconsolidated SPEs, and may consider at a later date whether guidance from IOSCO on unconsolidated SPEs would be useful.

International Accounting Standards Board

The International Accounting Standards Board (IASB) is an independent body that sets accounting standard. The IASB has developed a single set of global accounting standards that have been adopted by the European Union and will likely be adopted in the future by other countries, including the United States.

International Securities Association for Institutional Trade Communication

The International Securities Association for Institutional Trade Communication (ISITC) is an industry association that collaborates to develop and promote standards and market practices designed to enhance efficiency, lower risk, and build shareholder value.

International Capital Market Association

The International Capital Market Association (ICMA) is a self-regulatory organization for participants in the capital markets, but it has a European focus. The ICMA aims to promote high standards of market practice, appropriate regulation, trade support, education, and communication.

World Federation of Exchanges

The World Federation of Exchanges (WFE), formerly the Federation Internationale des Bourses de Valeurs (FIBV), is the trade association of regulated stock, futures, and options exchanges around the world. The WFE develops and promotes standards in markets, supporting reform in the regulation of OTC derivatives markets, international cooperation, and coordination among regulators.

International Council of Securities Associations

The International Council of Securities Associations (ICSA), which is an association of a wide range of financial market self-regulatory and trade associations, aims to:

- Aid and encourage the sound growth of the international capital market by promoting and encouraging harmonization and, where appropriate, mutual recognition in the procedures and regulation of that market.
- Promote mutual understanding and the exchange of information among ICSA members.

ICSA's membership includes self-regulatory organization from Canada, Japan, the UK, and the United States and securities dealers associations from Canada, Japan, and the United States.

International Swaps and Derivatives Association

The International Swaps and Derivatives Association (ISDA) is a trade organization of participants in the market for over-the-counter derivatives. The ISDA has pioneered efforts to identify and reduce the sources of risk in the derivatives and risk management business.

European Securities and Markets Authority

There has been a push in the European Union (EU) to protect investors and provide confidence for investments by promoting common goals for securities regulators.

The European Securities and Markets Authority (ESMA) is a securities supervisory organization set up by the EU, and it is another product of efforts to remedy the financial oversight shortcomings that led to the economic crisis in 2008. The organization was created as an EU Authority on January 1, 2011.

THE ROLE OF ESMA

ESMA's role is to provide stability to the EU nations' financial system by ensuring integrity, transparency, efficiency, investor protection, and orderly functioning of the securities markets. ESMA works toward the goal of a single set of regulations that apply to all EU members, so that buying and selling securities is a more stable and uniform process.

The powers of ESMA include:

- Drafting technical standards that are legally binding on EU members
- Resolving disputes between national securities authorities
- Prohibiting financial products that threaten financial stability for up to three months
- Performing on-site inspections
- Monitoring systems risk of cross-border financial institutions

- Supervising credit rating agencies
- Entering into administrative agreements with supervisory authorities

MARKETS IN FINANCIAL INSTRUMENTS DIRECTIVE

The EU implemented the Markets in Financial Instruments Directive (MiFID) in 2007, which was intended to help integrate Europe's national security markets. In Europe, the legal relationships between the parties in securities transactions has historically been a matter of private law—handled under the same principles that would remedy a contract dispute or tort. MiFID played a part in transitioning securities laws in Europe from the private to public realm, meaning increased regulations and government oversight.

MiFID introduced new reporting requirements for equity markets to bolster pre- and post-trade transparency. Additionally, MiFID did away with previous requirements that stocks be traded only through local markets, and it promoted electronic securities trading. Another significant regulation under MiFID requires financial institutions that carry out transaction on their client's behalf must be able to prove that they provided the "best execution" of the transaction; the institutions must take into account the price, costs, speed, likelihood of execution and settlement, size, nature, or any other consideration relevant to the order. Following the global financial crisis, ESMA reviewed MiFID and consulted with the European Commission in revising MiFID, and in October 2011, the European Commission published proposals for a revised MiFID. The revised proposals, commonly referred to as MiFID II, are intended to correct some of the problems of the original MiFID, as well as respond to lessons learned during the 2008 financial crisis. The revised proposals were entered into force on July 2, 2014, and must be applied by January 3, 2017.

Securities Fraud Schemes

In general, securities fraud schemes can be classified into two categories: schemes by registered persons and entities and schemes by unregistered persons.

Securities Fraud by Registered Persons and Entities

This discussion examines types of securities fraud and misconduct committed by registered individuals or firms.

Professional Misconduct

As it relates to the financial service provider, *professional misconduct* refers to acts that go against the profession. By serving as a trusted agent and representative, the financial service provider must, at all times, place the client's wellbeing ahead of any self-serving interests.

Financial service providers are subject to certain standards of conduct, and most aspects of such standards are defined by statute and industry practice. But different jurisdictions apply different standards of conduct, and the standards might also vary depending on the type of financial services being offered by the provider. For example, brokers and investment advisors are generally subject to regulations requiring that they recommend suitable investments. Likewise, registered investment advisors are generally required to act in the best interest of their clients and are prohibited from seeking to advance personal interests to the detriment of their clients.

And although not all aspects of professional standards are defined by statute and industry practice, financial service providers are held to a high standard of care. Key elements of their duties include requirements that they must:

- Comply with industry rules and applicable regulations.
- Be well-informed consultants through continuing education.
- Use reasonable efforts to determine the needs and objectives of their customers.
- Only recommend investments consistent with customers' objectives and risk tolerance.
- Maintain fairness in transaction costs.
- Provide full disclosure to the relevant aspects of any recommendation.
- Refrain from taking advantage of the clients or firm.
- Be a respected member of the community.

There are several reliable and long-established rules of thumb that can be used to determine if an advisor has violated his professional standard of conduct. Some examples are:

- For most accounts, a financial advisor's annual commissions and fees in relation to the assets should be between one and three percent.
- Portfolio turnover (or the value of the assets bought and sold) in excess of 300 percent justifies close examination.
- Advisors should maintain due-diligence files, records related to client recommendations, and portfolio analyses.

- Regardless of complexity, advisors should be able to articulate the primary features of any recommendation and should have evidence that they have communicated that to their clients.
- Firm-sponsored technology, such as client-contact programs, should be regularly used.
- Advisors should demonstrate an effort to revise client profiles to match any lifestyle changes.

Churning (Excessive Trading)

Churning is the excessive trading of a customer account to generate commissions while disregarding the customer's interests. Specifically, churning occurs when an investment professional excessively trades an account for the purpose of increasing his commissions instead of furthering the customer's investment goals.

For securities and options, commissions are charged when the trade is entered and liquidated. Futures have a round-turn commission scheme, meaning that the commission covers both the purchase and sale. Commissions on futures are not charged until the trade is closed out.

To prove that a registered person or entity has engaged in a churning scheme, a complainant must prove the following three elements:

- Trading in the account is excessive in light of the investor's objectives.
- The broker exercised control over trading in the account.
- The broker acted with intent to defraud or willful disregard for the investor's interests[3]

There are two common methods to assess the excessiveness of trading in an account: turnover ratios and cost-to-equity ratios. *Turnover ratios* measure how often, on average, the securities in an account are traded in a year. *Cost-to-equity ratios* measure the annual cost of the trading as a percentage of the client's investments. That is, cost-to-equity ratios measure the percentage of the average equity in the client's account that is consumed by trading costs.

Often, two questions arise in churning cases:

- Who had trading authorization over the account?
- When did the account activity and commissions become excessive?

[3] *Hotmar v. Lowell H. Listrom & Co.*, 808 F.2d 1385 (10th Cir. 1987).

If customers are making their own trades, they cannot possibly accuse the broker of churning their accounts. But if brokers or some other people have trading authority (discretion) over the accounts and participate in the commissions, a conflict of interest exists and there might be a legitimate churning claim.

Many of the regulatory definitions of churning are inherently vague and offer little practical guidance. Customer trading objectives are simple: make profits and avoid losses. A good test for detecting churning is to calculate the amount of monthly gross commissions generated from the account as a percentage of the average account balance. For example, an active trading account with an average daily balance of $10,000 might reasonably generate (on the high side) about $500 dollars (5 percent) in gross commissions in an average month. Gross commissions would probably increase in months when the markets are experiencing greater price volatility and trading has been successful.

When investigating a suspected churning scheme, the fraud examiner should ask the following questions:

- Did the broker have trading authority (discretion) over the account?
- Have gross commissions increased during periods of decreasing market volatility?
- Are the gross commissions for the month in question substantially higher than the average monthly gross commissions for this account?
- Are gross commissions greater than 5 percent of the average account balance?
- Did commissions consume realized profits and/or aggravate losses?
- Were numerous trades entered into and exited over short time periods for small gains or losses?
- Was the trading unit (number of contracts per trade) too large for this account (overtrading)?
- Were the trades made for this account recommended by the research department of the brokerage and disseminated to other customers?
- Did unauthorized trading take place?

If the broker had discretionary authority to trade the account and any of these factors are true, further investigation for churning is warranted.

Finally, brokerage supervisors are required to perform due diligence to ensure that churning and other trading abuses do not occur.

Unsuitable Recommendations

In many countries, securities laws and regulations impose a suitability requirement on broker-dealers, which are persons or firms in the business of trading securities. Broker-dealers subject to a suitability requirement are prohibited from recommending investments or investment strategies that are unsuitable for their clients. Thus, making unsuitable recommendations (e.g., recommending high-risk options to a senior citizen with limited assets) is prohibited in countries with such suitability requirements. But typically, a suitability requirement only arises when broker-dealers make recommendations or provide advice to clients to purchase a product.

Suitability is a well-established regulatory concept for the financial services industry in many countries. The International Organization of Securities Commissions (IOSCO), which is an international organization comprised of securities commissioners and administrators responsible for securities regulation and the administration of securities laws in their respective countries, has addressed the issue of suitability in a report titled *Suitability Requirements with Respect to the Distribution of Complex Financial Products*. The report focuses on protecting consumers, and it sets out nine principles, including suitability obligations, to be used by securities regulators in addressing the risks relating to the distribution of financial products whose terms and features are unlikely to be understood by average retail customers.

In the United States, the concept of suitability is a part of specific rules established by securities self-regulatory organizations (SROs), such as the Financial Industry Regulatory Authority (FINRA), and it is an obligation under the anti-fraud provisions of the federal securities laws. For example, FINRA Rule 2111 prohibits a broker-dealer from making a recommendation to a client if the broker does not have reasonable grounds for believing that the recommendation is suitable for the client.

The Markets in Financial Instruments Directive II (MiFID II), which governs financial markets in the European Union (EU), also contains suitability requirements.

Essentially, there are two rules relating to suitability: the know-your-customer rule and the suitability rule.

The *know-your-customer rule* provides that securities broker-dealers must know their customer financially to effectively service the customer's account and minimize the risk of recommending an inappropriate investment. To comply with the know-your-customer rule,

broker-dealers must use due diligence to ascertain relevant personal and financial information about clients and potential clients in regard to opening and maintaining accounts. Thus, this form of suitability violation occurs when a broker recommends an investment or an investment strategy to a client without having conducted due diligence to ascertain relevant personal and financial information about the client.

In addition to the know-your-customer requirement, there are suitability requirements that broker-dealers must follow when making recommendations to a client. Suitability rules prohibit broker-dealers from making recommendations to clients if they do not have reasonable grounds for believing that the recommendations are suitable for the respective clients. That is, a suitability rule requires a broker-dealer to make a customer-specific determination of suitability and to tailor his recommendations to the customer's financial profile and investment objectives.

This form of suitability violation occurs when a broker recommends an investment, recommends an investment strategy, or makes an investment that is inconsistent with the client's objectives, and the broker knows or should know the investment is inappropriate.

The suitability of an investment should be based on a client's investment profile, which should include, but is not limited to, the following factors:

- Age
- Employment status
- Investment objectives (i.e., short-term and long-term financial goals)
- Prior investment experience
- Other investments
- Financial situation and needs
- Investment time horizon
- Tax status
- Net worth
- Liquidity needs
- Expenses
- Level of risk tolerance

Selling Away

Selling away is a securities fraud scheme that occurs when an investment professional (e.g., a registered representative, stock broker, or financial advisor) trades, or solicits the trade of, securities not held or offered by the brokerage firm with which he is affiliated.

Selling away violates rules that prohibit investment professionals from engaging in any private securities transactions that fall outside the scope of their employment, unless they have obtained written consent from their employer.

Selling away is a popular scheme committed by financial advisors. Often, selling away schemes target the elderly or those who are financially inexperienced. And while selling away can be associated with traditional securities, it generally involves unregistered securities (e.g., partnerships, promissory notes, and programs).

Uncovering this type of fraud is difficult, but it is not impossible. Generally, examiners should start a selling-away investigation by asking investment professionals if they are aware of any colleagues who are engaged in such practices. In his *Securities Arbitration Procedure Manual*, David Robbins suggests making the following inquiries in a selling away case:

- Did the broker use the firm's marketing materials to market the investment?
- Were meetings for the investment at issue held at the firm's offices?
- Did the victim investors and the firm's management have contact about the investment?
- Were the funds for the investment made payable to the brokerage firm?
- Would it be reasonable to surmise that the investors should have known that the firm did not authorize the investment?[4]

Failure to Supervise

Broker-dealer firms must establish and maintain a system to supervise the activities of their registered representatives to ensure compliance with securities laws and regulations.

Parking

Parking is the practice of selling a security to one party with the understanding that the seller will repurchase the security later at an agreed-upon price. This scheme allows circumvention of ownership reporting requirements and net capital rules.

---

[4] Robbins, David. *Securities Arbitration Procedure Manual.* 3rd ed. Charlottesville: Lexis Law Publishing, 1990.

Operating Without a License or Registration

True brokerages are required to register and meet certain financial thresholds, and broker-dealers must register with the appropriate regulatory authority. Thus, operating a security business without a license or acting as broker-dealer without proper registration violates the law. Also, the personnel at true brokerages must be registered, and often, the salespeople at such firms must pass certain tests. There might also be other licensing or registration requirements depending on the type of business in which the brokerage engages.

To determine whether an individual or firm is licensed or registered, and, therefore, legitimate, check with the relevant regulatory authority (e.g., FINRA, SEC, FCA). Often, such checks can be performed by visiting the relevant authority's website.

Fraud examiners can also use the sites of financial regulatory authorities to research firms and individuals that operate in the securities industry. Often, fraud examiners can use such sites to check an entity's license status and search for complaints brought against them. If, however, a financial services firm or professional does not show up in the relevant authority's records, it is not legitimate.

The following red flags might indicate that an entity is operating a security business without the proper license or registration:

- Agents with criminal records
- Unexplained gaps in a promoter's work history
- Prior customer complaints
- A history of regulatory problems
- Questionable credentials
- Website lacks background information or contains generic contact information

Excessive Markups

Excessive markups involve selling securities at a marked-up price or buying securities at a marked-down price not reasonably related to the prevailing market price.

Misuse or Misappropriation of Customer's Securities

Financial advisors must observe high standards of commercial practice and equitable principles of trade. This means that advisors are prohibited from unauthorized use or borrowing of customers' funds or securities, and various other deceptions. Thus, this type

of scheme might involve outright theft of securities or using securities in improper ways—for example, as collateral for loans or to conduct other securities transactions (e.g., margin trading).

Unauthorized Trading

A broker cannot trade on a customer account without authorizations from the customer, and unauthorized trading occurs when a dishonest broker sells, buys, or exchanges securities for a customer without the customer's permission or authorization. Dishonest brokers might commit unauthorized trading due to the pressures of meeting certain capital requirements, generating commission income, or meeting internal performance targets.

Any losses accruing to the customer account because of an unauthorized trade, whether made by mistake or intentionally, are the responsibility of the brokerage firm and must be reimbursed to the customer.

Likewise, gains from unauthorized trades also belong to the customer. This rule prevents brokers from executing unauthorized trades, claiming error, and taking any profits that might occur. And because of these rules, the only entries to the brokerage company error account, which is used to record its trading mistakes pending their rectification, should be losses; therefore, profits in an error account should be investigated.

Customers must report unauthorized trades the brokerage firm's management as soon as they are detected. Silence would imply ratification of the transaction.

Red flags of unauthorized trading include:

- A high incidence of failures to pay for trades
- Excessive trade cancellations
- Excessive corrections and credit extensions
- Numerous customer complaints against a broker
- A pattern of stock being sold to customers from a broker's inventory and then purchased back into the inventory by the broker close to settlement at a loss

Systematically Trading Accounts Against Each Other

Systematically trading accounts against each other is illegal, and it usually occurs between investment pools, which are funds from numerous investors that are combined for the purposes of investment (e.g., mutual funds, investment trusts, unit trusts, and other

collective investment units). The scheme occurs when someone with trading authority simultaneously establishes opposite market positions in two separate investment pools that he controls. A person who has trading authority and other controls over the pool might receive a monthly management fee of about 1.5 percent of the pool balance, a percentage of any of the pool's gains—perhaps 10 percent per quarter—and a portion or all of the commissions on trades. But in such a business arrangement, the pool operator has a conflict of interest. It is in the pool operator's interest to maintain account balances that are as high as possible, trade the accounts for commissions, and have at least some profits.

To further illustrate this scheme, consider a hypothetical example in which a pool operator establishes two limited partnerships for trading commodities. The pool operator is a general partner in both partnerships, which means that he takes an active role in each business's operations. Also, the pool operator will be compensated with a monthly management fee of 1.5 percent of the pool's balance, 10 percent of the pool's gains per quarter, and commissions on trades. The pool operator buys 100 contracts of December Corn for Pool A, establishing a long market position, and at the same time, sells 100 contracts of December Corn for Pool B, establishing a short market position. (If these transactions occurred in the same account, they would offset each other.)

Over time, one of the pools will suffer a loss while the other will enjoy a gain, but even when this occurs, things will not have changed much for the pool operator. The amount of equity in the two pools combined will be about the same with the loss in one pool being offset by the gain in the other pool. This preserves the basis for the general partner's management fee while the profitable pool will owe him a percentage of the gain.

In the end, one of the investment pools will dissolve because of trading losses while the other will enjoy handsome profits. Then, this scheme will take on some of the characteristics of a Ponzi scheme if the pool operator creates a new limited partnership, advertises his success from the results of the profitable pool, and gets those who participated in the successful pool to provide positive word-of-mouth comments about his abilities. Thus, it is key to the success of such schemes that the participants in the original two pools don't know each other.

In this example, not only did the pool operator violate the laws and regulations that prohibit such conduct, he also committed a breach of contract. As the general partner, the pool

operator breached the contract used to form the limited partnership because he violated the fiduciary duties that he owed to the limited partners.

Supervisors and compliance managers of brokerages should be on the lookout for this type of activity. They can do little, however, if the general partner maintains the trading accounts at two separate brokerages.

When investigating these schemes, the CFE will need to acquire the trading records of all pools run by a pool operator to establish if such a trading scheme has occurred. The comparison of market positions over time is simple and the information is easily obtainable from the brokerages once it is discovered who they are.

Block Order Schemes

A *block order* is an order placed for the sale or purchase of a significant number of securities. Often, a block order occurs when several different accounts are combined on the same order. For example, a broker might wish to execute the same buy order for ten of his customers. To accomplish this, he might write an order ticket such as: "For account 12345 and others, buy 100 contracts of December cattle at the market." The justification for this type of order is that it is time sensitive. If the market is volatile, customers will need their order executed as quickly as possible. Writing ten separate order tickets for each account and calling the orders to the trading floor separately would take too much time. By combining all the orders on one ticket and providing one account number, the broker can save time. He will add the other account numbers and quantities to the order ticket when the executed order (fill) is reported back to him.

There is, however, potential for abuse with this type of transaction. Prices move rapidly in volatile markets, and with such block order transactions, the accounts that the order has been executed for have not all been made known. The time from when the block order is placed and when the fill is reported back to the broker can take several minutes. On some busy days, it can take an hour or more before the fill is reported back to the broker. During this time, the market is moving and the executed order will either be in a loss or gain position by the time it is reported back. It is during this lag time when fraud can occur.

For example, assume that 100 contracts of December cattle were bought at 80.00 (cents per pound) and that when the fill is reported thirty minutes later the market is at 81.00. This favorable change in market price (100 points) is equivalent to $400 profit per contract or

$40,000 profit for the entire order. After the fill is reported back to the broker, he gives out the "other" account numbers to the floor clerk to complete the order, with 55 contracts going to a favored account and five contracts going to the other nine accounts. The broker then immediately sells 55 December cattle contracts for the favored account, realizing a $22,000 profit. Of course, if the market had moved lower by the time the fill was reported, the favored account would not have been added to the order or the loss taken would have been minimal.

To prove such a scheme, the fraud examiner will need to obtain and analyze all of the following items:

- The monthly brokerage recap of the salesman
- Copies of all order tickets written by the salesman for the time period in question (brokerages must keep the hard copies for several years)
- A copy of the telephone audio recording of the placement of the order and reported fill from the trading floor (all calls to the trading floor are recorded and archived)
- Copies of the "daily equity statements" provided to the salesman by the brokerage firm detailing account numbers, account names, open positions, and the cash value of all accounts represented by the salesman

Market Manipulation

Market manipulation is a type of securities fraud consisting of a series of transactions designed to artificially raise or lower price or to give the appearance of trading activity for the purpose of inducing others to buy or sell. Market manipulation is especially common with penny stocks or micro-cap stocks. *Penny stocks* are low-priced (usually less than $5), speculative securities that are registered but do not meet the listing requirements of an exchange. *Micro-cap stocks* are the stocks of companies with very small market capitalization. In market manipulation schemes, the stock is sold to unsuspecting victims once the price has been artificially inflated.

Insider Trading

Insider trading occurs when an *insider*—someone who possesses inside information about a security—buys or sells securities on the basis of material information about the security that is not available to the public. *Inside information* is any material, nonpublic information about a security that is not generally available to the public and that could affect the security's price.

Examples of insider trading include:

- Corporate officers, directors, and employees who traded their corporation's securities after learning of significant, confidential business developments
- Friends, business associates, and family members of corporate officers, directors, and employees who traded the corporation's securities after learning of significant, confidential business developments
- Employees of law, banking, and accounting firms who were given inside information to provide services to the corporation whose securities they traded
- Government employees who traded a corporation's securities after learning of inside information about the corporation because of their employment with the government

Most jurisdictions have rules that forbid investors from buying or selling securities where the decision to buy or sell is based on material, nonpublic information, but the rules and efforts to enforce them vary widely. Some countries are strengthening their existing insider trading laws, some countries are only beginning to establish insider trading laws, and others do not enforce their laws already in place.

There are two basic arguments for prohibiting insider trading. The first argument posits that insiders should not be permitted to earn profits based on an informational advantage not held by the investing public. The second argument contends that insider trading undermines public confidence in the securities markets. That is, if investors fear that insiders will regularly reap profits based on unfair advantages, investors will not be as willing to invest. A lower number of investors will lead to a lower demand for securities, which in turn will lead to lower stock values and a deflated market.

Often, insider trading is an abuse of confidentiality, and securities markets are prime targets for such abuses because successful security transactions often require the astute use of confidential information. Frequently, insider trading involves trading by those in a position to use confidential information about factors affecting the market value of securities before such information is made known to the public.

Moreover, under the legal theory of misappropriation, an insider's use of nonpublic information to profit from the purchase or sale of securities may violate the insiders' fiduciary duty to their company or shareholders, although not all courts accept this argument.

Front Running—Dual Trading

Front running is a type of insider trading. Although it usually will not cause a direct loss to the customer, front running violates the rules of many exchanges. *Front running* involves the use of the privileged knowledge of a customer's order to buy or sell a large amount of a commodity, option, or security that, because of its size, is likely to move the market. Back office personnel could have knowledge of such an order and buy or sell for their own account ahead of the customer. Because order fillers on the exchange floor are allowed to trade for their own account and fill orders for customers (dual trading) they also have an opportunity to engage in front running.

Consider the following scenario: An order is received from a hedger to sell 500 December cattle futures contracts at the market. If the order filler knows that current market conditions are such that this order will move the market significantly lower, it would be very tempting to sell a few contracts for himself and profit from the market decline when he executes the customer order. Order fillers are required to operate in the best interest of the customer and "work" the order to get the best price. However, once the trader has established his short position, it is really in his own interest to drive the market as far down as possible when executing the 500 contract sell order. In this situation, the order filler might not give his best efforts and could hurt the customer.

In today's markets, which contain sophisticated surveillance technologies, exchange investigative personnel actively guards against this type of activity. The time stamps on the customer order, time and sales reports from the exchange, and the account activity of the trader would have to be obtained and examined to substantiate any front running allegations. This information is easily obtainable. Brokerage compliance personnel should easily detect front running by back office personnel by periodically checking their account activity or prohibiting them from opening trading accounts at all.

Material Misrepresentations and Omissions

Securities laws require that the investor receive full and fair disclosure of all material information, and they make it unlawful for anyone to obtain money or property by using a material misstatement or omission in the offer or sale of any securities.

Accordingly, misrepresentation occurs when an advisor gives an investor or prospective investor false or misleading information in an investment suggestion or a trading strategy he suggests a client undertake. An *omission* occurs when the issuer, in connection with the offer

or sale of securities, omits a material fact, or when the professional fails to inform the investor of material facts.

Making misrepresentations to the investor or failing to inform the investor of certain facts (omissions) is a violation of law only if the misrepresentation or omission is material. That is, for a misstatement or omission to be fraudulent, it must be material. A fact is *material* if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision.

As a general rule, to determine materiality, the fraud examiner needs to answer the following question: "Would a reasonable investor wish to know this information to make an informed decision?" If the answer is "yes," then this information, or the lack thereof, has a high likelihood of being deemed material. (If an actual investor acted based on the misrepresentation, that clearly strengthens the case, but it is not essential that the false or misleading statement influenced an investor, merely that a reasonable investor could have been so influenced.)

For example, if the issuer of a biotechnology stock falsely claims that the government agency responsible for reviewing and approving drugs has approved the entity's new cancer drug, the statement would be a misrepresentation that is material to any prospective investor. Similarly, if the chairman of a company had recently been released from prison after serving time for securities fraud, this information would be material and therefore should be included in any offering document. Failure to disclose this fact would constitute an omission of a material fact.

Securities Fraud by Unregistered Persons

Often, individuals who are not registered with securities regulators will engage in securities-related misconduct. When conducting examinations relating to alleged violations of securities laws, the fraud examiner should always begin by seeking the answer to these crucial questions:

- Is the security registered? If not, does it meet an exemption?
- Is the person offering or selling the security registered? If not, is the transaction exempt?
- Are there indicators of fraud present?

Those involved in the securities industry might be regulated by several agencies. In the United States, securities broker-dealers must register with the Securities and Exchange

Commission (SEC), and they must register in those states where they plan to do business. If they plan to do business with the public, they must also become associated with the Financial Industry Regulatory Authority (FINRA). Many regulatory agencies and exchanges throughout Europe also have registration and reporting requirements.

Backdating Stock Options

Backdating refers to the practice of marking a document with a date that precedes the actual date.

As a supplement to salary, companies frequently offer employees stock options, which grant the recipient the privilege to purchase a share of the company's stock at a future date for a specific price, called the strike price. A *strike price* is the value of a share at a particular date. Generally, the strike price is set at the price of the underlying stock on the day the option is granted; therefore, the option becomes valuable only with future increases in the stock price.

Companies grant stock options as an incentive for employees to boost company performance and thus raise the stock price, but the practice of backdating stock options gives the employee a chance to profit by purchasing stock at past low prices, providing an immediate payoff. Backdating stock options occurs when a company alters the date of the grant to a time when the stock was trading at a lower price in the interest of making the option instantly valuable and further increasing the employee's gain if the stock price continues to rise.

EXAMPLE

On June 1, 2009, Company XYZ grants its CEO a stock option that provides the executive the right to purchase 100 shares of XYZ stock on January 1, 2010, for the strike price. Per its usual policy, the strike price is set at the price of the company stock on the date of the option grant. On June 1, 2009 (the grant date), XYZ stock was trading at $40 per share. Therefore, if the stock price increases to $45 per share by January 1, 2010, the CEO could exercise the option and purchase the shares for $40 per share, and then sell them immediately on the market for $45 per share, resulting in a gain of $5 per share.

However, the company has recently experienced a dramatic increase in its share price. On May 24, 2009, the stock was trading for $15 per share. To provide the CEO with an opportunity to exploit the increase in share price, even though it has already occurred, the company chooses to backdate the stock options to make it appear as if the options were

granted on May 24, 2009. Because the strike price is set at the price of the stock on the option grant date, the strike price is effectively changed to $15 per share. As a result, the CEO now has the option to buy 100 shares of XYZ stock on January 1, 2010, for $15 per share. Thus, the CEO has immediately gained $25 per share (the difference between the stock price on the actual grant date of June 1 and the stated grant date of May 24) based solely on the manipulation of the grant date used.

Investigative Tips

This discussion examines some of the resources that fraud examiners should use when investigating suspected securities fraud.

Promotional Materials

When investigating allegations of securities fraud, the examiner should examine the prospectus, sales literature, contracts, and any correspondence.

Usually, when investigating allegations of securities fraud, the fraud examiner will discover that various types of solicitation materials have been provided to investors and potential investors. Solicitation disclosure is often in the form of documents titled "prospectus," "offering memorandum," or "private placement offering memorandum." These documents can sometimes provide the "smoking gun," and should therefore be examined in detail, especially in cases involving misrepresentations or omissions of material facts.

Additionally, examiners should examine the information in advertising media that is designed to persuade the public to invest. The examiner should ask: How did the investor hear of this opportunity? Through cold calls, direct mail, newspapers, magazines, television, or the Internet?

A properly prepared prospectus (which usually indicates that the issuer claims the security is registered) or a private placement memorandum (the issuer claims the security is exempt from registration requirements) would normally be expected to contain detailed information concerning the issuer and the security being offered.

Solicitation information should include various types of information. It should describe the type of security, the initial price, and the amount being offered for sale. The issuing company, its business, products, background, and the qualifications of its officers and

directors should also be described. Any legal problems involving the company or its officers should be disclosed. The financial condition of the issuer should be discussed with audited financial statements where applicable. Frequently, there will be projections or forecasts of expected future growth and development (see "safe harbor" provisions discussed earlier). Usually, there will be risk disclosures of various kinds in bold font stating that, for example, "these securities have not been registered" or "purchase of these securities involves a high degree of risk."

These documents should be examined thoroughly for misrepresentations and omissions. Look closely at the background of principals. If in doubt, conduct a detailed background investigation of the principal officers of the corporation. Look for any previous criminal or regulatory action relating to securities fraud or offenses involving dishonesty. Also check for lawsuits, bankruptcies, or other civil or administrative action against the entity or its principals. If there is evidence of legal action, look for the disposition of the action and for potential evidence gathered during the course of the suit. Also, verify any claimed experience in the relevant industry or academic qualifications.

Once the background investigation is complete, compare the background information with the information, if any, disclosed in advertisements and the offering document.

Also, when investigating an entity's background, the examiner should seek to answer the following questions:

- What promises are made regarding the viability of the product or service? Is a patent claimed? Does it exist?
- Is there a functioning business that can be checked out or is it in the developmental stage? Ascertain when and where the corporation was legally incorporated, or in the case of a partnership, where it was legally filed.
- Are investors promised guaranteed returns?
- Can financial statements concerning assets, liabilities, and income be verified?
- How will investor funds be used? Follow the money trail. Were the proceeds invested as represented or used for other purposes? Is the issue potentially oversubscribed?
- Are sales commissions paid to unregistered persons? Usually this is illegal. Also check to see if commissions paid are unusually high or are concealed from investors.
- Are the insiders retaining a majority of the stock while the investors fund the company?
- Are there any other undisclosed benefits to insiders?

- Is there adequate risk disclosure? Investors might not have been made fully aware of a high percentage of failure, the degree of competition, or inexperience on the part of the principals.

MONEY LAUNDERING

Introduction

Money laundering is the disguising of the existence, nature, source, control, beneficial ownership, location, and disposition of property derived from criminal activity. Put differently, money laundering is the process by which criminals attempt to disguise illicit assets as legitimate assets that they have a right to possess and spend. In this context, the term *assets* assumes the wider definition of that which is physical, intangible, or represented in the form of rights or obligations, such as a pension or trust fund.

Money laundering operations are designed to take the proceeds of illegal activity, such as profits from drug trafficking, and cause them to appear to come from a legitimate source. Once illegal money has been laundered, the perpetrator is able to spend or invest the illicit income in legitimate assets.

Money laundering is a big business, although estimates of how big differ greatly. Because it is illegal and thereby falls outside the realm of official economic statistics, any estimate of global money laundering is derived from a combination of experience, extrapolation, and intuition. The International Monetary Fund (IMF) estimated that the aggregate level of money laundering is between 2 to 5 percent of the world's gross domestic product (www.fatf-gafi.org), which amounts to trillions of dollars.

The laundering of money occurs in the context of all forms of illegal activities. Often, criminals seek to launder money by conducting transactions in cash (currency) in such a way as to conceal their true nature. Problems can, however, occur regarding large volumes of cash—transporting it, converting small currency denominations to larger denominations, and converting cash into assets that can be invested or spent.

The Money Laundering Process

There are many ways that criminals can launder funds, but the process itself is generally divided into three stages: (1) placement, (2) layering, and (3) integration.

Placement

Placement is the first stage of the money laundering process. In this stage, the launderer introduces his illegal profits into the financial system. It is at this stage that legislation has been developed to prevent launderers from depositing or converting large amounts of cash at financial institutions or taking cash out of the country.

Placement can take any number of forms. If the money launderer has a large amount of cash, he can physically move the money to a foreign location or carry it out of the country in a suitcase and deposit it in an offshore bank. Another choice is to *structure* transactions, where a deposit or other transfer is made using a method that is specifically designed to avoid regulatory reporting requirements or an institution's internal controls. Many countries require financial institutions to report all currency transactions above a certain threshold (e.g., more than $10,000) to the government. As a result, the most common type of illegal structuring scheme in the money laundering context is *smurfing*, where the launderer breaks up the illicit money into smaller amounts and deposits it into bank accounts or purchases cashier's checks, traveler's checks, or money orders. A red flag of a smurfing scheme is a customer who attempts to make many deposits just under the reporting threshold.

Money laundering schemes are most often detected at the placement stage. It is the most dangerous stage for the criminal because the placement process creates a direct connection between the profits and the crime; at this stage, the launderer is still associated with the crime's physical evidence.

Layering

If the placement of the initial funds goes undetected, the launderer can design numerous financial transactions in complex patterns to prevent detection. This stage of the money laundering process is referred to as *layering*, and it represents the most difficult area of detection. Once the funds have been deposited into a financial institution, a launderer can move them around by using layers of financial transactions designed to confuse the audit trail. The money can even be transported out of the country. Often, launderers take advantage of jurisdictions known for their lack of cooperation with foreign courts, investigators, and law enforcement agencies. If a launderer moves funds through several such jurisdictions, tracing the final destination can be burdensome.

Historically, layering primarily involved smuggling cash or running funds through traditional financial institutions, both domestic and foreign. While these practices are still very common, several types of transactions outside of traditional institutions are increasing in volume, such as alternative remittance systems, trade-based laundering, and digital currencies.

Integration

Integration is the final stage in the laundering process. In this stage, the money is integrated back into the economy in a way that makes it appear to be part of a legitimate business transaction. This stage of the process is also difficult to detect; however, if the integration process creates a paper trail—such as deeds for real estate, invoices, loan documents, transaction reports at financial institutions, or checks—and if there is cooperation from informants or foreign entities, then the chances of detection are improved.

A money laundering scheme cannot be successful until the paper trail is eliminated or made so complex that the flow of illegal income cannot be easily traced. The number of steps used to launder funds depends on how much distance the money launderer wishes to put between the illegally earned cash and the laundered asset into which it is converted. A greater number of steps increases the complexity of tracing the funds, but it also increases the length of the paper trail and the chance that the transaction will be reported.

The objective of money laundering is not only to disguise the source of illegal funds, but also to convert large stores of currency into other assets. In some cases, illegal funds are spent on personal assets, such as homes, cars, jewelry, and furniture. But the typical money launderer will not dispose of all his illegal currency in this manner; he will want to have a certain amount of liquid reserves for spending. Keeping large bundles of cash is inefficient because they are difficult to hide and transport. Therefore, money launderers will often convert substantial portions of their currency into negotiable instruments such as cashier's checks and money orders, which are routinely issued by financial institutions. Criminals prefer these negotiable instruments for two reasons. First, cashier's checks and money orders are bearer instruments, and the holder can use them or deposit them without having to prove the source of the funds. Second, they are "liquid" assets because the holder can use them immediately.

The following is an example of how a large money laundering scheme operated in the United States.

EXAMPLE

Alberto Barrera ran a rather sophisticated structuring operation that involved bank accounts in cities all over the United States. Barrera and his accomplices would fly to different U.S. cities, traveling to various banks and purchasing cashier's checks and money orders in amounts less than $10,000 (to avoid U.S. federal reporting requirements). They would then travel to banks in other cities, where they would deposit some of the purchased checks and money orders into accounts controlled by Barrera. Once the money was converted or deposited, it was transferred to banks in other countries.

Money Laundering Methods

There are many money laundering methods, and new techniques arise continuously. This makes keeping up with regulations and learning how to investigate such crimes an ongoing task for anti-money laundering (AML) professionals. There are many common and emerging schemes of which fraud examiners should be aware.

Using a Front Business to Launder Funds

One of the most common methods of laundering funds is to filter the money through a seemingly legitimate business, otherwise known as a *front business.* A front business can be a very effective way to launder money for a number of reasons. Front businesses provide a safe place for organizing and managing criminal activity, where the comings and goings of large numbers of people will not arouse undue suspicion. In addition, a front that conducts legitimate business provides cover for delivery and transportation related to illegal activity. The expenses from illegal activity can be attributed to the legitimate enterprise, and the illegal revenues can be easily placed into the enterprise.

The two methods most commonly used to hide assets or launder money through a front business are:

- Overstating reported revenues and expenses
- Depositing, but not recording, revenue

Overstating Reported Revenues and Expenses

Overstating revenues occurs when the money launderer records more income on a business's books than the business actually generates. The fictitious revenue accounts for the illegal funds that are secretly inserted into the company.

The following example shows how the owner of Luxury Antiques uses overstatement of reported revenue to disguise money earned from other sources.

EXAMPLE

Luxury Antiques is a chain of antique stores with several locations within and around a major metropolitan center. It is locally owned. The bulk of its activity is in the sale of antique figurines. Luxury Antiques sells an average of 200 pieces per month.

Customers are encouraged to pay in cash and, when they do so, are usually pleased when they receive a "special discount" (which can be as high as 25 percent) off of the "official invoice price." The invoice the customer receives shows the full price rather than the discounted price. If a customer questions this practice, the store owner explains it is done for "competitive reasons."

Over the course of a year, Luxury Antiques sells 2,400 total figurines for an average "official invoice price" of $4,000. This yields $9,600,000 of recorded revenues. Actual cash received from customers falls short of that figure by 20 percent, for a total of $7,680,000. The difference—$1,920,000—is now available for laundering purposes. To take advantage of this situation, the owner simply deposits cash receipts of $1,920,000 from his illicit sources as legitimate business income. The result is that $1,920,000 has been successfully laundered.

Another way for Luxury Antiques to overstate reported revenues is to create fictitious sales with all the normal paperwork. If 50 fictitious sales are created each month at the average "official price" of $4,000, an additional $2,400,000 of laundered receipts are produced each year. The result is that $2,400,000 of illicit funds can be disguised as legitimate business income. (Note that this method involves potentially more risk than the first because it involves completely fabricating all the elements of a sale rather than merely modifying one part of a normal sale.)

Overstating reported expenses will help counteract the key disadvantage of overstating revenues—that taxes will be due on the reported income. But because business expenses are tax deductible, additional tax liability incurred by inflated revenues can be reduced with fictitious business expenses. Therefore, if a company overstates its revenue, it will also want to overstate its expenses to offset its tax liability.

Another reason for overstating expenses is to siphon money out of the business to make payoffs, buy illegal goods, or invest in other criminal ventures. In practical terms, the method strongly resembles the more familiar practice of padding expense accounts. Among some of the commonly used schemes are payments for supplies never received, fees to fictitious consultants, and salaries for nonexistent employees. The possibilities for fraudulent payments are limited only by the imagination.

Overstating expenses can be accomplished using various methods. Return to the hypothetical business, Luxury Antiques, and look at three strategies employed by the store's owner to inflate expenses and make the laundered cash available for criminal activity:

- Fictitious employees
- Fictitious fees
- Inflated invoices

In the following example, the owner of Luxury Antiques uses fictitious employees to inflate expenses.

EXAMPLE

Luxury Antiques has six salespeople and two assistant sales managers on the payroll. All eight employees are fictitious. Their pay, as well as sales commissions paid to the fictitious sales managers, represents an annual expense inflation of $500,000. Luxury Antiques' owner does not have to pay taxes on this $500,000 and can take that amount of cash out of the business and put it into his own pocket.

In the following example, the owner of Luxury Antiques uses fictitious fees to inflate expenses.

EXAMPLE

Luxury Antiques has lawyers and consultants on "retainer" for a total of $600,000 per year. They perform little or no business work, but they do submit invoices for fees on

expensive stationery and with suitably vague descriptions of their activities. Once again, the money paid out is not taxed and can be put to illicit purposes.

In the following examples, the owner of Luxury Antiques uses inflated invoices to amplify expenses.

EXAMPLE

Luxury Antiques makes purchases from a supplier, who agrees to inflate invoices by 25 percent. The supplier then gives back four-fifths of the inflated amount, keeping the other one-fifth. On $500,000 of actual purchases per year, Luxury Antiques reports expenses of $625,000—an inflation of $125,000.

EXAMPLE

A Luxury Antiques supplier, Import Associates, which provides 40 percent of the antiques sold by Luxury Antiques, sells figurines to Luxury Antiques in lots consisting of 150 to 200 pieces. The individual prices and the exact number of figurines in each lot are vaguely described in these "wholesale" bills of sale. As a result of its long association with Import, Luxury Antiques is able to arrange for the invoices to be inflated by an average of 30 percent. This gains Luxury Antiques about $580,000 per year in inflated expenses (assuming 960 figurines at an average real cost of $2,000 = $1,920,000). By inflating the invoice by 30 percent, the invoice price will reflect a price of about $2,500,000, the difference representing laundered expenses.

It can be difficult to detect money laundering that includes both overstated revenues and expenses. When artificial price inflation is applied in moderate percentages to goods and services whose market value is difficult to establish (e.g., artwork, used cars, consulting fees, advertising expenses), detection is exceedingly difficult without inside information.

Conversely, complete fabrication of transactions or ghost employees is somewhat easier to spot.

Depositing, But Not Recording, Revenue

In one of the most common schemes at the local level, launderers deposit illicit cash into the front company's bank account rather than disguising it as revenue. These funds are not recorded like the money that flows into and out of a business as revenues and expenses. Like

a loan, this excess cash represents the proceeds of a transaction that is handled outside of the front business's daily activity. Also, like a loan, it appears on the company's balance sheet, which includes both assets and liabilities.

EXAMPLE

Each month, an extra $360,000 is deposited into Luxury Antiques' bank account. To offset the entry, sales are credited for the laundered cash by either being fictitious or marked up.

This type of scheme can be detected by examining the business's revenue records. Every legitimate asset in a company's possession must come from somewhere—if not from revenues, then from a limited number of other credible alternatives. The basic alternative sources include loans, proceeds from the sale of property or equipment, and capital investments from shareholders. All of these transactions require significant documentary evidence, which the fraud examiner should seek out to explain any suspicious infusion of cash into a suspect business.

Favorite Businesses for Hiding or Laundering Money

In general terms, the businesses chosen for money laundering possess one or more of the following characteristics:

- Revenue—Often, businesses chosen for money laundering are ones with a revenue base that is difficult to measure. Generally, revenue is difficult to measure in businesses with revenue from cash transactions with a highly variable amount per customer. In such businesses, extra money can be brought into the business and disguised as revenue.
- Expense—Front businesses often have variable expenses that are difficult to measure. With such businesses, launderers can extract money without raising undue suspicion.
- History—Many businesses used to launder money have historical ties either with the ethnic base of a particular criminal group or with other parts of an industry—either suppliers or customers.

BARS, RESTAURANTS, AND NIGHTCLUBS

Bars, restaurants, and nightclubs are commonly used to front money laundering operations for a number of reasons. These businesses charge relatively high prices, and customers vary widely in their purchases. Sales are generally in cash, and it is difficult to match the cost of providing food, liquor, and entertainment with the revenues they produce. Moreover, the range of goods and services these types of businesses provide is relatively broad.

Fast food restaurants are also frequently used as a front for money laundering operations. Although they tend to charge lower prices than other types of restaurants, most of their sales are made in cash, and expenses can be easily inflated. As a result, a red flag of front businesses is observing a low amount of business, despite the business's books showing a relatively high income for that period.

VENDING MACHINE OPERATIONS

Vending machine operations also possess many characteristics favorable to a money laundering operation. They have a highly variable and difficult to measure volume of cash receipts, and in large operations, there is a fair amount of flexibility with various transportation, installation, and promotion expenses, providing cover for the withdrawal of laundered funds.

WHOLESALE DISTRIBUTION BUSINESSES

Wholesale distribution businesses have historically been a prominent part of money laundering. Depending on the competitive environment, wholesale distributions do not normally require the same managerial skills necessary to operate a high-volume retail business. Wholesale distribution is attractive for money laundering because it is well embedded in a community's economic fabric.

From the revenue perspective, wholesale operations are somewhat less ideal for launderers because invoicing, rather than cash transactions, are typical. Even so, a diverse product line and falsified invoices will provide a substantial amount of flexibility. More important, the industry is ideal for money laundering from the standpoint of expenses. The activities required to run this kind of business are so diverse and difficult to measure that expenses are easy to inflate. A wholesale business's buildings, warehouses, transportation fleet, and contact with retail establishments are all attractive factors.

The Real Estate Industry

Money launderers often use the real estate industry to launder illicitly obtained money. Generally, the real estate industry is attractive to money launderers for various reasons. For example, the vast array of financial transactions linked to real estate provides money launderers an exceptional range of options for abusing these procedures to launder and use illegally obtained funds. In addition, real estate transactions often involve multiple parties (such as brokers, agents, and appraisers), which can obscure the source of investment funds

and the identity of the true owner. Finally, money launderers might earn additional profits from introducing illicit funds into the real estate industry, especially in vibrant real estate markets.

Although there is a vast number of methods to launder money in the real estate industry, there are a few common schemes that warrant identification and discussion, including:

- Loan-back schemes
- Back-to-back loan schemes
- Shell entities
- Appraisal fraud
- Monetary instruments
- Mortgage schemes
- Indirect investments in the real estate industry

Loan-Back Schemes

Money launderers often use loan-back schemes to finance the purchase of properties directly or indirectly through purchasing shares in property investment funds. In a typical loan-back scheme, money launderers will deposit illicit funds in an overseas entity that they own, and then the entity loans the funds back to the launderers. The purpose of the loan is to make the money source appear legitimate and to conceal the parties' identities or the nature of the financial transactions associated with the loans.

Back-to-Back Loan Schemes

As with loan-back schemes, money launderers often use back-to-back loan schemes to purchase real property using illicit assets (or receive real property as a result of fraud). In a back-to-back loan scheme, a money launderer obtains a loan by presenting collateral, which originated from illicit funds, to a financial institution. Like the loan-back scheme, this technique gives the loaned money the appearance of a genuine loan.

Shell Entities

Money launderers often use shell entities to purchase real estate with illicit funds. Generally defined, *shell entities* are organizations without active business or significant assets, and they can take the form of limited liability companies, trusts, business trusts, corporations, and other legal entities. Because there is a lack of transparency in the formation of shell entities, money launderers often use them to hide the identity of the true owner, the source of the money, or the destination of the money.

Appraisal Fraud

Appraisal fraud is often associated with money laundering schemes. Money launderers might purchase properties to launder money or might use illicit funds to service the interest on the debts. Such schemes can conceal the true identity of the property owners and the true origin of the funds used in the transaction.

Appraisal fraud occurs where appraisers fail to accurately evaluate the property, or when the appraiser deliberately becomes party to a scheme to defraud the lender, the borrower, or both. A common technique is the over- or under-valuation of property, which consists of buying/selling property at a price above/below its market value. In addition to manipulating appraisals, money launderers also over-value property through a series of subsequent sales, each time at a higher price, which tend to conceal the true purposes of the transactions.

Monetary Instruments

In many instances, money launderers purchase, build, or renovate property with cash, wire transfers, or other payable-through accounts. This allows the integration of large sums of illicit money into legal financial systems. If sold at a later time, it is difficult to relate the transaction to any criminal activity and therefore successfully conceals the true origin of the illicit funds and their ownership.

Mortgage Schemes

Often, money launderers will use illicit funds to pay the interest or repay the principal on mortgage loans, and in so doing, the illicit income is converted into seemingly legitimate profits when the property is sold. Mortgage schemes also involve under- and over-valuation of property. For example, in a common under-valuation scheme, a money launderer will under-value the purchase price of property, obtain a mortgage loan for the under-valued amount, use the loan to pay for the under-valued price, and pay the excess amount under the table with illicit funds.

Indirect Investments in the Real Estate Industry

Indirect investments in the real estate industry, which are those in which the investor has no direct control over the assets or investment vehicle, offer opportunities to conceal an investor's identification and monetary sources primarily because multiple parties are involved with the process.

Emerging Payment Methods and Schemes

The technological landscape behind conducting transactions is constantly changing, in large part to make payments faster and more convenient. This discussion examines some emerging payment technologies used to launder money, and it includes discussion of methods that have existed for a while, but are in the process of becoming prominent concerns.

ATMs

Often, launderers use automatic teller machines (ATMs) to launder money. ATMs are relatively inexpensive, and money launderers purchase the machines and place them either in establishments they control or in legitimate businesses. The machines work the same as any other ATM machine, and all transactions are legitimate. The money launderer simply fills the machine with cash from illegal activities. The customer uses the machine and never realizes the cash's source.

The ATM banking system debits the cardholder's account and credits the ATM owner's bank account. At the end of the month, the launderer receives a bank statement showing funds being deposited from a legitimate financial institution.

This option is attractive for money launderers because there are currently few jurisdictions that regulate the use and operation of privately-owned ATMs. There is usually no requirement to check the backgrounds of purchasers of the machines, and there are no mandatory reporting procedures and no rules for maintaining ATM sales records.

Prepaid Access Items

Broadly speaking, prepaid items are goods and services that are paid in advance of their actual purchase. Many businesses offer customers the ability to prepay for products and services, and this practice is beneficial to customers because it gives them the ability to give these items as gifts and also provides convenience. Moreover, prepaid items are great for businesses. They generate cash flow for items that have not been purchased yet, and some prepaid purchases are never redeemed, resulting in a windfall. Perhaps most important for large companies, prepaid items can open up international markets.

CATEGORIES OF PREPAID ITEMS

Prepaid items can be broken down into three categories: open loop, closed loop, and semi-open loop.

OPEN LOOP

Open-loop items are the most versatile form of prepaid item, meaning the funds on these items can be used for any type of purchase where the seller accepts that type of payment. For instance, prepaid debit cards are generally open-loop items and can be used virtually anywhere credit cards are accepted. They are usually associated with a credit card company (e.g., MasterCard or Visa) to facilitate the transaction. And with many open-loop items, users can withdraw cash from ATM machines around the world.

While in some ways they function similarly to checking accounts, open-loop items do not allow for negative balances; the user can only spend the amount on the card. Additionally, the user information that the issuer of the prepaid card collects is usually less than what a bank would collect for a person opening a checking or savings account. The prepaid issuers usually charge the user for each transaction, issue charges gradually over time, or institute some other type of fee.

While not as common as prepaid debit cards, other items could be considered open loop if they allow for "paid" funds to be withdrawn. For instance, mobile phone accounts that allow for withdrawal and transfer can be open loop.

CLOSED LOOP

Closed-loop prepaid systems are those where the user may only use the stored value to purchase items from the issuing organization or its affiliates, making them less versatile than open-loop items. Furthermore, closed-loop items generally may not be redeemed for cash, even at the issuing organization.

SEMI-OPEN LOOP

Also called *semi-closed loop items*, *semi-open loop items* can be used to purchase goods and services wherever sellers accept that form of payment. In the case of prepaid cards, they are also generally associated with a credit card company. However, as with closed-loop item, semi-open loop items are not redeemable for cash.

VULNERABILITIES OF PREPAID ITEMS

While mainly used for legitimate business, prepaid items can also be used by money launderers to hide and transfer assets. Some examples of prepaid items with potential for money laundering include:

- Merchant gift cards
- Prepaid debit cards (as opposed to a standard check/debit account)
- Payroll cards
- Prepaid mobile phones
- Mass transit cards
- Gaming and lottery cards

The most attractive aspect of prepaid items to money launderers is that issuers of these items and the people who use them are under relatively fewer regulatory restrictions than traditional financial institutions and banking customers. For instance, anti-money laundering regulations do not always cover prepaid items.

Additionally, traditional financial institutions are required to perform a certain minimum of due diligence on their customers, but for prepaid issuers, this burden is currently substantially less.

Prepaid items also offer a greater degree of potential anonymity than basic credit or debit cards. A person is rarely required to have a face-to-face transaction during any part of the process of obtaining and using a prepaid item. Moreover, the use of stolen IDs and fake addresses makes it possible for launderers to avoid attaching an obvious identity to the prepaid item.

Furthermore, prepaid items can be transported abroad with relative ease; thus, they can be used to move funds internationally and purchase goods or services almost anywhere.

Given the vulnerabilities of prepaid items, there are various ways in which criminals can use them in laundering schemes.

As a means of placing illicit proceeds, launderers could initially load the funds in prepaid items like open-loop cards and gift cards, which are fairly easy to obtain. Although there are maximum limits to the amount that a person can load onto a rechargeable prepaid item each

day, as well as total maximum account values imposed by the issuer, criminals could obtain multiple prepaid cards and add funds to them over time. The benefit of this use would be a less bulky, less suspicious, and more transportable type of asset.

Once the illicit funds are placed on prepaid cards, launderers can easily move them around for additional layering. And because prepaid items can be transported abroad with relative ease, criminal organizations often use prepaid items to transfer funds out of the country. Moreover, because prepaid items offer some level of anonymity, the transactions a suspect makes using prepaid items will not appear on the suspect's personal account statements.

Mobile Payments

Mobile payments, also known as *mobile banking*, involve using an account associated with a mobile phone—as opposed to cash, credit cards, and debit cards—to facilitate transactions. Similar to the way in which credit and debit cards significantly cut into the use of checks and cash for consumer transactions, mobile payments are likely to grow in popularity.

As compared to other transaction methods, mobile payments are vulnerable to money laundering schemes in a few key ways. For one thing, given that mobile payments are still in the process of growing and developing definition, regulations are not as sophisticated or complete as they are for older payment systems. Also, many developing countries lack functional AML and anti-terrorist laws, making mobile payments outside of the jurisdiction even more difficult to prevent and trace. Also, a user can send mobile payments to almost anywhere in the world, making them a tool that launderers often use to move funds to foreign jurisdictions.

In addition, the use of prepaid phones causes substantial money laundering issues because the owner of a prepaid phone can be virtually anonymous. Prepaid phones can be purchased for cash, and the user typically does not need to provide personal information to open or add funds to an account associated with the phone. Anonymity is a strong attraction for launderers because it helps to obscure the paper/digital trail leading back to them.

Digital Currencies

In response to market demand, online payment services, which accept funds in a variety of ways to transfer payment either to an individual or a merchant, are emerging. In addition, the increasing demand for new payment methods has led a growing number of online markets

to embrace online payment systems, which set their own clearing and settlement terms and offer no consumer protection or financial regulation. Since most transactions through these service providers are considered final and provide no recourse to individuals who believe they have been defrauded, law enforcement agencies suggest that they have become a popular payment system for individuals perpetrating online fraud.

Digital currencies are a type of online payment method that has emerged as a money laundering concern. Broadly defined, *digital currencies* are currencies that exist and are traded in a digital format. The term typically excludes government-backed currencies, despite the fact that they can also exist and be traded digitally. Digital currencies can come in several forms and can have limited or broad uses. Among the most popular digital currencies is Bitcoin, which features a peer-to-peer network that allows users to send units of the currency to each other online without the use of a traditional financial institution.

Digital currencies are often vulnerable to money laundering because many of them function as international person-to-person payment systems, which cross jurisdictional boundaries, creating difficulties for authorities pursuing enforcement or legal actions. As is typical with developing payment systems, digital currencies face less strict regulations than payments made through traditional financial institutions. Furthermore, many service providers who exchange or otherwise deal with digital currencies do not have effective customer identification or recordkeeping practices, while others actively promote anonymous payments.

One of the most difficult aspects of investigating and preventing laundering through digital currencies is the sheer number of them available. For instance, in May 2013, an international law enforcement effort led to the shutdown of Liberty Reserve, a popular digital currency service based in Costa Rica. Prosecutors alleged that the Liberty Reserve was operating as an unlicensed financial transaction service and that its lax processes allowed upwards of $6 billion in illicit assets to be laundered since its inception in the early 2000s.

However, soon after this shutdown, it was apparent that launderers had already found alternatives to Liberty Reserve, such as Perfect Money. Because these service providers operate online, they can set up in countries with lenient financial regulations in a short period of time. Additionally, many of the most popular digital currencies, including Bitcoin,

are practically impossible to shut down from a law enforcement standpoint because they operate using a decentralized, peer-to-peer network.

After the rise in popularity of Bitcoin, many similar alternative digital currencies also began to appear. Many have different features, so the money laundering potential varies between them. Generally, digital currencies give parties the ability to:

- Send and accept payments from any user in the world with an Internet connection for little or no transaction fee.
- Send or accept payments without the need for any identifying information (other than the users' randomly-generated "addresses").
- Conduct transactions in unlimited volume (assuming funds are available).
- Conduct transactions anonymously (there are investigative techniques to identify parties to digital currency transactions, but a sophisticated user could make the process very difficult).
- Confirm transactions within minutes or less.

Virtual Assets

Virtual assets are similar to digital currencies, but are generally intangible assets tied to a particular service or online community. For instance, a gambling website might offer its own mock-currency, or an online game might distribute virtual assets that users can purchase.

Often, virtual assets gain value outside of their original context (i.e., they gain "real world" value) because they are scarce and can be sold to other people through online markets. The laundering process using virtual assets often resembles some variation of the following:

1. Illicit assets are used to purchase virtual currency or items from third parties. Alternatively, a criminal organization hires people to gather the virtual resources themselves.
2. If the virtual assets are bought from third parties, the seller transfers the virtual items to an account controlled by the criminal.
3. The criminal could either sell the virtual assets himself for actual money, or give the virtual account information to another criminal as a means of transferring the value.

The actual sale price of virtual currency or items is usually not very high—a small proportion of transactions exceed a few thousand dollars. However, professional laundering

organizations can break up sales and transfers and eventually pass large amounts through the cycle.

EXAMPLE

The Seoul Metropolitan Police uncovered a money laundering ring that moved $38 million from South Korea to China during the course of 18 months. The group purchased in-game gold of an online video game "farmed" by low-cost laborers in China, and then sold it to exchangers in South Korea. The criminals placed the money into accounts opened under fake or stolen identities, and then disguised wire transfers to a Hong Kong–based paper company as product purchases. To avoid detection, group members used technology to spoof their IP address and make it look like they were operating out of an Internet café in South Korea.

Bulk-Cash Smuggling

Bulk-cash smuggling, which is the smuggling of cash out of the country where it was earned for deposit in foreign jurisdictions with lax financial institutions or to fund criminal enterprises, is also on the rise. The rise in bulk-cash smuggling is due to the increasingly effective anti-money laundering policies and procedures at financial institutions. In typical bulk-cash smuggling operations, smugglers hide cash in vehicles, luggage, express packages, commercial shipments, private aircrafts, or private boats.

For example, in 2012, an investigation into a major international bank, HSBC, revealed that criminals were using the bank to funnel large amounts of cash through its branches in Mexico. Much of this currency originated in the United States as drug proceeds before being smuggled into Mexico. An AML official of the bank estimated that at one point as much as 70 percent of the illicit currency deposited in financial institutions in Mexico was going through HSBC.

Trade-Based Money Laundering

Trade-based money laundering is generally the most complex of the money laundering methods. This method encompasses a variety of schemes that use international trade to disguise the transfers of illicit funds. Among the most notorious of trade-based money laundering operations is the Black Market Peso Exchange, a scheme where brokers purchase narcotics proceeds in the United States from cartels and exchange them for clean pesos in Colombia. Other common trade-based money laundering methods include manipulating

trade documents to over- and under-pay for imports and exports and using criminal proceeds to buy gems or precious metals.

Banks and Other Depository Financial Institutions

Unfortunately, a significant portion of money laundering occurs through financial institutions when employees intentionally—or at least knowingly—aid criminals. While there is risk of enforcement actions for violations, banks can generate a large volume of transaction fees from launderers' activities. Individual employees sometimes directly help launderers to earn a commission or to advance their careers. Moreover, management might turn a blind eye to known violations because the upshot is higher profits.

There are several ways that collusion occurs. On the individual level, it generally involves an agent of the bank or institution manipulating a control or other procedure to prevent detection of a crime. For example, a launderer who wants to smurf cash deposits could bribe a person responsible for reporting suspicious transactions or collude to provide false information in a new account application.

At the higher level, upper management could implement policies that it knows or should know are ineffective at preventing money laundering. Intent is difficult to prove in this instance, but might be demonstrated through evidence of management ignoring warnings, failing to keep up with industry standards, and implementing policies that do not provide a direct chain of responsibility to an organization's leadership.

Some banks—especially privately owned banks in low-regulatory zones—operate as front organizations for money launderers. This method can be used by large organizations to create transactions that are not likely to be reviewed by any regulatory authority (e.g., disguised bribe payments). Since the bank is essentially a front, the controlling organization can simply refuse to place controls that would stop money laundering.

Additionally, some jurisdictions have low capital requirements to start up a bank. This allows individual criminals with relatively fewer assets to also use this method.

Money Services Businesses

Money services business (MSB) is a term used in growing frequency to define a regulatory class of non-depository financial service providers that transmit or convert money. Although an

MSB has particular meanings in different jurisdictions, it generally includes any business that operates in one or more of the following capacities:

- Currency exchangers
- Check cashers
- Issuers, sellers, or redeemers of traveler's checks, money orders, or stored value
- Money transmitters
- Prepaid access providers or sellers

MSBs offer an alternative to depository institutions for both financial services and money laundering. For this reason, an individual unable to transfer illegal funds into the traditional depository banking system might turn to an MSB. In addition, most MSBs operate under less strict regulations than traditional financial institutions. For example, an MSB might not check a customer's credit report before opening an account, or it might require less rigorous proof of a customer's identity than a traditional bank. These overall less stringent requirements tend to raise the money laundering risk in certain transactions involving users of MSBs. However, there is a regulatory trend to expand certain requirements, such as customer due diligence programs, to MSBs.

Insurance Companies

Insurance policies are designed to protect assets (as well as life and health), but they are also assets in their own right. As is the case with most assets, they can become part of a money laundering scheme. Due to the recent growth in the financial products offered by insurance agents and brokers (including savings products, investment products, and tax planning services), the insurance industry has become increasingly attractive to money launderers. One of the causes for this increase is that insurance agents and brokers offer many savings, investment, and tax planning services that might be used to launder funds. Generally, the independent brokers and agents who often sell insurance products do not work directly for the insurance companies. As a result, these intermediaries might lack the knowledge or incentive to screen clients or to question payment methods, and it is this factor that money launderers often exploit.

Redemption Schemes

A person can redeem some insurance policies, such as life insurance, before the event that triggers the insurance occurs. In other words, the insurer agrees to pay the beneficiary of the

policy an amount less than what the payout on a claim occurrence (in the case of life insurance, the death of the insured) would be.

Using illicit assets, launderers can purchase life insurance or other redeemable contracts for themselves or their associates. If the investigator did not know that the launderer bought the insurance policy with illicit assets, the redemption payout would appear legitimate.

Prepayment Schemes

Insurance policies sometimes allow for premiums to be paid in advance. Some launderers make advance payments on insurance premiums. For instance, if a health insurer allowed $10,000 in advance premium payments, then the launderer could use the illicit assets to "store" those funds. Perhaps the launderer was going to buy that health insurance anyway; now illicit assets have taken care of that bill.

Moreover, some insurance policies are very expensive, such as a large company's general liability insurance, allowing for higher laundered amounts.

Canceled Policy Schemes

Launderers do not always need to keep or redeem the insurance policies they purchase. Many policies have cancellation provisions that, for a certain amount of time, allow the launderer to cancel the policy and have any unused premiums returned. This technique can be used to temporarily store illicit assets and confuse the money trail by having the cancellation paid out to a different account.

Casinos

Casinos operate in a high-volume cash-intensive industry and provide a broad range of financial services (such as deposit and credit accounts, funds transfers, check cashing, and currency exchange services) outside the traditional financial services system. As a result, casinos are susceptible to money laundering.

There are several ways that criminals use casino chips to launder funds, including:

- Holding the chips for a period of time and later cashing them in for a casino check or having the casino wire the money elsewhere

- Using the chips as currency to purchase narcotics, with the drug dealer later cashing in the chips
- Using the chips to gamble in the hope of generating certifiable winnings

Additionally, law enforcement authorities have become increasingly concerned about the potential to use the growing Internet gaming industry to launder funds. Generally created in jurisdictions without gambling restrictions, online casinos require little capital to set up. They offer virtual anonymity and many of the same features of a brick-and-mortar casino, such as standing accounts through which a patron may transfer funds via check, credit or debit cards, or wire transfers. For the most part, Internet casinos figure in the layering and integration stages. In essence, these cyber-casinos function as unregulated banks, providing virtually anonymous accounts to bettors.

Shell Companies

Shell companies are business entities that generally do not have any physical presence other than a mailing address and generate little to no independent economic value. In most situations, individuals and businesses form shell companies for legitimate reasons, such as holding the stock or intellectual property rights of another business entity, facilitating domestic and cross-border currency and asset transfers, or fostering domestic and cross-border currency corporate mergers. However, shell companies have become common tools for money laundering primarily because they have the ability to hide ownership and mask financial details, and because money launderers can create them with minimal public disclosure of personal information regarding controlling interests and ownership. This lack of transparency prevents the discovery of suspicious transactions and impedes investigations and prosecutions.

Charities and Nonprofit Organizations

Charities and nonprofit organizations are often used in fraud and other financial crimes, including money laundering. These organizations rely on gifts, and therefore can be used to disguise illicit assets. Typically, the launderer or an associate controls the organization, and can direct donated funds outside of actual charitable purposes.

EXAMPLE

In 2012, an orthodox rabbi from New York was sentenced to four years in prison for his involvement in a widespread money laundering and corruption scheme. The case was part of

> *the FBI's "Bid Rig III" crackdown that involved the arrests of more than 40 people, including politicians and other religious leaders. The rabbi ran a collection of community charities known as* gmachs. *An undercover informant approached the rabbi and sought his assistance in laundering money through the charities. The rabbi deposited check donations of almost $1 million into accounts owned by the charities. He then used an underground financial network that operated between the United States and Israel to convert the funds into cash. After taking a 10 percent commission, he physically delivered the cash to the undercover informant.*

With online donations available through non-traditional transfers (such as digital currencies), it is easier than ever for launderers to make virtually anonymous payments to corrupt charities and nonprofits.

Calling in a Specialist

Converting ill-gotten gains into cashier's checks or money orders is not particularly difficult for even the most unsophisticated criminal. However, because many launderers fear detection, they often engage others to help them launder funds.

Fraudsters may use *couriers* who arrange for the transportation of money to a site where it is converted into another form of currency. For instance, drug traffickers will physically transport money to a foreign jurisdiction, where it is deposited into a bank account or converted directly to checks or money orders. Since the courier has no apparent connection with the true owner of the funds, the money launderer retains his anonymity.

In addition, fraudsters may employ gatekeepers who facilitate access to financial services. A gatekeeper may be an individual or an institution, and frequently, gatekeepers are bankers, trust companies, lawyers, accountants, realtors, insurance brokers, stockbrokers, or other entities with access to financial services. Through investments, trust accounts, fund transfers, and tax avoidance schemes, these professionals can manipulate the financial, commercial, and legal systems to conceal the origin and ownership of assets.

Most gatekeepers are legitimate, but they offer products and services that both legitimate customers and fraudsters find attractive.

Gatekeepers often facilitate the following:

- Disguising the subject's involvement in a commercial transaction (e.g., disguising an individual's ownership in a limited partnership)
- Layering criminal property (e.g., transferring the property through a company to conceal the property's criminal source)
- Disguising the ownership of property owned by the subject

Alternative Remittance Systems

Alternative remittance systems (also called *parallel banking systems*) are methods of transferring funds from a party at one location to another party (whether domestic or foreign) without the use of formal banking institutions. These systems are characterized by the lack of direct physical or digital transfer of currency from the sender to the receiver. Instead, in the typical alternative remittance system, the payer transfers funds to a local broker who has a connection in the region where the payee is located. The latter broker then distributes the funds to the payee.

How They Work

The parties involved in alternative remittance systems form a network and track their exchanges on an informal ledger. Unlike formal financial institutions, these ledgers will generally not list specific information about the payers and payees (such as bank account numbers and names), but will keep track of amounts owed. When the first broker requests that another broker in the network distribute funds, the debt is recorded in the ledgers. These debts between brokers could be paid back by offsetting transactions (i.e., the first broker pays someone locally at the request of the second broker). Alternatively, the parties could meet to settle all outstanding debts at a later time. Below is an example of an alternative remittance system.

EXAMPLE

1. *Ana in London contacts and gives $50,000 in cash to Broker A in London to get $48,000 to Bob in Dubai. Broker A takes a commission of $2,000.*
2. *Broker A contacts Broker B in Dubai and arranges the transfer; a code is exchanged.*
3. *Broker A gives Ana a code to be communicated to Bob.*
4. *Ana communicates the code to Bob.*
5. *Broker B and Bob make contact in Dubai.*
6. *Bob relays code to Broker B and is given the money.*

7. *Broker A owes Broker B $48,000 worth of t-shirts. Broker A sends the merchandise from London to Broker B in Dubai, plus $1,000 in extra merchandise as a share of the commission.*
8. *Transaction is complete.*

Often, brokers in the alternative remittance system are business partners who do legitimate business with each other on a regular basis. Because it can be difficult to transfer large amounts of money between countries, a debt might be paid with merchandise or a favor (e.g., Broker B owes Broker A money from a past transaction, and in a new transaction, pays the recipient, thereby relinquishing his debt to Broker A from the former transaction).

Alternative remittance systems are more than a thousand years old, tracing their origins to merchants wanting to avoid transferring currency through dangerous territory. Moreover, transferring funds in this manner is not necessarily illegal (although some jurisdictions require brokers to register with the government). If available, using such systems can be beneficial because the commission that the networked brokers take might be lower than a banking fee for international transactions. Additionally, the payers and payees do not need to have bank accounts to perform the transactions.

Typically, the network of parties in an alternative remittance system work on the basis of trust. There are often family connections between the parties. While there is little legal enforcement available to guarantee that the networked parties will live up to their agreements with the payers and payees, many people across the world rely on this system to send and receive funds. For instance, many migrant workers rely on some form of alternative remittance system to send funds to their families in their native countries.

Alternative Remittance Systems and Money Launderers

The relative anonymity and lack of a paper trail afforded by alternative remittance systems makes them attractive to money launderers, as well as to people involved in terrorist financing. For instance, a criminal who came upon illegal profits in the form of cash could transfer those funds out of the country through an alternative remittance system without the risk of a digital paper trail or arousing suspicion from a large, international currency transfer. Such transfers that are designed to hide assets might violate anti-money laundering regulations.

Alternative remittance systems are largely regional. Each system has unique features and goes by a certain name, including the following:

- Hawala (Middle East, North Africa, Horn of Africa)
- Hundi (Indian subcontinent)
- Fei chien (China)
- Poey kuan (Thailand)

EXAMPLE

In the case of United States v. Omian *et al.,*[1] *the defendants pleaded guilty to owning and managing an unlicensed hawala transmittance system. To avoid filing Currency Transaction Reports with the federal government (mandatory in the United States for currency transactions of $10,000 or more), the defendants structured the payments. Prosecutors found that the defendants caused $9.7 million in payments to be disbursed in Yemen to unknown recipients. The original senders included individuals, businesses, and mosques.*

An alternative remittance system is a tempting opportunity for launderers because it:

- Doesn't require formal identification
- Takes hours rather than days to transfer the money overseas
- Is cheaper than paying bank and shipping fees because brokers generally take a very small commission
- Does not require currency conversion
- Lacks a coherent paper trail

The very essence of alternative remittance systems bypasses regulation, such that money can be transferred without government and financial institution oversight. While many such networks are free of mal-intent, the system lends itself to abuse.

For brokers who operate storefront retail or service businesses in addition to their side exchanges, bank deposits rarely trigger investigation by a financial institution unless they are exceedingly high for the particular business. As always, such money can go undetected by putting it toward personal and business expenses.

[1] Grand jury indictment available at www.documentcloud.org/documents/229339-nasser-indictment.html.

Red flags of money laundering could also indicate an alternative remittance system scheme. The following transactions might indicate money laundering:

- Use of cash as payment for a transaction that is typically handled by checks or other forms of payment
- Lump-sum payments made by wire transfer or with foreign currency
- Reluctance to provide normal information when setting up a policy or account, or providing minimal information
- Purchase of investments in amounts considered beyond the customer's apparent means
- Use of a letter of credit or other methods of trade finance to move money between countries where such trade is inconsistent with a customer's usual pattern
- Establishment of a large investment policy and then, within a short time period, a customer requests cancellation of the policy and that the cash value be paid to a third party
- Use of wire transfers to move large amounts of money to or from a financial haven country such as the Cayman Islands, Colombia, Hong Kong, Liechtenstein, Luxembourg, Monaco, Panama, or Switzerland
- Services provided internationally but paid for locally
- Suspicious and seemingly related transactions involving a particular ethnic group or nationality

Combating Money Laundering in Alternative Remittance Systems

Alternative money movement systems have kept up with technology, which frustrates efforts to detect and prevent money laundering that uses these methods. Hawala systems based in Asia and the Black Market Peso Exchange based in Colombia have migrated to the use of instant messages, chat technology, and email to make discovery and tracing of communications even more difficult. The absence of a traditional paper trail has always been a challenge in working with these systems, but the advent of instant global communications has made them far more difficult to monitor.

The leading emerging threat in alternative remittance systems is identity theft. It has all but displaced the traditional fake identities used in fraud cases, especially money laundering. It is easier to assume the identity of a real person than it is to create a fake record that is as convincing. Considering that when a money launderer uses a stolen identity, it is not used to gain credit or exposed to loss, there is no reason for the identified person to ever learn that the accounts were opened using his name. Thus, the risk of discovery is low and the

opportunity for misdirection is high. In all, it's a near-perfect solution to the enhanced due diligence requirements being exercised by financial institutions.

Less savvy launderers, however, are still using straw men, both known and random, including family members, children, in-laws, and drifters, to play this role.

International Anti-Money Laundering Efforts

In the 1980s, the mounting global drug crisis led to the birth of international anti-money laundering (AML) efforts. As a result, international organizations began taking on initiatives to fight money laundering, while others were created for that same purpose. The principal organizations include the United Nations (UN), the Financial Action Task Force on Money Laundering (FATF), and the Egmont Group. Following the events of September 11, 2001, however, the international community's AML focus shifted from anti-drugs to anti-terrorism, and many international organizations revised the AML framework to not only examine funds from illegal sources, but to also examine funds whose purposes were illegitimate.

The United Nations

The United Nations (UN) has steadily increased its role in fighting money laundering over the past few decades, particularly in the areas of illegal drugs and human trafficking. The UN provides informational resources such as statistical studies, expert advice to policymakers, red flags, and risk factors of money laundering. The UN also sets policies for its members to adopt, such as its requirement that members criminalize money laundering. While these policies generally lack an effective enforcement mechanism, many members take measures to comply with them.

As the first international organization to undertake significant steps to combat money laundering with the 1988 Vienna Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the UN plays an important role in anti-money laundering efforts. The UN has a broad range of membership with 193 member states, and the UN operates the Global Program Against Money Laundering (GPML), which was established in 1997.

Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

In 1988, the UN adopted the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, a mandate to combat money laundering and organized crime. After the Convention was adopted, the UN established the Global Programme against Money Laundering (GPML), which provides member states with assistance to comply with international AML standards. In addition, the GPML, in participation with other international organizations, maintains the International Money Laundering Information Network (IMoLIN), a website that provides the international community with information and tools concerning AML.

Resolution 1373

The UN-adopted Resolution 1373 was created in September 2001 as a response to the 9/11 attacks in the United States. It called on countries to criminalize aiding terrorist groups, freeze funding to such groups, and cooperate with other countries to pursue them. It also marked an increased authority of international law. Historically, UN resolutions and requirements were voluntary; members might refuse to sign or enforce the resolution or rule. Resolution 1373, however, stated that all members shall pass its provisions, and a threat of sanctions looms for any country that does not comply.

Convention Against Transnational Organized Crime

The UN also created the Convention against Transnational Organized Crime, which requires members to:

- Criminalize participation in an organized criminal group, laundering of the proceeds of a crime, and corruption involving public officials.
- Regulate and supervise financial institutions and other industries vulnerable to facilitating laundering.
- Take measures to confiscate proceeds of crimes.
- Process requests of other members to enforce penalties for criminal offenses, confiscation, and so on; subject to approval.
- Afford member countries mutual legal assistance and law enforcement cooperation in transnational investigations.
- Train law enforcement personnel to prevent, detect, and control laundering and organized criminal offenses.

The Financial Action Task Force on Money Laundering (FATF)

The Financial Action Task Force (FATF) is an intergovernmental body that was established at the G-7 Summit in 1989. Its purpose is to develop and promote standards and policies to combat money laundering and terrorist financing at both the national and international levels. The FATF works in close cooperation with other international and regional bodies. Notably, the International Monetary Fund and the World Bank provide assistance in monitoring countries' progress in implementing and adhering to the standards set forth by the FATF.

Originally composed of 16 members, the FATF has expanded continuously and is presently made up of 36 members (34 countries and territories and 2 regional organizations). The current members of the FATF are: Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Cooperation Council, Hong Kong (China), Iceland, Ireland, India, Italy, Japan, Kingdom of the Netherlands, Luxembourg, Mexico, New Zealand, Norway, Portugal, Republic of Korea, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Almost every nation with active anti-money laundering enforcement operations is a member of the FATF.

The FATF releases various model policies and data to help countries combat money laundering, the most influential of which is its *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferations: the FATF Recommendations* (referred to as the *Recommendations*).

The FATF Recommendations

The FATF's *Recommendations*, revised in 2012, created the most comprehensive standard with which to measure a country's AML, counterterrorism, and nuclear proliferation laws and policies. They serve as a basic framework of laws that its members should have. While the recommendations are not required by members and the FATF acknowledges that following each rule might not be possible, members of the FATF often adopt them.

The FATF also evaluates each member's compliance with the recommendations in its Mutual Evaluations.[2] These periodic publications detail members' deficiencies and

[2] Available at www.fatf-gafi.org/topics/mutualevaluations.

recommend remedial measures. They are a good start to understanding a country's AML laws and procedures.

Some of the key measures in the recommendations provide that countries should:

- Use a risk-based approach when setting AML policy.
- Create policies that increase cooperation and coordination with other countries.
- Specifically criminalize money laundering and terrorist financing.
- Enable authorities to trace, freeze, and confiscate assets suspected in laundering and terrorist financing.
- Require financial institutions to:
  - Establish AML and counterterrorist financing programs.
  - Perform due diligence on customers.
  - Determine if customers are politically exposed persons.
  - Keep transactional records for at least five years.
  - Avoid correspondent banking with shell banks.
  - Continuously monitor wire transfers.
- Apply the above due diligence and recordkeeping requirements to designated nonfinancial businesses and persons, including:
  - Casinos
  - Real estate agents
  - Jewelry and precious metals dealers
  - Professionals who prepare business entities, buy real estate, and serve as a trustee
- Register money transmitters.
- Create financial intelligence units (FIUs) and require financial institutions and other high-risk industries to report suspicious activity to them.
- Ensure law enforcement has interdisciplinary personnel and the proper authority to investigate.
- Have detection methods for cash smugglers at borders and have a declaration system.
- Develop proportionate penalties for violations by individuals and entities.
- Cooperate to the fullest extent reasonably possible through legislative, judicial, and law enforcement efforts.

Revisions to the Recommendations

There were originally 40 FATF recommendations regarding money laundering. Shortly after the World Trade Center attack in 2001, the FATF mandate was expanded beyond money

laundering to support the worldwide effort to combat terrorist financing (CFT). During an extraordinary plenary meeting in Washington, DC, in October 2001, the FATF adopted

Eight Special Recommendations on Combating Terrorist Financing, which were revised in 2004 and expanded to the *Nine Special Recommendations.*

Money laundering techniques change in response to developing countermeasures. Launderers rely on increasingly sophisticated methods to achieve their objectives, including the assistance of professionals and the use of separate legal entities to mask ownership and control of funds. In light of this fact, the FATF made significant revisions to the *Recommendations* to help national AML/CFT systems. The most important provisions set minimum standards for legal systems, sound practices for financial institutions and related professions, and guidelines for international cooperation.

In 2012, the *Recommendations* were revised again, including a structural change that dropped the distinction between the original AML regulations and the special recommendations. The major changes included:

- A focus on a risk-based approach to combating money laundering and terrorist financing
- The inclusion of tax crimes as a predicate offense to money laundering violations
- Focused sanctions pursuant to the United Nations on parties that proliferate weapons
- A strengthened emphasis on anti-corruption measures, as corruption is often linked with money laundering

Provisions of the Recommendations

There are several provisions of the FATF's *Recommendations* that have helped to standardize the regulations and terminology in the international effort to stop money laundering.

LEGAL SYSTEMS

Under the *Recommendations,* countries should adopt legislation that effectively criminalizes acts of money laundering and establishes the widest possible range of predicate offenses. In reference to money laundering, a predicate offense is a crime whose proceeds must be converted into a legitimate form. At a minimum, every serious offense should constitute a predicate offense, regardless of where it is committed. In addition, countries should implement laws and regulations that permit authorities to confiscate laundered money, the proceeds of predicate offenses, or property of a corresponding value.

FINANCIAL INSTITUTIONS AND RELATED PROFESSIONS

The FATF revised the *Recommendations* over time to set stricter guidelines for financial institutions and professionals who are routinely involved in substantial financial transactions. Such professionals specifically include casinos, real estate agents, lawyers, and dealers in precious metals and precious stones. The measures address customer due diligence, reporting suspicious transactions, deterring money laundering and terrorist financing, and regulation and supervision.

ANTI-MONEY LAUNDERING PROGRAMS

Under the FATF's *Recommendations,* countries should require financial institutions to implement anti-money laundering and terrorist financing programs. A financial institution's anti-money laundering (AML) program is highly dependent on which jurisdictions it operates in, as well as the services that it offers. Generally, financial institutions should adopt the AML policies and procedures in the *Recommendations,* but they need to tailor their programs to the requirements of the specific jurisdictions in which they operate. According to the *Recommendations,* these programs should include:

- The development of internal procedures and controls, including adequate screening procedures to ensure high standards in employee hiring
- Ongoing employee training programs on money laundering risks
- An independent audit function to test the effectiveness of the programs
- The designation of a compliance officer at the management level

CUSTOMER DUE DILIGENCE

The *Recommendations* set out the fundamental measures that financial institutions must take to identify and verify the identity of customers and beneficial owners. Although it is most important to conduct due diligence when a business relationship is first established, due diligence should be exercised on an ongoing basis. These requirements set firm, more detailed standards while also providing flexibility and allowing adaptation to new industry practices. In addition to the fundamental obligations, the *Recommendations* also deal with other issues, such as the timing of verification, the measures to be taken with respect to existing customers and for legal persons or arrangements, and when simplified customer due diligence (CDD) measures may be appropriate.

According to the *Recommendations,* the CDD measures to be taken by financial institutions and designated nonfinancial businesses and professions are:

- Identifying the customer and verifying the customer's identity through reliable, independent source documents or data
- Identifying the beneficial owner of the account or service, including the ownership and control structure of organization
- Obtaining information and understanding the purpose and intended nature of the business relationships involved in the account or service
- Conducting ongoing due diligence on the business relationship and transactions of the customer to ensure that they are consistent with the customer's profile

Some countries allow their financial institutions to rely on persons other than employees and agents to perform some of the required CDD measures. The FATF recognizes this as a common commercial practice and permits countries to allow their institutions to rely on third parties, provided that the conditions laid out in the *Recommendations* are met. The ultimate responsibility remains with the financial institution that is relying on the third party.

Greater care must be exercised in CDD measures that involve politically exposed persons and their close relations. *Politically exposed persons* are individuals who hold prominent public positions in foreign countries, such as heads of state, senior politicians, high-ranking military officials, and members of the judiciary. Middle ranking or more junior members are not included in the definition.

DETERRING MONEY LAUNDERING AND TERRORIST FINANCING

Within certain limits, countries and institutions are free to determine the extent of measures appropriate to the specific risk of money laundering or terrorist financing they face. However, all countries are required to (1) establish a financial intelligence unit to receive suspicious transaction reports, (2) designate law enforcement agencies for AML/CFT investigations, and (3) involve financial supervisors in AML/CFT initiatives. These authorities should have appropriate duties and powers, the necessary resources, and effective mechanisms to cooperate and coordinate during investigations. To ensure that systems are effective and subject to review, comprehensive AML/CFT statistics must be maintained.

The FATF has consistently found that the lack of transparency concerning the ownership and control of legal persons and arrangements is a problem for money laundering investigations. The measures required under commercial or other laws regarding obtaining or accessing such information vary widely from country to country. The *Recommendations,*

therefore, set out the key objective of ensuring that adequate, accurate, and timely information on the beneficial ownership and control of legal persons and arrangements is obtainable or accessible. In particular, countries must be able to show that companies issuing bearer shares cannot be misused for money laundering. Bearer shares are share certificates that can be issued without the name of the beneficial owner.

The *Recommendations* dissuade countries from allowing the establishment of shell banks within their jurisdiction or engaging in transactions with such financial institutions. A shell bank is a bank that is incorporated in a jurisdiction in which it has no physical presence and that is unaffiliated with a regulated financial group.

REPORTING OF SUSPICIOUS TRANSACTIONS

Under FATF Recommendation 20, a financial institution should be required to file a report when it "suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing." Some jurisdictions also set additional requirements for reporting suspicious transactions, such as if a cash transaction surpasses a certain threshold. The *Recommendations* define *financial institutions* to include:

- Depository and lending institutions (i.e., traditional banks)
- Money services businesses
- Financial guarantors
- Securities brokers or traders, including those who trade in:
  - Money market instruments
  - Foreign exchanges
  - Exchange, interest rate, and index instruments
  - Transferable securities
  - Commodity futures
- Security issuing services
- Investment portfolio managers
- Parties that invest, administer, or manage funds or assets on behalf of others
- Insurance companies servicing life insurance and other investment-related insurance

Also, the parties that should file suspicious transaction reports have broadened to include designated nonfinancial businesses and professions (DNFBPs), including:

- Casinos (including Internet- and ship-based casinos)
- Real estate agents

- Dealers in precious metals and stones
- Legal professionals at professional firms (not internal legal professionals)
- Trust and company service providers

REGULATION AND SUPERVISION

All countries need adequate measures to ensure that financial institutions and other businesses and professions are complying with their obligations. The required measures take into account the risks and the regulatory structures that already exist in the relevant sectors. The required measures are:

- Financial institutions and casinos should not be owned or managed by criminals.
- The measures applicable to banks, insurance, and securities firms for prudential purposes also apply when combating money laundering.
- Currency exchange and money remittance businesses must, at a minimum, be licensed or registered and monitored for compliance.
- Other financial institutions should be regulated and subject to supervision or oversight to detect the risk of money laundering or terrorist financing.
- Casinos must be licensed and supervised.
- On a risk sensitive basis, other businesses and professions must have effective systems for monitoring and ensuring compliance, which could either be by a government authority or by a self-regulatory organization.
- Competent authorities must establish guidelines and provide feedback.

LARGE CASH TRANSACTIONS

Under the best practices provided in the FATF's *Recommendations,* countries should implement a reporting requirement for financial institutions and designated nonfinancial businesses and professions (DNFBPs) that engage in cash transactions above the jurisdiction's designated threshold. The reports should cover domestic and international cash transactions. Many jurisdictions implement this reporting requirement.

CROSS-BORDER TRANSFER OF CURRENCY

Under the Financial Action Task Force's Recommendation 32, countries should implement disclosure requirements for individuals who are physically carrying currency or currency equivalents (i.e., bearer instruments) in or out of the country in amounts above the designated threshold. Generally, individuals who are carrying currency or the equivalent above the jurisdiction's designated threshold while attempting to cross jurisdictional borders

should be required to disclose the amount to authorities, and face penalties if they fail to do so.

INTERNATIONAL COOPERATION

The *Recommendations* contain several provisions that address international cooperation. Notably, the Recommendation on mutual legal assistance covers several concepts that are in the 25 Non-Cooperative Countries and Territories Criteria discussed below. The most significant provisions deal with cooperation between administrative and law enforcement authorities concerned with combating money laundering and terrorist financing. This prescribes the need for the widest possible cooperation, and for clear and effective gateways.

Countries with Substantial Money Laundering Issues

The FATF maintains a list of countries that have detrimental rules and practices which obstruct international efforts to curtail money laundering. Furthermore, the FATF urges its members to protect the international financial system from money laundering and terrorist financing by applying counter-measures when dealing with these countries. In compiling this list, the FATF looks at factors such as a country's:

- Financial regulations
- Requirements for registration of business entities and identification of the owners of those entities
- Laws regarding the international exchange of information in money laundering investigations
- Strength of anti-money laundering laws
- Allocation of sufficient resources to prevent and detect money laundering activity

As of this publication, the most recent FATF report found that the following jurisdictions to have substantial money laundering and terrorist financing risks:

- Iran
- North Korea

Additionally, the report found that the following jurisdictions had not made sufficient progress in addressing the deficiencies (as identified by the FATF) in their anti-money laundering efforts:

- Algeria
- Myanmar

International Monetary Fund/World Bank

Created to revive international trade in the post-World War II era, the International Monetary Fund (IMF) and the World Bank were designed to enhance international commerce by creating a system supported by global monetary cooperation. Today, the IMF and the World Bank actively participate in global anti-money laundering efforts through financial sector assessments, technical assistance in the financial sector, and policy development.

The Egmont Group

The Egmont Group is an informal international network of financial intelligence units (FIUs), which are national centers that collect information on suspicious or unusual financial activity, designed to fight money laundering by encouraging global cooperation and mutual exchange of information. The Egmont Group exists to increase the sharing of information and coordination between FIUs, and it offers training for FIU personnel.

European Union

The European Commission enforces several European Union (EU) policies that involve anti-money laundering efforts. The most prevalent is the Third Anti-Money Laundering Directive (Third Directive). The Third Directive applies to the financial sector as well as to lawyers, notaries, accountants, real estate agents, casinos, and company service providers. Its scope also encompasses all providers of goods when cash payments are made or received in excess of €15,000. Those subject to the Third Directive are required to:

- Verify the identities of their customers and of their beneficial owners, and to monitor the transactions and business relationships of the customers.
- Report suspicions of money laundering or terrorist financing to the jurisdiction's financial intelligence unit or other proper authorities.
- Ensure proper training of personnel and establish appropriate internal controls.

On June 26, 2015, the EU's Fourth Anti-Money Laundering Directive (Fourth Directive) took effect. The Fourth Directive replaces the Third Directive. However, EU countries have until June 26, 2017, to implement the Fourth Directive.

While the Third Directive applies to all providers of goods who make or receive cash payments in excess of €15,000, the Fourth Directive lowers this threshold to €10,000. The Fourth Directive further expands its scope to cover providers of gambling services. Among

other changes, the Fourth Directive increases sanctions for noncompliance, contains new risk assessment requirements, expands customer due diligence requirements, and mandates enhanced due diligence for politically exposed persons (PEPs).

Other AML measures enforced by the European Commission include:

- Directive 2006/70 requires measures to guard against corruption involving PEPs and simplified customer due diligence procedures. This Directive will be repealed when the Fourth Directive takes full effect on June 26, 2017. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:214:0029:0034:EN:PDF)
- Regulation 2015/847 requires information on the payer to accompany transfers of funds for the purposes of the preventing, investigating, and detecting of money laundering. On June 26, 2015, this regulation replaced Regulation 1781/2006, the former wire transfer regulation.(http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R0847&from=EN)
- Regulation 1889/2005 requires persons entering or leaving the EU to declare currency sums of €10,000 or more. (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0009:0012:EN:PDF)
- EU Council Decision 2000/642 lays out arrangements for cooperation among EU members' financial intelligence units. (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:271:0004:0006:EN:PDF)

Enforcement and Prevention Strategies

Financial institutions, brokers, and insurance companies should be aware and should make their employees aware of situations that could indicate money laundering activity.

AML Compliance Programs

Most financial institutions are now required to have an anti-money laundering (AML) compliance program in place. However, every business that has the potential for transactions dealing with significant amounts of cash should institute a compliance program and a money laundering awareness program. All employees should be made aware of the money laundering laws and the serious implications of such laws on the institution and the employees. Employees should be educated to be aware of transactions that might suggest

possible laundering activity. Procedures should be implemented detailing what an employee should do if a customer or transaction appears suspicious.

Minimum Standards

At a minimum, a written AML compliance program should:

- Establish a system of internal policies, procedures, and controls to ensure ongoing compliance with the regulatory AML regime.
- Provide for independent testing of compliance by internal auditors and/or outside examiners.
- Designate a compliance officer(s) to ensure day-to-day compliance with AML laws and regulations.
- Provide training on an ongoing basis for all personnel.

Compliance Officer

A business should select a person or team responsible for the day-to-day monitoring of the compliance program. The compliance officer should be given broad authority to monitor all aspects of the institution's compliance, including the development and refinement of the program and the monitoring of employee training programs. Such an individual should also have the authority to conduct regular and ad hoc audits to ensure that the program is functioning effectively, and to hire outside consultants as necessary to investigate problems.

Policy Statement

All entities that have a potential for dealing with significant amounts of cash should have a written policy against handling the proceeds of drug trafficking or other criminal activity. The policy should provide that the institution requires its employees to operate with the highest moral and ethical principles. It should include a statement that the company refuses to do business with criminals and money launderers; a commitment to conduct business only with legitimate business organizations; a statement against doing business with organizations that refuse to provide proper documentation of their identity and purpose; clear directions for referring all suspicious transactions to the appropriate department; and a commitment to comply with the spirit and specific provisions of AML law.

Know-Your-Customer Programs

Financial institutions should implement know-your-customer (KYC) programs. Generally, there are two components to an effective KYC program. First, a financial institution should

identify and conduct background checks on all customers opening an account to prevent the creation of fictitious accounts. Second, financial institutions should monitor existing customers' activity to recognize when customers might be involved in suspicious activity.

More specifically, such programs should provide for effective customer identification, account monitoring, and appropriate action in suspicious circumstances.

To provide for effective customer identification, financial institutions and professionals should implement the following procedures:

- Identify the customer and verify the customer's identity through reliable, independent source documents or data.
- Identify the beneficial owner of the account or service, including the ownership and control structure of organizations.
- Obtain information and understand the purpose and intended nature of the business relationships involved in the account or service.
- Conduct ongoing due diligence on the customer's business relationship and transactions to ensure that they are consistent with the customer's profile.

Additionally, the following are particular areas of concern for KYC programs.

NEW DEPOSIT ACCOUNTS

For individual deposit accounts, minimum identification standards should be established. The information to be obtained should include:

- Name
- Address
- Date of birth
- Government-issued identification number
- Current employer
- Business and residence telephone numbers

The customer should be required to submit some form of identification that includes a photo, such as a driver's license or passport, and a copy should be made and kept in the customer's file. If there are any doubts or inconsistencies about the information provided, the employee should be instructed to notify the appropriate department.

Minimum standards for new business accounts should include:

- Business name and address
- Telephone number
- Taxpayer identification number
- Documents establishing the formation of the business entity (articles of incorporation, partnership agreement, etc.)
- Copies of all assumed name filings or doing business as (DBAs) filings
- A full description of the operations of the business
- Credit and banking references
- The identity of the officers, directors, or other principals

The account representative should also consider making a personal visit to the customer's place of business. Besides promoting good customer relations, a personal visit will help identify whether the business is legitimate or simply a front. The representative can also use this opportunity to get to know the principals of the business.

NEW LOAN ACCOUNTS

An institution should perform due diligence in establishing a new loan account because, if the customer is engaged in money laundering, there is a risk of forfeiture of collateral pledged on the loans. Real or personal property that is traceable to drug sales or that is purchased with laundered funds is subject to seizure by the government. If the property seized is pledged as collateral, the financial institution must prove that it was an innocent lienholder of the property and had no knowledge of the illegal activity.

Minimum standards regarding the information to be gathered should include:

- Reliable identifying information similar to that required for new deposit accounts
- Reliable financial information such as financial statements and copies of tax returns
- The purpose of the loan
- Credit history and prior banking references
- Verifiable, legitimate means of repayment
- Assurance that the loan amount is consistent with the purpose of the loan and the nature of the business

SERVICES FOR NON-ACCOUNT HOLDERS

Banks often issue cashier's checks, money orders, and traveler's checks and perform currency exchanges, wire transfers, or check cashing services for non-account holders. Strict identification requirements should be established for transactions with persons who are not regular bank customers. In fact, regulations require that in some instances, banks keep a record of the identity of persons who are not established customers. Such regulations usually require at a minimum the person's name and address, official photo identification, and government or employer identification number.

MONITORING ACCOUNTS

While identification of customers is important, it is equally important to monitor the activity of accounts. The institution should identify unusual transactions that might not be consistent with the normal business of the customer. Unusual and dramatic changes in wire transfer, monetary instrument, and check transactions are important to identify. If unusual transactions or activities are noted, the institution should take some action to protect itself. The appropriate action in some cases might be to discuss the changes with the customer to find out the reasons for said inconsistencies. Increased transactions might be the result of an increase in sales or the result of a promotional activity. However, if the discussion leads to a reasonable suspicion that the transactions are illegitimate, the institution might be required to notify the appropriate government agency.

Special Problems for Insurance Companies

Although financial institutions such as banks are primarily associated with money laundering activities, insurance companies have become major targets of money laundering operations because of the variety of services and investment vehicles they offer that can be used to conceal the source of funds.

The most common form of money laundering that insurance companies face involves single premium contracts or policies. Examples include purchases of annuities, lump sum top-ups to an existing life insurance contract, and lump sum contributions to personal pension contracts.

Insurance companies, like other financial institutions, should educate their employees to look out for transactions that appear to be inconsistent with a customer's known legitimate

business or personal activities, or the normal transactions for that type of account. To that end, insurance companies should institute Know-Your-Customer programs.

Red Flags

The following transactions might indicate money laundering is taking place. The list should be used to identify those transactions and customers that might require further investigation.

- Large purchase of a lump sum contract when the customer typically purchases small, regular payment contracts
- Use of a third-party check to make a purchase or investment
- Lack of concern for the performance of an investment, but great concern for the early cancellation of the contract
- Use of cash as payment for a transaction that is typically handled with checks or other forms of payment
- Lump sum payments made by wire transfer or with foreign currency
- Reluctance to provide normal information when setting up a policy or account, or providing minimal information
- Purchase of investments in amounts considered beyond the customer's apparent means
- Use of a letter of credit or other methods of trade finance to move money between countries where such trade is inconsistent with the customer's usual pattern
- Establishment of a large investment policy, and within a short time period, the customer requests cancellation of the policy and cash value paid to a third party
- Use of wire transfers to move large amounts of money to or from a financial haven country, such as the Cayman Islands, Colombia, Hong Kong, Liechtenstein, Luxembourg, Monaco, Panama, or Switzerland
- Request to borrow the maximum cash value of a single premium policy soon after paying for the policy

Detection

Most insurance companies must file reports of suspicious activity and comply with the requirements imposed by anti-money laundering (AML) legislation, including the implementation of an AML compliance program.

Accordingly, insurance companies should implement mechanisms to detect suspicious activity. *Incoming and outgoing wire transfer logs* can help companies identify possible patterns suggestive of money laundering. *Account activity reports* generally show weekly and/or monthly

balances, deposits, and withdrawals. Review of these statements can identify those accounts with large increases in average balances and numbers of transactions. *Policy cancellation reports* should identify policies canceled within a specific time period. Report details should include the amount of the cash surrender value, the identity of the sales agent, and the actual term of the policy.

The "Tracing Illicit Transactions" chapter in the Investigation section of the *Fraud Examiners Manual* provides more information about techniques for detecting illicit income and payments. Included in that chapter are details on analyzing financial records, financial and behavioral profiles, and net-worth analysis.

TAX FRAUD

Introduction

Tax fraud refers to intentional actions that a taxpayer commits to defraud the government of owed tax dollars. It is a type of fraud committed against the government, typically involving false claims or concealed information.

Most governments have laws prohibiting tax fraud, but these laws differ in substantive ways from country to country. Examining the tax fraud laws in every country is beyond the scope of this material, so fraud examiners dealing with tax fraud should consult with local legal counsel for guidance.

Tax Evasion

Tax evasion is a subset of tax fraud; typically, tax evasion is used in the criminal context. *Tax evasion* refers to any fraudulent actions that a taxpayer commits to avoid reporting or paying his taxes. To qualify as tax evasion, most jurisdictions require a willful attempt to evade or defeat the tax in an unlawful manner.

Tax evasion, however, should not be confused with tax avoidance. *Tax avoidance* refers to a legal means of lowering one's tax bill through legitimate deductions, credits, and shelters. The intent of the taxpayer to wrongly file a tax return or provide other false tax information will determine the difference between tax evasion and tax avoidance.

The primary distinguishing characteristic of tax evasion as compared to tax avoidance is that tax evasion is illegal, but tax avoidance is legal.

Intent

The most important distinction in determining whether an individual or company has committed tax evasion is whether the party acted with criminal intent. *Intent* is a mental attitude with which an individual acts. To establish criminal liability for tax evasion, most jurisdictions require a willful attempt to evade or defeat taxes in an unlawful manner.

For the purpose of tax law, a good faith or legitimate misunderstanding of the law based on the law's complexity typically negates willfulness (the voluntary, intentional violation of a known legal duty). That is, honest mistakes, in contrast to willful evasion, do not constitute

tax evasion. However, courts might find that a person's misunderstanding of the law was unreasonable and still find willfulness. Willfulness can be inferred from conduct, such as:

- Keeping a double set of books (not to be confused with keeping separate books and tax records, which might require different recording techniques)
- Making false entries or alterations or creating false invoices or documents
- Destroying books or records
- Concealing assets
- Covering up sources of income
- Avoiding making records that are typical in transactions of the kind
- Engaging in conduct designed to mislead or conceal

Also, keep in mind that the presence of willfulness is important for determining criminal liability for tax fraud, but violations of proper tax procedures can still result in fees and interest penalties. Honest mistakes and misinterpretations of the law will usually not prevent such fines.

International Tax Avoidance and Evasion

Tax evasion often transcends national boundaries due to the investigative and jurisdictional limits of a country's revenue authorities. Often, tax evasion is accomplished through tax shelters, tax havens, and secrecy jurisdictions. *Tax shelters* are investments that are designed to yield a tax benefit to the investor. Such investments are made to produce tax write-offs, generate deductions, or convert ordinary income into capital gains taxed at a lower rate. Tax shelters might be legal or illegal; they are generally aimed at avoidance, although they might, on occasion, cross the line into evasion if they take abusive forms. An illegal, abusive shelter is one that involves artificial transactions with little or no economic reality. For example, abusive tax shelters might artificially inflate the value of donations to charity; falsely identify an asset for business use that is mainly intended for pleasure; claim excess depreciation or depletion; or engage in the cross-leasing of luxury items such as automobiles, boats, vacation homes, and aircrafts.

In contrast, *tax havens* are countries that offer favorable tax treatment to investments. Tax havens might be legal or illegal, depending on the nationality and the residence of the individual and the tax code of the country where the activity takes place.

Often, individuals try to skirt their tax responsibilities by hiding their assets abroad in secrecy jurisdictions. A *secrecy jurisdiction* is a country that has enacted laws that afford financial

secrecy. Such jurisdictions may provide financial secrecy through domestic bank secrecy laws that bar insight by outsiders or through blocking statutes that prevent the disclosure, copying, inspection, or removal of documents located in the host country. Moreover, in some secrecy jurisdictions, legal depositions may not be taken on national territory in connection with judicial proceedings being undertaken abroad. Secrecy jurisdictions are often relatively small countries whose customers are largely foreign persons.

Evidence of Tax Fraud

Evidence of tax fraud may be direct or circumstantial. *Direct evidence* includes testimony that tends to prove or disprove a fact in issue directly, such as eyewitness testimony or a confession. *Circumstantial evidence* is evidence that tends to prove or disprove facts in issue indirectly, by inference.

Direct Evidence

Certain circumstances constitute direct evidence of tax fraud, including:

- Unexplained bank deposits (e.g., using bank accounts in another person's name or a fictitious name)
- Submission of false documents (e.g., if a taxpayer claims medical deductions but cannot provide any evidence that he had seen or paid the bills)
- False explanations for prior conduct (e.g., the taxpayer destroyed his company's cash register tapes, which were the only records for the company's sales)
- Participation in an illegal business (e.g., over several years, a taxpayer who ran an illegal lottery substantially underreported his income)
- False claims of extra withholding exemptions (e.g., a taxpayer claimed fifty withholding exemptions, but could not substantiate that he was entitled to claim them)

Circumstantial Evidence

Certain circumstances constitute circumstantial evidence of tax fraud, including:

- Illicit income, which can be proved by showing that the subject's assets or expenditures for a given period exceed that which can be accounted for from admitted sources of income
- Income in excess of deposits (e.g., audits of service industry people in Texas led to assessments of several thousand dollars in back taxes and penalties)

Types of Tax Evasion Schemes

There are many different types of tax evasion schemes, and they will vary depending on what kinds of taxes exist in the jurisdiction. Some common types of tax evasion schemes include:

- Income and wealth tax evasion
- Falsifying tax deductions
- Tax credit schemes
- Consumption tax schemes

Income and Wealth Tax Evasion

Taxes on periodic income or wealth (e.g., real property taxes) are a source of revenue for many governments, but fraudsters often commit tax evasion by falsifying or omitting material information. Common forms of criminal income and wealth tax evasion include:

- Failing to submit a report of one's taxable income, if such a report is required
- Intentionally misrepresenting one's income or wealth
- Pretending to transfer assets to another person or entity to lower tax liability
- Intentionally failing to withhold the taxable portion of an employee's income, if so required
- Failing to report foreign bank accounts or other taxable assets, if required
- Falsely claiming income was earned in another jurisdiction to lower tax liability

Falsifying Tax Deductions

In the context of income and wealth taxes, *tax deductions* are itemized expenses subtracted from gross income or assets to reduce the taxpayer's total liability. For instance, a company that is taxed by a percentage of its gross sales might be allowed to deduct the cost of making the goods (materials, employee costs, etc.). Deductions are designed to make certain taxes fairer, but they also might be used inappropriately by tax evaders. Examples of the fraudulent use of deductions include:

- Falsifying expenses, such as recording fictitious salaries to nonexistent employees
- Fraudulently inflating expenses, such as bribing a supplier to inflate an invoice
- Submitting false information to qualify for improper deductions, such as pretending to qualify for a tax deduction for having children living at home
- Misclassifying nondeductible expenses as deductible

Tax Credit Schemes

Similar to deductions, *tax credits* are an amount subtracted from a person's or entity's tax liability, but are not necessarily tied to an expense. Additionally, some tax credits might result

in a tax refund if the credits are greater than the person's total tax liability. For instance, a government might give tax credits to individuals with low income to reduce their tax liability. Tax credits are often used to encourage certain behavior, such as taxing carbon emissions by industrial companies. Taxpayers might attempt to evade taxes by misrepresenting their eligibility for a tax credit (e.g., an energy company underreporting its carbon emissions).

Consumption Tax Schemes

Consumption taxes are those collected from the proceeds of the sale of goods or services. Some of the common taxes include:

- *Sales tax*: a tax on goods or services, usually assessed at the consumer level and collected by the retailer or seller at the point of sale
- *Value-added tax* (VAT): a system that imposes a tax on a single item at each point of sale along the item's path from manufacture, to wholesale, to retailer, to consumer; the tax is collected by the seller in the transaction and only the difference between the price paid by the initial purchaser and the price paid by the subsequent purchaser is taxed
- *Excise tax*: a tax on a narrow class of goods or services (e.g., tobacco or gasoline), usually assessed one time (per jurisdiction) at the manufacturer or wholesaler level

As with any form of tax, there are common schemes by which fraudsters attempt to evade consumption taxes, including:

- Omitting transactions from tax records to evade consumption taxes
- Deflating the value of transactions in tax records (e.g., recording the portion of a transaction paid with a credit card, but not recording cash received for the same transaction)
- Disguising a transaction that should be subject to a domestic consumption tax as a tax-free foreign transaction
- *Missing trader schemes*, in which the culprit collects a value-added tax from a large transaction but, rather than paying the tax to the government, disappears with the proceeds
- Applying for a refund of a value-added tax that the subject or a co-conspirator in the transaction chain never paid to the government (called a *carousel scheme*, because the goods are often transferred among the co-conspirators several times)
- Smuggling goods into a jurisdiction to avoid paying excise taxes

Common Defenses to Allegations of Tax Fraud

A suspect or a criminal defendant might raise various defenses to accusations of tax fraud. Whether these defenses are legitimate depends on the laws of the jurisdiction.

The following are common defenses to tax fraud.

No Deficiency

The defendant can establish that there is no deficiency. If there is no deficiency, there is no tax liability. This is generally the best defense, if available, because several other defenses might negate willfulness, but do not necessarily eliminate a tax liability with interest and penalties.

Lack of Willfulness

A lack of willfulness reduces the defendant's culpability for fraud. Again, a good faith belief that one is not violating the tax law, based on a misunderstanding caused by the law's complexity, negates willfulness. The rule applies even if the defendant's interpretation of the law is irrational or unreasonable. Whether the defendant actually has such a belief is an issue for the jury or fact finder to decide.

Avoidance, Not Evasion

A taxpayer charged with tax crimes might argue that he engaged in legal means of lowering his tax bill through legitimate avoidance mechanisms, such as deductions, credits, and shelters. Thus, establishing that the taxpayer was engaging in tax avoidance and not evasion provides a defense to tax fraud.

Objectively Reasonable Position

A defendant might also claim that he took an "objectively reasonable" position with respect to his tax obligations.

Claim of Right Doctrine

In the United States, a taxpayer must recognize income if he receives the income, even if he does not have a fixed right to the income. For instance, a person could be given cash under a contract with the contingency that the cash will be taken back if the person fails to perform some task. Even so, as long as the taxpayer has control of the cash and can spend it, the contingency would not stop the requirement to recognize the income.

Thus, a taxpayer may seek to avoid a tax by claiming that he does not have an unrestricted right to the money at issue (or evade the tax by claiming that his rights are restricted when in fact they are not).

Mental Illness

Certain mental illnesses and incapacitating conditions negate criminal intent for tax crimes. This defense is applicable in regard to the time the return was prepared.

Reliance on an Attorney or Accountant

If a taxpayer properly relied on expert advice for the conduct in question, the jurisdiction might find no criminal liability. But generally, for this type of defense to succeed, the defendant must establish all of the following conditions:

- The taxpayer specifically relied on the advice from an expert.
- The expert is qualified, which is determined by a facts and circumstances test.
- The taxpayer gave full disclosure of the facts to the expert.

Ignorance of the Law

Generally, ignorance of the law is not a defense to criminal charges, but in some jurisdictions, this defense might succeed against allegations of tax fraud if the defendant can show that he had a good faith misunderstanding of the tax requirements.

Innocent Spouse

Innocent spouse relief permits a spouse to avoid tax liability in certain circumstances. Under this doctrine, a spouse may be excused from tax liability for tax or tax penalties if a joint tax return was filed and the spouse can establish the following elements:

- The underpayment of tax is due to unreported income or disallowed deductions that are attributable to the other spouse.
- The spouse "did not know and did not have reason to know" of the facts surrounding the underpayment of tax.

Additionally, innocent spouses may obtain relief for "erroneous" income items.

Statute of Limitations

A defendant can assert the statute of limitations as a defense to a tax fraud claim. Statutes of limitations set the maximum time after an event when legal proceedings may be initiated, but

the statute of limitations differs for civil and criminal claims related to tax fraud. In some jurisdictions, there is no statute of limitations for tax fraud.

Ineffective Defenses

Generally, some defenses will be ineffective against charges for tax crimes. For example, the death of the taxpayer cannot be used as a defense because taxes owed as a result of tax evasion typically survive the taxpayer's death, meaning the deceased taxpayer's estate will still be liable. Also, liabilities owed as a result of tax evasion may not be discharged in bankruptcy proceedings. If a person commits a tax fraud offense, amending fraudulent information held by the government will not generally relieve the taxpayer of criminal liability.

INDIVIDUAL RIGHTS DURING EXAMINATIONS

Because many fraud examinations might lead to legal action, fraud examiners should be familiar with the basic rights and freedoms of those involved in investigations, especially of those suspected of fraud. Being knowledgeable about individuals' basic rights and freedoms is particularly important for fraud examiners conducting investigations that could result in criminal action. The gathering of evidence, for instance, in violation of the law may result in the expulsion of that evidence later at a criminal trial. Accordingly, if the fraud examiner has any reason to believe that his investigation might ultimately result in legal action being taken against the subject of an examination, it is best to conduct the investigation in accordance with the rights guaranteed under the applicable laws.

Also, employees involved in investigations of suspected fraud may have certain rights and obligations, and fraud examiners should be aware of any such matters.

This chapter presents some general concepts of individual rights that are common in many countries, particularly those operating under the common law and civil law systems, but it first examines employees' duties and rights during investigations.

Employees' Duties and Rights During Investigations

Again, employees involved in investigations of suspected fraud have certain duties and rights, whether they are merely bystanders who could have some information relevant to the investigation or are suspected of committing fraud.

Employee duties and rights, however, vary among jurisdictions and from case to case, but generally, such duties and rights apply to employees who work in government and private-sector workplaces. Thus, private and government employers can violate their employees' legal rights.

Employees' Duty to Cooperate

In most jurisdictions, a duty to cooperate exists in every employer/employee relationship, but such duties vary. In the United States, for example, some states have statutes defining the scope of this duty; in others, the duty is found to be implied from the basic nature of the employment relationship.

Generally, the duty to cooperate extends to workplace investigations; therefore, employees have a duty to cooperate during an internal investigation as long as what is requested from them is reasonable.

What is reasonable is determined by the facts and circumstances of the particular case and by the duties for which the employee was hired. For example, if inventory items were missing, it would probably be reasonable to request that a warehouse supervisor review inventory records because this falls within the scope of his work duties. But under such facts, it might not be reasonable to ask the same supervisor to review detailed tapes from the company's cash registers, and it almost certainly would not be reasonable to ask the warehouse supervisor to let company investigators search his personal residence.

The issue of whether an employee has a duty to cooperate often comes up when investigators seek to interview employees about suspected workplace misconduct. In general, interviews should be considered reasonable if they address matters within the scope of the employees' actions or duties.

Duty to Preserve Information Relevant to Litigation

Employees may have a duty to preserve relevant information. Common law jurisdictions, in which litigants are usually obligated to disclose relevant information to the opposing side, impose a duty on litigants to take affirmative steps to preserve relevant evidence, and this duty might arise prior to the commencement of litigation. For litigation occurring in common law courts, the duty to preserve relevant evidence typically arises when litigation is reasonably anticipated or contemplated. When an organization is involved in litigation, this duty to preserve applies to the organization's management, and it extends to employees likely to have relevant information. A violation of the duty to preserve occurs when information that is relevant to anticipated or existing litigation is lost, destroyed, or otherwise made unavailable.

But in civil law systems, in which the primary responsibility of discovering evidence is placed on the presiding judge, there are no specific rules requiring litigants to preserve information for discovery because there is no common-law-style discovery in civil law systems. Consequently, civil law systems tend to have a more narrow scope of what evidence is required for litigation, and the issue of when to take affirmative steps to preserve evidence is established by the court. Nonetheless, destruction of evidence is not permitted because parties must refrain from such procedural abuses.

Violating the duty to preserve relevant information can result in several adverse sanctions for the offending party, and such sanctions can arise from both intentional acts and accidental acts through negligence. The adverse consequences can include, but are not limited to, monetary penalties (e.g., paying the opposing party's legal fees and costs), the drawing of adverse inferences of fact, and criminal penalties. The theory behind such consequences is that the individual who makes evidence unavailable following the probable initiation of a lawsuit is aware of its detrimental effect upon a case.

Examples of situations that could give rise to sanctions for failing to preserve evidence include intentionally or accidentally:

- Erasing computer files (e.g., documents, images, databases, etc.) relevant to anticipated or existing litigation
- Losing or destroying physical evidence relevant to anticipated or existing litigation
- Losing, destroying, or altering documents or records relevant to anticipated or existing litigation
- Failing to suspend routine destruction of electronic data relevant to anticipated or existing litigation

Employees' Contractual Rights

Employees may have contractual rights that are enforceable against their employers. Employers and employees may enter into contracts that govern the employment relationship, and if the employer violates the contract, the employee can sue for breach of contract. Such contractual rights can affect the employer-employee relationship and, in particular, they can limit the ability of the employer to compel full cooperation in a fraud examination.

Often, employee contractual rights at issue during investigations stem from a union contract, a collective bargaining agreement, or an employment contract. For example, if the employee is a member of a union, the union contract or collective bargaining agreement might contain certain clauses that restrict the employer's investigatory procedures.

Additionally, employees might have a written employment agreement containing provisions concerning the employees' rights during an investigation. Generally, such contracts can be express or implied. Just because the employer does not have a written, signed, and formalized contract with an employee does not mean that there is no agreement in place.

Many courts have held that company policies, employee manuals, and past practices can create "implied" contractual relationships between the employer and the employee.

Whistleblower Protections

Many jurisdictions have whistleblower laws designed to encourage individuals to bring forth complaints of wrongdoing by providing protections for those who report unlawful conduct. These laws shield employees who report their employers for misconduct by protecting them from any adverse employment action or retaliatory action from their employers.

Whistleblower laws do not, however, prevent individuals from being fired for engaging in unrelated fraudulent behavior.

More than 12 countries have comprehensive whistleblower protection laws, and more than 50 countries have adopted more limited protections for whistleblowers. In the United States, for example, there are numerous federal laws protecting whistleblowers from retaliation or illegal treatment and every state has some form of anti-retaliation legislation protecting whistleblowers.

Similarly, in the United Kingdom, the Public Interest Disclosure Act 1998 (PIDA) protects employees against being subjected to any retaliatory action on the ground that they made a protected disclosure—instances concerning criminal offenses, miscarriages of justice, environmental damage, etc.—about their employer or coworker.

Therefore, employers should not conduct investigations as a means to retaliate against employees, and they must be careful to conduct investigations in a way that avoids the appearance of retaliation. Likewise, management should consult counsel before discharging or taking action against any individuals to determine the applicability of any whistleblower protections.

Employees' Privacy Rights and Workplace Searches

Employees may have certain privacy rights that can affect numerous aspects of the employer-employee relationship, such as conducting investigations, surveillance and monitoring, searches, and polygraph testing. An employee's privacy rights may stem from, and be protected by, various sources of law, including constitutional law, human rights law, statutory law, common law, labor law, contract law, and other sources. Different countries approach the issue of employee privacy differently.

Surveillance of Employees

An employer, in certain circumstances, can use monitoring and surveillance methods to uncover employee wrongdoing. Employers have an interest in promoting workplace efficiency and protecting themselves from liability, and surveillance can be used to achieve such ends. But because employees have privacy rights in the workplace, an employer's surveillance practices may infringe on such rights.

Various national or local laws govern the availability and methods of such techniques.

Additionally, because various laws govern monitoring and surveillance practices, these laws are complex and their principles can be interpreted differently in different jurisdictions. Accordingly, legal counsel should always be consulted before engaging in any such practices. To complicate things further, the privacy laws might vary depending on the type of surveillance.

Although an employer might use surveillance techniques to investigate its workplace for wrongdoing, its employees may have privacy rights that protect them from such activities. In general, employees are afforded privacy protection in areas where they have reasonable expectations of privacy.

Reasonable Expectations of Privacy

Employers generally can investigate their workplaces by means of workplace searches and area surveillance, but employees may have privacy rights that protect them from certain forms of searches and surveillance. In general, privacy laws prohibit unreasonable searches and surveillance in areas where employees have reasonable expectations of privacy.

There are no easy rules for determining whether an employee has a reasonable privacy expectation in a particular area. Some areas in question might include a desk drawer, a file cabinet, a locker, or even an entire office, depending on the circumstances.

The key issue to consider when assessing the existence of a reasonable expectation of privacy is whether a reasonable person would expect the area or item to be free from intrusion. The employee does not have to have an ownership interest in, or legal custody over, the area or item to have a reasonable expectation of privacy in it. Thus, even though an

employer might own the office where an employee works, that employee can still have a privacy interest in the office that prohibits the employer from conducting a search or surveillance.

One of the key factors used to determine the existence of a reasonable expectation of privacy is the amount of control an employee exercises over the area or item to be searched. If, for example, the employee has *exclusive control* over the area or item in question, this fact tends to show that the employee has a reasonable expectation of privacy in that area or item. For instance, assume that an employee has a file cabinet in his office, that the employee is the only person who uses it, that the cabinet has a lock on it, that the employee is the only person with a key, and that the cabinet remains locked when the employee is not using it. These facts indicate that the employee has exclusive control over the contents of the cabinet, and thus has a reasonable expectation of privacy in its contents. In other words, based on the circumstances, the employee would be justified in believing that others cannot and will not enter the file cabinet without his consent. The employee in this scenario has a protected privacy interest in the contents of the file cabinet. A search of this file cabinet by the public employer would have to comport with the *reasonableness* standard as discussed above.

Conversely, an employee probably cannot claim a privacy expectation in a work area that is open to the public and shared with other employees. For instance, using the previous example, assume that the file cabinet does not have a lock, that several employees store and retrieve files from it, and that it is generally understood that employees can access the cabinet's files without the employee's consent. Under these facts, the employee cannot reasonably expect that the contents of the cabinet are private. Under these facts, the employee would not have a reasonable expectation of privacy in the file cabinet; therefore, a search of that file cabinet would probably not violate his rights.

Reasonable privacy expectations can also attach to communications, such as data stored on hard drives and other electronic communications like phone calls, emails, and text messages.

In terms of surveillance, employees are likely to have reasonable privacy expectations in bathrooms, changing rooms and other personal areas within the workplace.

Obviously, there are many factors that go into determining whether an employee has a reasonable expectation of privacy. Before conducting a search or surveillance, employers

should discuss it with legal counsel to make sure they are not intruding upon an employee's privacy interests.

Reducing Employees' Expectations of Privacy

Employers can reduce their potential liability for violations involving searches and seizures by lowering employees' expectation of privacy in the workplace. If an employer puts employees on notice that their offices, desks, files, voice mail, computers, and so forth are not private, then employees cannot assert that they have a reasonable privacy expectation in those areas.

The best method that employers can use to lower employees' expectations of privacy is to adopt a written privacy policy that puts employees on notice that the workplace is not private and require employees to sign it. Such policies should provide that, to maintain the security of operations, management may gain access to and search all work areas and personal belongings, including desks, file drawers, lockers, briefcases, handbags, pockets, and personal effects.

The policy should also notify employees that computer systems (including the Internet, email communications, hardware, and files) are solely for business use, and that the company reserves the absolute right to monitor, review, audit, and disclose all matters sent over the system or placed in storage.

In addition, the policy should state that workplace areas are subject to surveillance and that business phone calls may be monitored.

Employers should take appropriate steps to ensure that all employees are aware of and understand the privacy policies. For instance, management should give a copy of the policies to new employees when hired and have them sign an acknowledgment that they read and understood the policies. Employers should provide all employees with copies of changes or updates to the policy and post policies in a prominent place in the workplace. Such actions are necessary because, unless otherwise informed, an employee may have an expectation of privacy in an item that his employer needs to search.

When policies are in place, the courts have held that an employee has no (or a very low) expectation of privacy. Therefore, communicating policies to employees substantially reduces the risk of privacy violations.

Also, to reduce their potential liability for violations involving searches and seizures, employers can take the following measures:

- Retaining a key to all desks, lockers, and so on
- Requiring employees to provide keys to all personal locks
- Obtaining consent to search workplace areas

Rights and Obligations Under Criminal Law

Generally, individuals arrested or questioned by the police for suspected involvement in criminal activity have certain rights, such as the right to remain silent and the right to counsel. This discussion examines some of those rights.

The Right to Remain Silent

A tenet of many legal systems is that a criminal suspect or person accused of a crime has the right to remain silent both at the investigative stage and at the trial stage of criminal cases.

The right to remain silent is centered on the right of those who are suspected of committing a crime to refuse to answer questions by the government when the questioning occurs under the threat of judicially imposed punishment. The right to remain silent applies to individuals being questioned by government authorities, but not someone who is being questioned by private party acting on its own accord. Accordingly, the right to remain silent generally does not apply in internal investigations by private employers.

These rights, however, differ in common law and civil law systems.

The Right to Silence in Common Law Systems

Common law systems recognize the right to remain silent. To review, common law systems are those in which court decisions have a precedential authority, and the judicial proceedings are typically adversarial in nature. Essentially, the right to remain silent in common law systems guarantees those suspected of a crime the right to refuse to answer questions or to provide certain personal information that might be incriminating. Thus, the right to remain silent prevents government authorities from forcing a criminal defendant to give testimony against himself. Note, however, that the right does not protect the defendant from being ordered to provide other types of evidence, such as the weapon used in an alleged assault or a sample finger print.

Generally, if the subject has a right to remain silent, government authorities must warn the subject of this right before they can question him. In the United States, for example, police officers must give *Miranda* warnings to criminal suspects in a custodial interrogation. *Miranda* warnings, which advice suspects that they have the right not to answer questions and the right to legal counsel during interrogations, are required only if a person is being subjected to custodial interrogations. *Custodial interrogations* refer to guilt-seeking questioning initiated by law enforcement officers after a person is in custody. A person is in custody in two situations:

- When the suspect is under arrest
- When the suspect is not under arrest but has otherwise been deprived of freedom in any significant way

There are *Miranda* equivalents in other countries. For example, in Canada, individuals have similar rights pursuant to the Charter of Rights and Freedoms. Also, the European Union (EU) has published a directive on the right to information in criminal proceedings. The agreed law, known as "the Reding Rights," means that suspects in the EU who are detained receive a letter listing their basic rights during criminal proceedings.

Again, the right to remain silent applies to individuals being questioned by government authorities or someone acting at the government's request, but not when someone is being questioned by private party acting on its own accord. Accordingly, the right to remain silent generally does not apply in internal investigations by private parties (e.g., a company). Therefore, non-government fraud examiners or investigators can usually interview a subject without informing him of the right to remain silent.

Also, because the right to remain silent does not apply in internal investigations by private companies, private employers generally can fire employees for refusing to answer questions that might incriminate them (i.e., for refusing to cooperate). Likewise, when a private employer is interviewing an employee who has no right to remain silent, the employer can use a threat of termination to coerce the employee to answer questions.

Although the right to remain silent does not apply in internal investigations by private employers acting on their own accord, it may apply if the private entity is acting in connection with government authorities. For example, if the examiner has been in touch with law enforcement before interviewing a suspect in an internal investigation, then the answer as to whether the suspect has a right to remain silent is not as clear. If police or other

law enforcement personnel are involved, then the suspect may have certain legal rights, including the right to remain silent. The failure to follow certain precautions may invalidate any evidence obtained by the investigator.

While the right to silence is the general rule, some common law jurisdictions provide exceptions under certain circumstances. For instance, in England and Wales, the right does not apply to investigations conducted by the Serious Fraud Office, a UK government department that investigates and prosecutes complex fraud.

The Right to Silence in Civil Law Systems

The right to remain silent is not as uniform in civil law jurisdictions as it is in common law jurisdictions. Again, civil law systems are those in which all laws are codified and the judicial proceedings tend to be inquisitorial. While the right to silence usually exists in some form, the trend is that civil law jurisdictions tend to place less value on the right to remain silent by creating various exceptions to the rule.

Several jurisdictions, for instance, provide a right to silence during the investigation of a crime, but at trial the defendant may be compelled to answer. Other jurisdictions allow for the defendant to remain silent, but allow the prosecution to comment on the silence as indicative of guilt. Check the laws of the local jurisdiction to find under what circumstances, if any, a defendant's right to remain silent may be curtailed.

Like in most common law systems, some civil law systems require government authorities to warn criminal subjects of their right to remain silent. For example, in Germany, criminal suspects must be informed of their right to remain silent before any interrogation.

But not all civil law systems impose such requirements. For example, in France, when individuals are arrested and detained by the police, the police do not have to inform the suspects of their right to remain silent.

Right to Counsel

The right to counsel is the right of criminal defendants to have a lawyer assist in their defense, even if they cannot afford to pay for one. Thus, if an individual is the subject of a criminal investigation by government authorities, he may have some type of right to consult an attorney or have an attorney appointed. This right is generally found in both civil and common law jurisdictions.

Generally, the right to counsel does not apply if there is no government action. Thus, in most cases, a private employer can interview an employee without the presence of the employee's attorney.

Police officers and other state agents who violate an accused's right to counsel do so at their own peril. Any evidence gathered in violation of an accused's rights may be inadmissible at trial.

Generally, a subject can waive his right to counsel, but to be valid, any waiver must be voluntary and premised on a true appreciation of the consequences of giving up that right. For example, if the detainee waives his right to counsel while drunk, the waiver will not likely stand because, under such circumstances, the subject cannot make a meaningful determination of whether or not to waive the right to retain counsel.

Many jurisdictions create exceptions to the right to counsel in criminal trials, the most typical being minor violations.

Right to a Trial by Jury

Some jurisdictions entitle defendants to the right to a trial by jury in criminal prosecutions. The right to a jury is a criminal defendant's option to have the facts of his trial decided by a jury (i.e., group of his peers sworn to give a verdict on the basis of evidence submitted in court). Juries are most common in jurisdictions with common law, adversarial systems. The right to a jury generally varies in common law and civil law jurisdictions.

In a trial by jury, the judge and jury serve important roles. In most common law jurisdictions, the jury is responsible for finding the facts of the case, while the judge applies the law, rules of evidence, and generally moderates the proceeding to ensure a fair trial.

Some jurisdictions with jury trials allow the defendant to waive his right to a jury trial. If a defendant waives this right, the judge decides both the facts and the law in what is called a *bench trial*.

Typically, jury trials are available only for serious criminal offenses. In fact, in civil law systems, juries are generally only used for the most serious cases. In some jurisdictions, jury trials are not available for civil cases.

There are, however, some democratic countries that have no criminal jury system. These include Chile, the Czech Republic, Hungary, India, Israel, Mexico, the Netherlands, and South Africa.

Right to a Trial by Jury in Common Law Systems

The right to a jury is paramount in many common law systems, and jury trials are available for most criminal trials (and even some civil trials). Typically, jurisdictions with jury trials allow defendants to waive their right to a jury trial.

In most common law jurisdictions, the jury is a group of citizens summoned at random, and it is responsible for deciding the facts of the case, while the judge makes the legal decisions. The number of people on a jury varies between jurisdictions, as does the number of people on the jury required to find a defendant guilty. This means that, in a criminal case, ordinary citizens will decide whether the accused is guilty or innocent of the charge against him.

Right to a Trial by Jury in Civil Law Systems

There is a common misconception that civil law systems do not provide for the right to juries, but that is only true in some jurisdictions. In civil law systems, trials are conducted by the judge or judges, who may sit alone or with jurors, also known as *lay judges*.

In civil law systems, juries are generally only used for serious cases. For example, in France, which is a civil law country, serious crimes are heard by criminal trial courts that sit with three judges and six or nine jurors. The role of jurors in civil law systems may not be as strong as it is in common law countries, and jury trials may not be as available in civil law systems, but they do exist.

Right to Be Free from Unreasonable Search and Seizure by Government Agents

Most countries have laws that provide the public with the right to be free from unreasonable search and seizure by government authorities. For example, in the United States, the Fourth Amendment to the U.S. Constitution guarantees the right of all citizens to be free from unreasonable searches and seizures. In Canada, Section Eight of the Canadian Charter of Rights and Freedoms protects all individuals from unreasonable search and seizure.

The right to be free from unreasonable searches and seizures protects individuals from actions by government authorities; it does not protect against actions by private parties acting on their own accord.

Limits on Using Confessions in Criminal Cases

A *confession* is an admission of misdeeds, and there may be laws limiting the use of suspects' confessions in criminal cases. In criminal cases, statements made by the accused to persons in authority are very frequently the primary, if not the only, evidence implicating the accused in the crime charged.

In some jurisdictions, confessions made out of court by the accused may only be admitted into evidence if the prosecution shows that the statement was made freely and voluntarily. In general, a confession is voluntary if it is not coerced by physical or psychological means, but determining whether a confession is voluntary will depend on the facts.

The rule requiring free and voluntary confessions has its origin in the fear that without such a rule, evidence would be obtained by torture, threats, or violence. In many jurisdictions, courts will admit a statement as long as it is voluntarily and freely made, even if it is obtained through deception.

Moreover, in jurisdictions limiting the admissibility of confessions, the law may require the government to establish the accuracy of the statement if it intends to use it against the accused. Courts give more credence to written statements than to oral statements. Therefore, law enforcement can avoid much difficulty by having a statement recorded.

Additionally, if a statement is to be admitted in such jurisdictions, the government may be required to show the accused had the mental capacity to make such a statement.

The Law Relating to Government Search and Seizure

The law relating to search and seizure is extremely complex. In many countries, the state's power of search and seizure is derived from common law and statutory law, and rights providing search and seizure protections can even vary within a country based on the laws of a particular state or province.

Search Warrants

Again, most countries have laws that provide the public with the right to be free from unreasonable search and seizure by government authorities, and though interpretation can vary, this right sometimes requires that the government obtain authorization (e.g., a search

warrant) by a judicial officer or other authorized person before it conducts a search of a person, location, or vehicle for evidence of a crime.

A *search warrant* is a court order that grants government authorities the right to search a premises or property for information pertinent to a case. Search warrants were developed because, in most countries, governments do not have a general right to search a person's home without permission. And even today, in common law jurisdictions, there is no common law authority to search someone's home without the permission of the owner or occupier. These principles continue to guide us today so that if a court finds a search warrant invalid, a legal action can be brought against a person who searched the premises without consent or a valid warrant. Furthermore, the material seized under an invalid search warrant may not be admissible in court.

The requirements for search warrants or other similar authorization, however, do not apply to private parties acting on their own accord because the right to be free from unreasonable searches and seizures does not protect against actions by such parties. The right to be free from unreasonable searches and seizures only protects individuals from actions by government authorities. Thus, to determine whether a search warrant is required for a search to be conducted in an investigation, it is necessary to first determine whether government authorities are involved in the search.

Also, the right to be free from unreasonable search and seizure by government authorities can extend to searches in the workplace.

Warrants and similar legal devices are used in most countries, but the warrants range in importance. In the pattern of emphasizing defendants' rights, common law countries tend to require that warrants be issued in more situations than civil law countries. Civil law countries tend to curtail the need more often. For instance, some jurisdictions do not require warrants for flagrant offenses. Moreover, the threshold for obtaining a warrant is typically easier in civil law systems than in common law systems.

Reasonableness

In general, searches must be reasonable and they must be conducted in a reasonable manner. Whether it is reasonable to conduct a search and whether the search was conducted in a reasonable manner is determined by the totality of the circumstances. What constitutes a reasonable search varies by country. In most common law countries, a reasonable search is

one carried out pursuant to a search warrant issued on a showing of probable cause. *Probable cause* has been defined as those facts and circumstances sufficient to cause a person of reasonable caution to believe that a crime has been committed and that the accused committed it. Thus, authorities must have reason to believe that a crime has likely occurred. The determination of reasonableness depends on the individual's reasonable expectation of privacy and the degree of intrusiveness of the search compared to the interest advanced by it.

In civil law systems, the requirements for reasonableness of a search tends to be more relaxed, either because warrants are less often required or because something less than probable cause is required to conduct the search (or both).

Exceptions to the Warrant Requirement

Even if a warrant is technically required, there are a number of recognized exceptions to the warrant requirement. Two key exceptions are consent searches and evidence in plain view.

CONSENT SEARCHES

Consent is a recognized exception to the requirement that government agents must obtain a warrant before they search a person, location, or vehicle for evidence of a crime. Individuals are always free to consent to searches. If a suspect consents to a search or seizure by police or government agents, the consent eliminates the need for a search warrant. That is, the consent to search waives the person's right to be free from government searches. Thus, the government does not need a warrant to perform a search if a person with proper authority consents to a search.

Courts will closely scrutinize any such "consent" to make sure it was truly voluntary, particularly when it leads to the seizure of incriminating evidence. To be valid, an individual's consent to a search or seizure must be voluntary.

Consents to searches or seizures by government agents obtained by force, duress, or bribery are generally held to be involuntary and invalid; therefore, such consent does not constitute a valid waiver of a person's right to be free from unreasonable searches. Jurisdictions are mixed, however, as to whether consent obtained by deceit constitutes a valid waiver.

In the context of workplace searches, an individual's consent might not be voluntary if it requires a choice between exercising legal rights and continued employment.

Also, there is generally no requirement that government agents warn suspects that they have a right to refuse consent.

Consent may be implied in circumstances where the individual can choose between entering an area and submitting to a search, or not entering, as when one enters a secured courthouse, boards an airplane, or crosses an international border.

Additionally, consent may be given by third parties to searches of property over which the third parties have authority, such as a co-tenant in a leased apartment.

EVIDENCE IN PLAIN VIEW

In many countries with a warrant requirement, the plain-view doctrine is an exception to the general rule that the government must obtain a search warrant before conducting a search of a person, location, or vehicle for evidence of a crime. Under this doctrine, evidence in plain view of a law enforcement officer who has a right to be in a position to observe it may be seized without a warrant. The plain-view doctrine applies when a government official inadvertently discovers contraband or evidence of another crime during a search or arrest, even if there was no prior authority to seize the evidence. Thus, the doctrine applies only if a police officer is legally authorized to search the premises in which he inadvertently discovers the additional evidence in plain view.

The plain-view doctrine does not apply unless the police officer discovered the evidence inadvertently. Thus, if discovery of the evidence is anticipated, and no other exception applies, the officer must first obtain a warrant. That is, if the officer knows in advance the location of certain evidence and relies on the plain-view doctrine to seize the evidence, the seizure will be considered illegal.

Also, evidence will not be admissible under the plain-view doctrine unless it is apparent to the police that the items observed were evidence of a crime or otherwise subject to search and seizure.

Investigations in Private Actions

The right to investigate, examine, or audit for fraud is implicit in most business, accounting and legal systems. No special authority is required, although the activities of investigators and others may be regulated.

A fraud examiner may lawfully interview witnesses, collect evidence where lawfully available, collect and review documents, and examine public records, without fear of liability, if the examiner acts prudently and in good faith.

Of course, investigations in private actions are subject to certain legal limitations, some of which—such as the laws prohibiting unauthorized electronic surveillance—are enforced with criminal as well as civil penalties. Overzealous or imprudent acts by private parties (even if technically legal) can result in counterclaims, liability, and legal sideshows that can delay, disrupt, or even completely derail a meritorious case. Thus, fraud examiners must keep in mind the rights of those involved in any private investigation.

Below is a brief discussion of some legal issues that can arise as a result of an investigation, particularly one conducted in an irresponsible manner, carried out without predication, or conducted in a way that violates the rights of those involved. Each can be avoided if the examiner is guided by common sense and professional standards and confines himself to measures reasonably necessary to accomplish legitimate objectives. The examiner should always pursue the facts, not people; should ask rather than accuse, prove rather than allege.

Defamation

Many countries have defamation laws that provide redress against harm to reputation. Generally speaking, *defamation* refers to the unprivileged publication of false statements about a person that causes harm to that person's reputation.

Defamation can be a crime or a civil violation, and the law varies by jurisdiction as to whether it is a criminal offense or a civil wrong. For example, defamation actions can be brought under the criminal and the civil law in most Southeast Asian countries. Also, in most civil law countries, defamation is dealt with first as a crime, rather than a civil wrong.

In most common law jurisdictions, the law of defamation comes in two forms: libel and slander. *Libel* refers to defamatory statements in writing, and *slander* refers to spoken statements, although the distinction often is blurred in cases involving electronic media. Thus, the key difference between libel and slander is the form in which the defamatory statement is made. In other jurisdictions, there is no distinction between libel and slander. For example, German law makes no distinction between libel and slander.

The threat of a defamation lawsuit is always present when allegations of wrongdoing are made against certain employees. For example, a claim of defamation might arise in the context of an interview as a result of unfounded accusations or statements made by the interviewer, where someone in addition to the employee and the interviewer is present.

If a plaintiff brings a successful claim for defamation, he may recover special damages (out of pocket losses), general damages to reputation, and (in some jurisdictions) punitive damages, which can be substantial.

Elements of Defamation

In general, the elements of libel and slander are the same, and to recover for defamation, the plaintiff must generally prove all of the following elements:

- The defendant made an untrue statement of fact.
- The statement was communicated (published) to third parties.
- The statement was made on an unprivileged occasion.
- The statement damaged the subject's reputation.

UNTRUE STATEMENT OF FACT

To be defamatory, a statement must be a statement of fact (not opinion) and be untrue. Thus, truth is an absolute defense to defamation.

COMMUNICATED TO THIRD PARTIES

To be defamatory, a statement must be published, either orally or in writing, to a third party. Defamation does not occur when one accuses another directly and in the presence of no other parties; to be defamatory, a statement must be heard or read by a third party.

ON AN UNPRIVILEGED OCCASION

Also, for a statement to qualify as defamatory, the occasion in which the statement is made must be an unprivileged one. If the statement is made on a privileged occasion, then no liability can attach to the declarant. Basically, the law recognizes that there are some circumstances in which the need to share information is so important that people will be allowed to make mistakes from time to time without having to worry about being sued for defamation. Statements that are made in these circumstances are said to be privileged.

Assuming that an employee can establish that defamatory statements were made and communicated to a third party, the most important defense privileges available include:

- Statements made during a judicial proceeding
- Statements made in preparation of judicial proceedings
- Statements made between a solicitor and his client
- Good faith statements made to protect a legitimate interest of the speaker or recipient—such as a communication between an employee and his employer regarding an important business matter or the results of an examination into suspected fraud

Accordingly, fraud examiners are protected by a number of recognized privileges in the law of defamation. In short, the fraud examiner who works in a prudent manner should not be concerned about liability for defamation.

DAMAGE THE SUBJECT'S REPUTATION

Additionally, to be actionable as defamatory, a statement must damage the reputation of a party. But in cases involving public figures who claim defamation, the statement must also be made with malice to create liability.

Privacy Laws

Privacy laws are designed to protect the rights of individuals to be left alone.

The legal systems of different countries, however, perceive privacy issues differently. For example, U.S. notions of privacy are different than those held by people in other parts of the world. Specifically, in the United States, the right to privacy is perceived as part of the concept of liberty, but in most of the world, privacy is perceived as a central tenet of human dignity. Moreover, in Europe and Canada, privacy is considered a fundamental right. Consequently, Canadian and European legal systems impose greater legal restrictions on employers wanting to monitor or use surveillance in the workplace than the U.S. legal system.

Two Categories of Privacy Laws

There are two categories of privacy laws: general privacy laws and specific privacy laws. General privacy laws are designed to protect the general privacy of the personal information of individuals. Specific privacy laws regulate particular aspects of particular types of information. Common types of specific privacy laws are those that concern:

- Online information
- Financial information
- Health information

- Communications
- Privacy at home

Human Rights Legislation in the European Union

The European Convention on Human Rights, which is the authoritative human rights instrument in Europe, provides that individuals have the right to respect for private and family life in Article 8. The Treaty Establishing the European Union, in recognizing Article 8, requires member states to respect the fundamental rights guaranteed therein.

Also, the Charter of Fundamental Rights of the European Union, which sets forth a binding list of rights for the European Union and its member states, affirms that "[e]veryone has the right to respect for his or her private and family life, home and communications."

Civil Invasion of Privacy

Invasion of privacy laws concern a person's right to keep his life private and free from intrusion, and in many common law countries, invasion of privacy is a civil wrong that can be addressed by a court through a lawsuit.

That is, some common law countries recognize a right to bring a civil action for damages for invading an individual's personal privacy. In the United States, courts have recognized a cause of action for invasion of privacy where there is a public disclosure of private facts, even if the private facts are otherwise true and accurate. In Canada, legislation has been enacted in several provinces making invasion of privacy a civil wrong, "actionable without proof of damage, for a person, willfully and without claim of right, to violate the privacy of another." For example, Manitoba, British Columbia, Saskatchewan and Newfoundland have all enacted such laws.

Some countries, like the United Kingdom, do not recognize invasion of privacy as a civil wrong. However, courts in the United Kingdom have used breach of confidence actions to address the misuse of private information.

While in other countries, it is unclear whether there is a civil cause of action for invasion of privacy.

The two most common forms of invasion of privacy applicable to fraud examinations are intrusion into an individual's private matters and publicity of private facts.

INTRUSION INTO AN INDIVIDUAL'S PRIVATE MATTERS

The civil wrong regarding intrusion into an individual's private matters (often referred to as *intrusion upon seclusion*) occurs when an individual intentionally intrudes into another individual's private matters and the intrusion would be highly offensive or objectionable to a reasonable person. The elements of this civil wrong include:

- An intentional intrusion
- Into an area where an individual has a reasonable expectation of privacy
- The intrusion would be highly offensive or objectionable to a reasonable person

There is no invasion of privacy if the information at issue is open to public view or has been disclosed to others.

An intrusion claim can be based on physical intrusions, wiretapping, eavesdropping, and other forms of surveillance. Thus, liability for this civil wrong may arise from conducting an unwarranted search of another's personal property, performing intensive physical surveillance, or obtaining private bank account information, absent legal authority. Also, questioning employees about activities not related to job performance might constitute an intrusion into seclusion.

PUBLIC DISCLOSURE OF PRIVATE FACTS

Public disclosure of private facts occurs when one party makes public statements about another party's private life that are not of public concern. For instance, disclosing information obtained in an interview conducted as part of a fraud investigation to individuals not involved in the investigation might constitute a public disclosure of private facts.

To establish liability for the public disclosure wrong, the plaintiff must prove all of the following elements:

- The defendant made public statements about another party's private life.
- The statements were not of public concern.
- The statements would be highly offensive to a reasonable person.

The key to this cause of action is that the information must be private in nature and not a matter of public interest.

Also, unlike the requirements to establish a claim for defamation, liability for this cause of action can arise even if the statements at issue are true. Because giving unreasonable publicity to true, but private, information about an employee can give rise to a claim for invasion of privacy, the need to communicate information about the employee must be balanced against the intrusion into the employee's privacy. Thus, examiners must be careful when disclosing investigatory materials or conclusions.

The gist of this civil wrong is the unwarranted publicity of private facts, not the discovery of private facts. In the United States, courts have held that the publicity must be broad and pervasive for liability to attach. Thus, one case found no liability when a bank gave the account information of one of its customers to the customer's employer, and another court exonerated an investigator who reported credit information to an insurance company. The collection of such information can, however, violate the civil wrong for intrusion into seclusion.

Data Privacy

Most countries have data privacy laws (also known as *information privacy* or *data protection* laws) that protect personal information about individuals from disclosure, unauthorized access, and misuse. As innovations in technology make it easier to track, compile, and process personal information about individuals, fraud examiners who deal with personal information must take steps to comply with local and international data privacy laws. These laws can significantly affect data collection, data use, and cross-border transfer.

Typically, these laws address:

- How personal information is handled
- How personal information is collected
- How personal information is used
- Who has access to personal information
- When personal information is amended, changed, and deleted

Also, data privacy laws focus on personal information, but they define personal information in different ways. Nevertheless, on a general basis, personal information refers to any information about an identifiable individual, such as:

- An individual's personal characteristics (e.g., name, gender, age, government identification number, household income, home address or phone number, race and ethnicity, physical characteristics, family status, marital status, and employment status)

- An individual's health information (e.g., health history, visit history, health conditions, received health services)
- An individual's activities and views (e.g., religious affiliations, political views, personal opinions)

Data privacy laws are based on Fair Information Practices, which are a set of standards for addressing the privacy of information about individuals. Different countries have their own standards for data privacy, and the Organization for Economic Co-operation and Development (OECD) has published *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines), which were developed to harmonize national privacy legislation and prevent interruptions in international flows of data.

The OECD Privacy Guidelines set out eight principles for the processing of data by private and public sectors that member countries should incorporate into national law, and in terms of substance, the OECD Privacy Guidelines are very similar to other expressions of Fair Information Practices.

Even though countries have their own requirements for the protection of data privacy, most countries impose requirements that converge around the principles that all personal information must be:

- Obtained fairly and lawfully
- Used only for the original specified purpose
- Adequate, relevant, and not excessive to the specified purpose
- Accurate and updated
- Accessible to the data subject
- Protected by reasonable security safeguards
- Destroyed after its purpose is completed

To illustrate, consider the applicable regulations in the European Union, the United States, and Canada.

EUROPEAN UNION

The EU Data Protection Directive (also known as EU Directive 95/46/EC) is the principal data protection instrument in the European Union. The EU Data Protection Directive regulates the processing, using, and transferring of personal data within the European Union, and it places limits on transmitting personal data to non-EU countries.

The EU Data Protection Directive establishes the blueprint for data privacy laws across Europe, and it mandates that all EU member states enact laws and regulations that satisfy certain minimum standards, which include, among other things, requirements that data controllers:

- Give their identity and purpose when collecting data directly from the subject.
- Notify the subject of their identity, the type of information they are collecting, and their purpose when collecting data from a third party.
- Collect data for only specific, legitimate purposes.
- Avoid processing data unless certain conditions are met.
- Avoid processing data unless necessary to achieve a specific, legitimate purpose.
- Keep data confidential and secure.
- Give data subjects the right to information about the processing of their personal data.
- Give data subjects the right to access and correct any inaccurate data.

UNITED STATES

The United States does not have a comprehensive set of generally applicable data protection laws. Instead, the United States uses a sectoral approach where different economic sectors operate under different legal requirements. This approach, which relies on a mix of legislation, regulation, and self-regulation, creates a system in which privacy standards emerge from a complex interplay of overlapping state and federal laws and regulations, as well as industry practices.

Data privacy regulation in the United States is more prevalent in areas where abuses of personal information are most likely to occur, such as the financial and health care industries.

CANADA

Canada, like the United States, uses a sectoral approach to protect data. In Canada, an individual's private data may be protected by, among other things, the Constitution, common law, federal law, and provincial law. But even so, the overarching federal data protection law in Canada is the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA governs how management of private-sector organizations collect, use, and disclose personal information in the course of commercial business.

Among other requirements, PIPEDA sets out ten principles that establish ground rules for the collection, use, and disclosure of personal information. These ten principles state:

- OrganizationOrganizations are responsible for any personal information under their cont rol.
- Organizations must identify why it collects, uses, or discloses personal information, they must document why the information is collected, and they can only use the information for the stated purpose.
- Organizations must obtain an individual's consent to collect, use, or disclose that individual's personal information (except in certain situations).
- Organizations must limit the collection of personal information to that which is necessary for the purposes identified.
- Organizations can only use personal information for the purpose for which it was collected except with the consent of the individual or as required by law.
- Organizations must keep all personal information accurate and up-to-date.
- Organizations must protect personal information with security measures that are appropriate to the sensitivity of the information.
- Organizations must make personal information readily available upon request, and they must disclose their personal information policies and practices.
- Individuals must have the right to access and correct personal information covered entities may have collected about them.
- Individuals should be able to challenge an organization's compliance with any PIPEDA privacy principle.

International Data Transfers

Many countries have adopted legal restrictions on international data transfers. Thus, an important issue that arises in transnational investigations concerns the transmission of personal data to outside countries.

Data transfers cover any sharing, transferring or disclosing, giving access to, or otherwise making available, information to third parties (e.g., corporate entities and government authorities).

Some countries, such as those within the European Union, Hong Kong, and India, limit the transmission of personal data to other countries, whereas other countries, such as Thailand, do not.

Moreover, even where countries provide protection for cross-border data transfers, there are discrepancies in the implementation and application of such protections among the different countries. Some countries, such as those in the European Union, impose restrictions on the transmission of personal data to other countries, but others, such as Canada and Japan, have laws that do not distinguish between cross-border and domestic transfers to third parties. Instead, they impose certain obligations on collecting entities to remain accountable for protecting personal information transferred to third parties.

Member states of the European Union impose specific restrictions on cross-border transfers. In particular, member states of the European Union have laws that prohibit the transfer of personal information to jurisdictions outside of the European Union unless the country of final destination offers an adequate level of protection for data. The European Commission, which is the executive of the European Union, is authorized to make an "adequacy" finding as to whether a country offers an adequate level of protection, and it has done so for some countries.

In contrast to the restrictions on cross-border transfers in the European Union, Canada applies an organization-to-organization approach under the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs how private-sector organizations collect, use, and disclose personal information in the course of commercial business. PIPEDA provides that organizations that collect data are responsible for protecting personal information transferred to other jurisdictions. And under PIPEDA, organizations that collect data must take all reasonable steps to protect personal information from unauthorized disclosures while it is in the custody of third parties. That is, under PIPEDA, organizations must be satisfied that a recipient of personal information has policies and processes in place to ensure that personal information in its custody is safeguarded.

Given the wide range of legislation and practices regarding cross-border transfer laws and restrictions, fraud examiners working in other countries must become familiar with laws governing privacy and must adapt their procedures according to local rules.

Nevertheless, there are three basic options by which management can legitimize cross-border transfers of personal information:

- Obtain the consent of the data subject.
- Establish a contract between the entities exchanging the information (i.e., between the transmitting entity and the receiving entity).

- If transmitting from the European Union to non-European Union countries, rely on adequacy decisions by the European Commission. That is, limit the transfer of data to countries that offer an adequate level of protection, as determined by the European Commission.

False Imprisonment

Many countries have false imprisonment laws that protect against unlawful confinement. *False imprisonment* is the unlawful restraint by one person of the physical liberty of another without consent or legal justification.

To recover for a claim of false imprisonment, the plaintiff must prove all of the following elements:

- The defendant used words or actions intended to restrain the plaintiff.
- The defendant's words or actions resulted in the restraint of the plaintiff without the plaintiff's consent (i.e., against the plaintiff's will) and without legal justification.
- The plaintiff was aware that he was being restrained.

A claim of false imprisonment might arise if an employee is detained in any way during a search or interview. Generally, an employer is entitled to question an employee at work about a violation of company policy without incurring liability as long as the employee submits to the questioning voluntarily; that is, not as a result of threats or force.

There are no precise rules as to when a false imprisonment occurs, but factors such as the length, nature, and manner of the interview might determine whether liability arises. Other factors used to determine if an individual has been falsely imprisoned include:

- Conducting an interview in a room that is small and confined in nature (e.g., small, windowless, not easily accessible)
- Locking the door to the interview room
- Blocking the exit to the interview room
- Conducting an interview in a room with severe lighting
- Requiring the employee's presence or continued presence by any amount of physical force (e.g., holding the employee's arm to escort him or pushing the employee into a chair)
- Using violent behavior of any kind during the interview, including yelling, pounding on desks, or kicking furniture or walls

- Using a physical barrier to restrain the employee (e.g., locking the door or standing in front of the exit)
- Making threats of immediate physical force to restrain the employee
- Conducting an interview in the presence of numerous people

Defenses to claims of false imprisonment include good faith and probable cause to believe the person restrained has committed an offense.

Malicious Prosecution

A *malicious prosecution* claim seeks recovery of damages for having to endure and defend a groundless lawsuit that the defendant filed, or caused to be filed, against the plaintiff. Thus, if a person files, or causes the government to file, a groundless criminal prosecution against an individual, the person against whom the charges were brought may retaliate by bringing a malicious prosecution lawsuit.

In general, to bring a successful malicious prosecution claim, the plaintiff must show evidence of a deliberate, groundless prosecution involving the following elements:

- The defendant instituted a criminal action against the plaintiff.
- Those proceedings ended favorably for the plaintiff (e.g., the charges are dismissed).
- There was a lack of reasonable and probable cause for the defendant's conduct (i.e., there was no just cause).
- There was an improper purpose underlying the defendant's conduct, not an honest belief in guilt (i.e., the defendant acted with malice).

Intentional Infliction of Emotional Distress

Intentional infliction of emotional distress refers to any unprivileged conduct that is so outrageous and egregious that it exceeds all bounds usually tolerated by civilized society and that is intended to cause injury (or was committed with reckless disregard for the likelihood of its causing injury) to another. It is a civil action available mainly in common law countries.

To recover for intentional infliction of emotional distress, the plaintiff must prove all of the following elements:

- The defendant engaged in extreme and outrageous conduct.
- The defendant acted intentionally or recklessly (i.e., the defendant intended that his conduct would cause severe emotional distress, or he acted recklessly with regard to whether his actions would cause severe emotional distress).

- The victim actually did suffer emotional or mental distress as a result of the defendant's conduct.

For liability to attach, the offending conduct must "outrage the sensibilities of a reasonable man." Mere angry words or insults, or allegations or implications of wrongdoing (if based on reasonable grounds) are not enough. Also, it is not enough that the individual is merely "upset" by the conduct.

In addition, the cause of action is not actionable unless there is proof of actual physical harm; there must be a "visible and provable" illness resulting from the conduct of the defendant.

Wrongful Discharge

Wrongful discharge occurs when an employer discharges an employee for an improper reason (e.g., discrimination), in violation of actual or implied employment contract or company policies.

The scope for wrongful discharge, however, varies by jurisdiction.

Legal Protections Regarding Interviews

Interviews, and especially interviews of suspects, can expose the organizational powers administering the interview and the individual conducting the interview to certain legal risks. Thus, before engaging in an interview, the fraud examiner must understand the ramifications of his actions, which requires an understanding of certain legal issues and how they limit or affect the ways in which an interview may be conducted.

Of particular significance is the fact that most jurisdictions place restrictions concerning the ways in which employers can conduct interviews. Such restrictions might stem from employee-employer contracts, collective labor laws, laws protecting labor rights, the common law, laws protecting fundamental rights, other applicable statutes, and so on.

Thus, it is in the organization's best interest to have someone review all aspects of the employer-employee relationship—including company policies, contractual relationships, and prevailing law—before conducting interviews.

MENU

THE CRIMINAL JUSTICE SYSTEM

Criminal law deals with offenses of a public nature, whereas civil law is the body of law that provides remedies for violations of private rights. A criminal defendant has certain rights, but these rights vary substantially from jurisdiction to jurisdiction. This chapter describes several procedures and issues in criminal cases that fraud examiners should be aware of.

International Covenant on Civil and Political Rights

Most countries have signed and ratified the United Nations' International Covenant on Civil and Political Rights (ICCPR), which commits them to recognizing various rights of citizens. Part III of the ICCPR includes the rights of those accused of crimes. Members of the ICCPR adopt their own version of laws to uphold such rights, but do not always implement (or enforce) every provision. Despite inconsistencies, the ICCPR is useful in understanding the existence of rights throughout various jurisdictions.

The following are protections most relevant to fraud examination.

Freedom from Improper Arrests

Under the ICCPR, individuals have the right to liberty and shall not be subjected to arbitrary arrest or detention. Arrests must be done in accordance with procedures established by law. Once a person is arrested, the person is entitled to a proceeding before a court to decide without unnecessary delay the lawfulness of the detention and must be released if there is no lawful reason.

Most countries provide some degree of protection from unreasonable searches and arrests by the government. The two major types of issues concerning arrests are the conditions under which a person may be lawfully arrested and the rights that a person under arrest has (e.g., right to remain silent, right to legal counsel, etc.). A *custodial arrest* occurs whenever a government officer has a person in custody, meaning an officer has indicated that the person is not free to leave. It is important to determine when an arrest occurs to establish what rights the subject of the arrest had at a given time.

Generally, the government may not make an arrest unless there is a good reason to believe that the suspect committed an offense. Many countries require a warrant signed by a judge or magistrate to authorize an arrest. However, even where warrants are required, there are

typically exceptions that allow law enforcement officials to make arrests without warrants. Typical examples of such exceptions include:

- An offense that occurred in the presence of an officer
- The discovery of contraband in the suspect's possession
- Emergency situations

The location of a person might also be relevant to whether an arrest is lawful. For instance, detainments and arrests at airports or border checkpoints might require a lower threshold of suspicion. In contrast, arrests in a person's home are more likely to require an arrest warrant.

Right to Be Informed of Charges

Once a person is arrested, he has a right to be informed of the charges brought against him in a prompt manner. The charges must be presented in a language the suspect can understand.

Right to a Fair Hearing

The ICCPR states that all people accused of crimes are entitled to a fair hearing before a court or other tribunal, and the results of the trial should be made public to protect the transparency of the criminal justice system. This right includes:

- Adequate time to prepare a defense
- The ability to be represented by legal counsel of the defendant's choosing and to freely communicate with counsel
- The right to have accusations and the procedures explained through a translator for free, if necessary
- The right to be tried for charges without undue delay
- The right to examine or have examined the witnesses against the accused
- Freedom from testifying against oneself or compelled confessions

Presumption of Innocence

Under the ICCPR, everyone accused of a crime shall be presumed innocent until proven guilty according to the law.

Right to Appeal

The ICCPR states that every person convicted of a crime should have the right to have both the conviction and the sentence reviewed by a higher tribunal.

Right to Privacy

Under the ICCPR, no one should be subjected to arbitrary or unlawful interference with privacy, family, or home correspondence or be subjected to defamation. Moreover, subjects should have the right to legal protection from such interference, whether from government or private parties.

The Charging Process

Once the government has arrested someone for a crime, the person under arrest must be formally charged with a crime by the filing of a charging document. Depending on the crime and the jurisdiction, the charging process will vary. But generally, if an accused is in custody, then there is usually a set time during which he must be presented to a judge or magistrate.

The judge will then decide whether to detain the accused, or release him, and on what conditions. If an accused is released under the condition that he deposits money or other valuable security with the court, he is posting bail. *Bail* is a money bond to ensure that defendants will show up for trial. If a defendant who is out on bail fails to show up for trial, the bond is forfeited, and a warrant for the defendant's arrest is issued.

Charging Documents

The criminal court process begins with the filing of a charging document, which contains a formal, written accusation of the crime.

Common Law Charging Documents

In many common law jurisdictions, there are two types of charging documents: the information and the indictment.

An information is sworn under oath by an informant, and an indictment is signed by the prosecuting counsel. In practice, informations are usually drafted by police officers, and indictments are prepared by prosecutors.

An *information* is an accusation made in writing and under oath before a justice in which the informant states that he has personal knowledge or that he believes on reasonable grounds that the accused person has committed an offense.

An *indictment* is an accusation in writing of a serious (that is, indictable) offense and is brought in the name of the government. Typically, it is a document used only after the accused has been admitted to stand trial following a preliminary inquiry, but it may also be used in the absence of a preliminary inquiry or where the accused has been discharged at a preliminary inquiry.

Civil Law Charging Documents

There are various types of charging documents used in civil law systems. Some call charging documents *indictments*, *petitions*, or something similar, but they are all functionally equivalent to indictments in common law countries in that they lay out criminal charges in writing.

However, some civil law systems have no such equivalent. In such cases, the closest thing to a charging document is most likely the defendant's arrest warrant, which should lay out the defendant's alleged violations. If a case goes to trial, the charges can also be found in the evidentiary report created during the examination phase of the criminal litigation process.

Prosecutorial Discretion and Bargaining Agreements

Whether criminal cases are actually brought to trial might depend on prosecutorial discretion, meaning that the decision to prosecute is left to the discretion of the appropriate jurisdictional authority. Prosecutors exercising this discretion consider issues like the potential for deterrence, the strength of the available evidence, and the resources (time, labor, money) incurred by going to trial.

All countries provide some measure of prosecutorial discretion; the prosecutor will not (theoretically) pursue cases for which there is no evidence. However, countries vary widely on how much discretion the government has to prosecute criminal cases. In the United States, for instance, the prosecutor has very wide discretion as to whether a person is prosecuted, and private citizens have little control over such decisions. In some jurisdictions, victims of crimes may commence "private prosecutions" if the government declines to do so on its own. Other jurisdictions, like Germany, give prosecutors almost no discretion and require them to prosecute any crime where there is sufficient evidence.

Another method of disposing of cases in a growing number of countries is through *bargaining agreements*, which occur when a defendant makes an agreement with prosecutors to plead guilty or submit a recorded confession in exchange for lesser charges or a reduced sentence. It is usually within the prosecution's discretion as to whether to offer a bargain. The goal

behind bargaining agreements is to make the criminal justice process more efficient by reducing the need for trials. The practice has become more popular in the last few decades, and many countries that previously resisted using bargaining agreements have introduced them in various circumstances. The bargaining process works differently in common law and civil law countries.

In most common law countries, a criminal defendant enters a plea before the court in response to the charges. The most common pleas available are *guilty* and *not guilty*. A plea of not guilty results in a full trial, whereas a plea of guilty results in a truncated trial to formally record the evidence and sentence the defendant. When the prosecution has substantial evidence of wrongdoing, criminal defendants often enter into a *plea bargain* before trial where, in exchange for pleading guilty instead of not guilty, the charges or sentence sought are less than they legally could be.

Most civil law countries do not have pleas, per se (there is no option for the defendant to enter a guilty plea), but there can still be bargaining agreements. A defendant can enter a confession, but the confession is submitted as evidence in an otherwise standard proceeding. However, a confession in evidence clearly reduces the difficulty of prosecuting the case, so an agreement among the prosecution, the defendant, and the court can be made to reduce the sentence in exchange for a voluntary confession. Bargaining agreements are controversial in many countries and are not as widely used in civil law jurisdictions as in common law jurisdictions. Additionally, when they are allowed in civil law jurisdictions, the circumstances under which they are available are typically more limited.

Defenses

A *defense* is an assertion by a defendant that seeks to explain away guilt (or liability for damages in civil proceedings). Whether a defendant can raise a defense depends on the offense and the existence and availability of defenses in the relevant jurisdiction. The more common defenses include:

- Alibi
- Consent
- Triviality of the offense
- Duress
- Entrapment
- Ignorance of facts

- Mistake
- Infancy
- Insanity
- Necessity of the act
- Protection of property
- Self-defense
- Public duty
- Legal impossibility
- Protection of others
- Statute of limitations (common law systems) or period of prescriptions (civil law systems)
- Court's lack of jurisdiction

In criminal fraud cases where intent is an element of the crime, defendants might advance a number of theories to excuse their guilt and hide the truth (e.g., by alleging some inhibiting factor that prevented the defendant from forming intent). For example, while ignorance of the law might not be an excuse, it can influence a fact finder at trial, particularly if the crime is complex and financial in nature (e.g., a tax evasion case in which the government used the net-worth method to prove the defendant's income). Some types of computerized embezzlements fit this category, too, as well as bank fraud, securities fraud, and price-fixing conspiracies. In short, while ignorance of the law might not be an excuse, it sometimes induces pity or sorrow.

Likewise, a defendant might attempt to use advanced age, sickness, and illiteracy to evoke sympathy. Such assertions are not generally considered proper legal defenses, but they might persuade the judge or jury to be lenient in sentencing.

The defenses that cause prosecutors the most headaches are assertions of poor investigative work (e.g., improper arrests, searches, seizures, and interrogations; improper handling and documentation of evidence; and privacy invasions). In fraud examinations, a defendant might make allegations of sloppy auditing and mishandling of work papers.

Also, the use of undercover operations in criminal investigations can lead to the use of entrapment defenses. *Entrapment* occurs when law enforcement officers or government agents induce a person to commit a crime that he is not previously disposed to commit. To make this defense, the defendant claims that the peace officer or undercover agent solicited,

encouraged, or incited the criminal act, and without that incitement, the defendant claims that he would not have committed the act.

Additionally, defendants might raise collateral matters, accusing investigators of libeling, slandering, and defaming them during the investigation.

The Trial Process

The Burden of Proof in Criminal Trials

The *burden of proof* is the evidence one party must present to prove each element necessary to establish the existence of a cause of action. In most jurisdictions, an accused person is presumed innocent until proven guilty according to law in a fair and public hearing of an independent tribunal, and in criminal trials, the government has the burden of proof with regard to the offense. The accused, theoretically, does not have to present any evidence. The burden is on the government to prove every element of the offense.

In criminal cases, the burden of proof is typically the highest level found in the jurisdiction, meaning it is as hard as or harder to prove a criminal case than an administrative or a civil proceeding. In most common law systems, the burden is phrased as *beyond a reasonable doubt,* and therefore, the verdict must be based on assurance beyond a reasonable doubt. Plainly put, beyond a reasonable doubt requires judges and jurors to be as sure as they possibly can be that the defendant committed the acts as charged to find him guilty. In purely philosophical terms, there might not ever be absolute certainty, but the reasonable doubt standard is lower than that.

Conversely, civil trials in common law systems typically only require a party to prove a case by a *preponderance of the evidence,* or "more likely than not," to support a decision; therefore, proving criminal violations requires stronger evidence than civil actions.

However, beyond a reasonable doubt is not a universal burden of proof for criminal trials. Most civil law systems that use an inquisitorial court process apply a different standard, sometimes called the *conviction intime* or *inner conviction of the judge*. It means that the fact finder needs to be convinced on an inner, deep-seated level. While this standard is still quite high, it

is generally thought to be somewhat less rigorous than beyond a reasonable doubt. Additionally, civil law systems typically do not change the standard between civil and criminal cases.

Fraud charges can be especially hard to prove because the evidence is by its nature overwhelmingly *circumstantial* (i.e., composed of documents and their interpretation versus the testimony of eyewitnesses).

The standard in criminal cases, whether the steady civil law system standard or the heightened standard in common law jurisdictions, entails making an assured judgment based on the evidence as presented. The appeals process recognizes that more than one examination of the charge(s) might be necessary to ensure an accurate, fair-minded verdict.

Participants in the Trial Process

Witnesses

In most common law systems, the accused person has the right to cross-examine any witness called by the government to give evidence, to call his own witnesses, and to testify himself. In general, the judge or jury is to give a verdict based only on the sum of this evidence given during the trial. Note that in most civil law jurisdictions, there is no right to cross-examine a party.

Generally, witnesses are only allowed to testify to their personal experience or observations regarding the facts at issue. That is, witnesses generally cannot testify to their own opinions or testify about statements made by others.

Expert witnesses, however, are allowed to give opinion testimony. Experts are allowed to testify if the judge feels that there is some issue in the case that may be difficult for jurors to understand and that the expert testimony would aid the jury.

Additionally, in some common law jurisdictions, a defendant in a criminal trial is entitled to call character witnesses on his behalf who often have no knowledge of the charges or facts at issue, but who are prepared to testify to the defendant's character. Such testimony must be given in the form of the witness's opinion or testimony as to the defendant's general good reputation; testimony as to specific incidents of good conduct is not permitted because such would prove too confusing and time-consuming.

The Prosecutor

The prosecutor is the government's representative and advocate in criminal trials. The job of the prosecutor is not to win, but see that justice is done. This means that the prosecutor should see to it that all relevant evidence and witnesses' testimonies are presented, even if favorable to the accused. Moreover, the prosecutor should treat all witnesses, including the accused, with moderation and fairness. In some civil law systems, the prosecutor's role in investigating criminal cases is replaced or shared with a judge or magistrate.

Defense Counsel

The defense counsel is the representative of the accused. The job of the defense lawyer is to make sure that the accused is not convicted unless evidence that is fairly and legally obtained proves the case. If the prosecution cannot prove its case beyond the applicable burden of proof (possibly because there is simply not enough evidence, or because the evidence was obtained illegally by the police), then the accused person is entitled to be acquitted.

The Judge

In criminal trials, the judge serves to make sure that the trial is conducted fairly and impartially and according to the rule of law. If there is no jury, then the judge will decide the issues based on the evidence submitted. But if there is a jury, the judge will instruct the jury on whatever parts of the criminal law apply to the case, and he will make sure they know that their decision must be made according to that law.

In common law jurisdictions, the judge presides while the prosecutor and defense attorney call witnesses and introduce evidence designed to prove the guilt or innocence of the accused. The judge's role is to be impartial and to serve as a referee over the parties.

In civil law systems, judges are more active participants, and are typically responsible for gathering evidence from the parties. Unless the civil law system allows for jury trials, the judge(s) also serves as the fact finder and decides matters of law.

Jury Selection

Both common law and civil law systems use juries to help decide cases, although the role of the juries and the methods in which they are selected usually vary from country to country.

Common Law System

Most juries in a common law criminal court consist of 12 or fewer jurors. The jurors are selected from the local population, often by a random lottery using voter registration records and the like. However, the jury that hears a criminal case is not required to reflect a cross-section of the community or contain individuals of the same race or age as the defendant.

While jury trials are typically used in criminal proceedings in common law jurisdictions, this is not always the case. For some cases, usually minor criminal offenses, a jury trial might not be available. In serious cases, however, jury trials are typically available. Additionally, many common law jurisdictions allow the defendant to waive the right to trial by jury. When no jury is present, the judge serves as the fact finder.

Potential jurors, however, may be dismissed, and there are three ways in which this may occur. First, a judge may exercise discretion and dismiss a juror upon his own initiative. This happens when a juror fails to meet the minimum qualifications or is otherwise unable to serve.

Second, a juror may be dismissed *for cause* (i.e., a request that a prospective juror be dismissed because his predispositions make him unfit to serve as a juror). A challenge *for cause* can be made on the following grounds:

- Name of the potential juror is not on its panel
- Juror is biased
- Juror has been convicted and sentenced to imprisonment
- Juror is an alien
- Juror is unable to perform his duties
- Juror cannot speak the official language in which testimony would be given

Third, in many common law jurisdictions, the prosecutor and the accused are each entitled to what are often called peremptory challenges. A *peremptory challenge* allows a litigant to remove someone from the jury panel without comment or justification (i.e., without giving cause). The number of peremptory challenges, however, varies according to the charge against the accused. The prosecution may not use its peremptory challenges in a way solely influenced by racial factors. The United Kingdom no longer allows peremptory challenges.

Additionally, either the accused or the prosecutor may challenge the entire jury panel on the ground of partiality, fraud, or willful misconduct on the part of the officer by whom the

panel was returned. The jury panel is the group of potential jurors. If a jury panel is challenged, the judge will determine whether the alleged ground of the challenge is true or not. If true, a new jury panel is returned.

Civil Law Systems

Juries are less frequently used in a civil law system; they are usually reserved for serious crimes, and some countries do not use them at all. Several civil law systems feature a mixture of judges and laypersons when juries are used. For instance, a panel could have three judges and nine laypersons who would decide the outcome of the case.

Alternatively, some countries (those following the German model) feature criminal trials with a panel of both professional and lay judges. These panels are unlike juries in the sense that they do not comprise randomly selected peers of the defendant, but they serve the similar fact-finding function of juries.

Unlike common law juries, civil law systems generally do not allow the parties to make pre-emptive strikes to eliminate jurors. However, the judge may typically replace jurors for bias or other valid cause.

Discovery

Discovery refers to the formal process whereby the parties to litigation collect evidence and learn the details of the opposing side's case. Criminal discovery practices vary considerably between adversarial jurisdictions (found in most common law systems) and inquisitorial jurisdictions (found in most civil law systems).

Adversarial Discovery Process

Recall that in adversarial jurisdictions, the parties involved in litigation primarily drive the discovery process, while the judge ensures that discovery procedures are followed correctly.

The adversarial process can be divided into the pretrial and trial stages. Most discovery between the parties is conducted in the pretrial stage. Both parties may request limited information from each other, and alleged failures to comply with evidentiary rules may be submitted to the judge, who may then order a party to comply. The prosecution, working with law enforcement, gathers all evidence on the government's behalf.

Some evidence, however, will not be available to a party until it is introduced as evidence during the trial by an opposing party.

Inquisitorial Discovery Process

The evidence-gathering process in inquisitorial criminal proceedings is quite different from adversarial proceedings. Criminal discovery in inquisitorial jurisdictions is driven by a judge. Some inquisitorial systems have two types of judges: the examining judge and the trial judge. *Examining judges* oversee the evidence-collection process in criminal proceedings, while *trial judges* preside over the trial. The trial judge presents evidence collected previously, questions witnesses, hears arguments, and makes rulings. In some jurisdictions, however, prosecutors share or replace the role of examining judges, while other jurisdictions have a single type of judge who is responsible for both overseeing investigations and performing trial functions.

The discovery process in inquisitorial jurisdictions occurs primarily in the first two of the three phases of criminal proceedings, which are the investigative phase, the examining phase, and the trial.

- In the investigative stage, the public prosecutor, judge, or both (depending on the jurisdiction's process) collect documentary and tangible evidence regarding the case. The investigating party then decides whether there is sufficient evidence to submit the case for prosecution.
- If there is sufficient evidence, the case moves on to the examining phase, which is mostly conducted in writing. The judge (an examining judge, if the jurisdiction uses them) completes a written record of the evidence and may also collect testimony and additional evidence. Some jurisdictions refer to this evidentiary record as the *trial dossier*. If the judge certifies that there is a valid case against the accused, the matter moves forward to trial.
- The trial commences with the exhibition of the examining record before the parties and the trial judge, jury, or panel. The parties argue their case before the trial judge (or jury, if applicable).

In inquisitorial trial proceedings, the evidentiary record or dossier is already available at the outset of the trial, whereas the entirety of each party's evidence is produced and recorded at trial in adversarial jurisdictions.

Disclosures

Criminal procedure for requiring parties to disclose information to each other also tends to vary in adversarial and inquisitorial jurisdictions.

DISCLOSURES IN ADVERSARIAL JURISDICTIONS

Generally speaking, discovery in adversarial jurisdictions is more secretive than in inquisitorial systems, especially in criminal cases. Both the defense and the prosecution typically have far fewer rights to access information possessed by the other party than parties in non-criminal litigation. The prosecution is heavily limited in disclosures it may obtain, and the defendant typically has the right to refuse to testify. The prosecution generally must obtain evidence through search warrants or other means, rather than requesting the items from the defendant. However, the defense might still be required to turn over certain types of evidence that it intends to use at trial, such as the basis for any legal defenses raised, documents or tangible items, results of tests intended to be used at trial, statements of expert witnesses it plans to use at trial, and other items as required by the laws of the jurisdiction.

The defense is similarly limited in what it may request from the prosecution. The defendant typically does not have a right to the work product of the state, which includes reports, memoranda, and other internal documents made by the government attorney in preparing for and prosecuting the case. However, most jurisdictions also require prosecutors to turn over all exculpatory evidence that would tend to refute the guilt or mitigate the punishment of the defendant.

DISCLOSURES IN INQUISITORIAL JURISDICTIONS

The evidence available in inquisitorial jurisdictions is substantially less private than adversarial jurisdictions. The entire record, as submitted by the judge presiding over the examining stage of the litigation, is provided to the parties before the trial phase commences. The defense has full access to the dossier on the case. Therefore, there is rarely an element of surprise, as all parties have examined what evidence is expected to be presented.

The judge may obtain the defendant's testimony, but the defendant usually has the right to remain silent. Since the discovery process is mainly the responsibility of the court, the parties do not submit pretrial discovery requests to each other, although they can request that the judge obtain certain items of evidence.

How a Trial Is Conducted

Most trial processes share many traits, but each court system has its own rules for how a trial should be conducted. The most obvious contrasts occur in the context of common law verses civil law systems. In common law systems, the trial phase consists of both the presentation of evidence and the determination of guilt or innocence. Later, there is a

separate sentencing hearing if the defendant is found guilty. In civil law systems, the evidence-gathering portion of the trial takes place separately from the decision of culpability and sentencing.

In many other regards, however, the processes are similar. A typical small summary trial is held in a courtroom, with very few people present. There will be a judge, a prosecutor, an accused person (with or without a defense lawyer), a court clerk (to handle the paperwork and keep a record), a sheriff's deputy (mainly for security), and possibly a few spectators. People who are going to be witnesses are usually kept outside once the trial begins, so they are not influenced by what others say in the witness box before them.

Once the judge is seated, everyone else may also sit, except when speaking to, or being spoken to by the judge. There will be microphones in front of the judge and the lawyers' tables, and in the witness box. In common law systems, a tape recording is made of everything that is said at the trial, so that a printed transcript can be made later if the verdict is appealed.

Once everyone is seated, the clerk will call the case, and the prosecutor will introduce himself to the judge. The defense then does the same and confirms that it is ready to go ahead with the trial.

At the start of the trial, there will be introductory talks by the judge and by lawyers for both sides. The aim is to lay out the framework of the case and, if applicable, make sure the jury has an idea of what the main issues will be and to suggest to them how they should evaluate the evidence that will be given, either through witnesses or in the form of exhibits.

In common law systems, the prosecution calls its witnesses first. Each witness is brought in, swears an oath (or makes a solemn declaration) to tell the truth, and is questioned by the prosecutor. Then the defense is given a chance to cross-examine the witness. Alternatively, in civil trials, the judge questions each witness directly and presents evidence from the examination report created prior to the trial.

Once all evidence has been presented, the normal procedure is for the judge to allow the defense to summarize what the evidence has shown and to argue for the judge or jury to acquit. The prosecutor then makes his own final points, trying to convince the judge or jury to convict. The prosecutor is held to a particularly high standard during the closing

arguments. Generally, he may not misstate the evidence, express a personal opinion as to the defendant's guilt or the credibility of witnesses, or otherwise make prejudicial or inflammatory remarks. The prosecutor is expected to stick to the facts and to the reasonable inferences that can be drawn from them.

Occasionally in common law trials, the judge may "direct" a verdict of not guilty on one or more charges. A judge will direct a verdict if no evidence was presented in relation to some aspect of the charge, or for some other reason that makes a guilty verdict not legally possible. If that happens, the jury will be told not to consider that charge. If there is a charge on which the judge has not directed a verdict, the jury will then retire to consider it; otherwise, they will be released.

Reaching a Verdict

Common Law Systems

In common law systems, a jury is usually the independent fact finder in serious criminal cases. There are often questions that come up in the jury room, about the evidence or the law, and the foreperson will relay these back to the judge via the sheriff. Usually, the judge will answer questions by having the jury come back into court.

In reaching a verdict in a criminal trial, the jury must be unanimous, meaning that every juror must agree with the verdict**.** A simple majority is not sufficient for a verdict of guilty. The requirement of unanimity is designed to prevent the conviction of innocent people—an aim that is vital to the preservation of the justice system.

If there is still disagreement after the jury makes a full discussion and considers the evidence, then the foreperson should inform the court that the jury cannot reach a verdict. The judge may call the jury back into the courtroom for more instructions, but it is improper for him to push the jury too hard for a verdict where there is genuine disagreement.

When the jury is unable to reach agreement (what is called a "hung" jury), the judge will generally discharge the jurors and declare a mistrial. If there is a mistrial, the defendant can be retried if the prosecution elects to do so.

Civil Law Systems

Ordinarily, a judge is the sole fact finder in a civil law system and renders the verdict after considering all the evidence presented. When a jury is present, they discuss and make decisions along with the judges, so there is no need for formal consultations.

Additionally, the unanimity requirement in common law systems is not present in most civil law jurisdictions. The minimum requirement is typically somewhere above a simple majority, such as 10 out of 12 jurors, but the requirement may vary among jurisdictions.

Sentencing

Following a verdict of guilty, the judge and/or jury, as applicable, must impose a sentence.

When a defendant is convicted of a crime, courts in common law systems typically hold a sentencing hearing to determine the manner in which the defendant will serve his sentence, but before the sentencing hearing, a government worker will prepare a *pre-sentence report* that will review the defendant's character, background, associates, prior criminal record, and other factors relevant to setting an appropriate sentence. The report is designed to assist the sentencing judge in assessing punishment. Additionally, the pre-sentence report may contain a *victim impact statement*; that is, an assessment of the financial, social, psychological, and medical impact upon, and cost to, the victim of the crime.

While evidence of the defendant's prior convictions are not typically admissible during the trial phase in common law jurisdictions, the defendant's criminal record is relevant and admissible in sentencing (i.e., such evidence is admissible when determining the defendant's punishment, not guilt). However, if a defendant testifies on his own behalf in a criminal trial, he is typically subject to cross-examination just like any other witness, and the prosecution can impeach his credibility by showing prior convictions.

Civil law systems typically do not provide for a separate hearing for sentencing. The decisions of guilt and punishment are made and announced together, and prior convictions are admissible evidence.

Appeal

In most jurisdictions, a convicted individual has the right to appeal the trial court's decision. An *appeal* is the procedure for obtaining review by a higher court to assure that the trial was conducted in a lawful manner and that the judgments comply with the law. In an appeal, the appealing party petitions an appellate court to overturn or modify the lower court's decision. The appellate court can reverse a conviction if the error denied the defendant a fair trial.

Another divergence exists between common law and civil law systems in their appellate processes. In most common law countries, appellate courts consider potential errors of law *de novo* (meaning they evaluate them independently of the trial court's determinations), but generally adopt the factual findings of the trial court. No jury is present, and there is typically no new evidence entered into the record. Therefore, appeals in common law systems are typically limited to issues of law. Very rarely will an appellate course reverse a factual finding of the trial court in a common law jurisdiction, such as when there is an egregious and obvious mistake.

In most civil law systems, courts can review cases for both issues of fact and law. The appellate court can usually perform *de novo* reviews of both the factual and legal determinations by evaluating the compiled evidentiary dossier.

Generally, convictions may be appealed if the appeal is filed in a timely manner and based on proper grounds.

Punishment

When a defendant is found guilty of a crime, there are a variety of sanctions available. The court may impose any combination of imprisonment, probation, restitution, forfeiture, restitution, and fines.

Corporate Criminal Liability

In many jurisdictions, corporations and similar business entities may be *vicariously liable* (the absolute liability of one party for the misconduct of another party) for criminal and civil violations. Most common law systems follow the doctrine of *respondeat superior* ("let the master answer"), which holds that a business entity is liable for the acts of their employees if

those acts occur within the scope of employment and with some intent to benefit the corporation. Therefore, the employee needs to have committed each element of the crime for liability to be transferred to the corporation.

While civil law systems originally did not allow for the criminal liability of legal entities under the doctrine of *societas delinquere non potest* ("societies cannot offend"), some countries (such as France) have recently amended their laws to allow corporations to be criminally liable for the acts of employees. However, not all civil law countries allow for such liability (such as Germany), relying instead on administrative and civil penalties for business entities.

Of the jurisdictions that recognize corporate criminal liability, they either allow a corporation to be criminally liable for virtually every crime that an individual may be liable for, or they have an exclusive list or description of violations for which corporations may be liable.

Generally, vicarious liability is very broad and imposes liability on a corporation even if those in management had no knowledge or participation in the underlying events. Moreover, the acts of any employee, from the lowest clerk to the CEO, can impute liability upon a corporation, and a corporation may be liable for the acts of its employees that violate security laws, banking laws, anti-bribery laws, and many others.

To establish criminal liability for some crimes, the government must prove that the defendant acted with a wrongful mental state (i.e., a "guilty" mind). This intent can be attributed to companies, despite the fact that they are artificial entities. When a corporation is being charged with a crime that requires proof of a mental state, the moving party must only show that the agent who committed the wrongdoing had the required state of mind. Thus, the required mental state is attributable to the corporation. For example, to impose liability against a company for fraud, the moving party must prove that an agent of the company made the alleged false statements with specific intent to defraud.

Liability of a Corporation's Directors and Officers

The current legal environment in many jurisdictions imposes civil and criminal liabilities on a corporation's directors and officers. Generally, director and officer liability stems from the certain duties imposed by law to their corporation. The duties, which are discussed in more detail below, are as follows:

- *Duty of loyalty*. Directors and officers must act solely in the best interest of the employer/principal, free of any self-dealing, conflicts of interest, or other abuse of the principal for personal advantage.
- *Duty of care*. Directors and officers must conduct business affairs prudently with the skill and attention normally exercised by people in similar positions.
- *Enumerated duties*. Some jurisdictions have numerous laws to regulate directors' and officers' actions and decisions regarding the management of their companies, including securities laws, antitrust laws, racketeering laws, tax laws, intellectual property and patent laws, and corporate laws.

Corporate Deferred Prosecution Agreements

Of the jurisdictions that allow for corporate criminal liability, some also use deferred prosecution agreements. Generally, *deferred prosecution agreements* occur when prosecutors file criminal charges against a company, but then agree not to prosecute the claims as long as the company successfully complies with the deferral agreement's terms. These requirements typically focus on getting the business to reform its policies and reduce the risk of illegal practices. Essentially, deferred prosecution agreements help companies avoid indictment, trial, and conviction while providing a jurisdiction's justice system with another channel for disposing a corporate case that punishes malfeasance and effectuates changes in a company's culture.

Similar to plea bargaining, deferred prosecution agreements are controversial, and many countries do not provide for such resolutions of criminal cases. However, the complexity and public cost of trying massive fraud cases has led to more jurisdictions adopting such strategies.

MENU

THE CIVIL JUSTICE SYSTEM

Introduction

This section reviews the legal aspects of actions by private parties—including fraud examiners, auditors, accountants, security personnel, private investigators, and lawyers—to investigate and recover losses due to fraud. Many of these cases will end up in the civil justice system.

A *civil action* or civil suit arises when individuals or business entities (such as corporations or partnerships) disagree on a legal matter. A civil action usually involves a dispute over something (such as the terms of a contract) or a claim that one party has violated a legal duty owed to it by the other party. In a fraud case, the victim may be able to seek compensation from the fraudster in a civil action based on common law fraud, breach of fiduciary duty, or misrepresentation. The person who sues is called the "plaintiff" and the person being sued is called the "defendant."

Procedure in Civil Cases

The procedure in a civil case can be quite complex. Furthermore, the terminology describing steps in the process is not consistent in legal systems throughout the world. This discussion focuses on jurisdictions that follow the three phases of civil litigation: pleadings, discovery, and the trial itself.

Beginning the Civil Action

Fraud examinations often begin before litigation occurs, but since fraud examiners should work with an eye toward potential litigation, it is helpful to understand what is necessary to begin this process. A civil action begins when the plaintiff files a pleading with the appropriate court, usually in the jurisdiction in which the defendant resides or where the claim arose. The pleading sets out the complaint against the defendant and the remedy that the plaintiff is seeking. Depending on the practice and procedure of the court in which the action is commenced, such a document may be called a writ of summons, a statement of claim, a declaration, or an application.

The required contents of the plaintiff's pleadings vary somewhat between jurisdictions, but most jurisdictions require *fact pleadings*, meaning the plaintiff must identify:

- The grounds for legal relief
- A summary of the evidence
- The specific facts on which the party's claim relies
- Key items of expected evidence

Some jurisdictions have elevated pleading requirements, and also require witness lists and the production of specific documents.

A minority of jurisdictions require simpler *notice pleadings*, in which the facts in the pleading must merely put the defendant on notice of the alleged claims, but do not need to include the specific facts underlying the case.

When a pleading is filed, a court officer "issues" the claim. This is done by affixing the seal of the court to the pleading and signing the document on behalf of the court. Copies, as issued, are then delivered to (or "served on") the defendant.

Once the originating document is delivered to the defendant, the defendant must, within a specified period, provide the court with a statement of defense in response to the originating document. If the defendant fails to do so, he risks losing the suit by default. That is, if the defendant does not respond within the specified period, the defendant forfeits the case, and the court issues a default judgment holding the defendant liable as it deems fit. When making a default judgment, the court assumes that because the defendant did not put up a defense, the allegations must be true.

The liability assigned in a default judgment usually is limited to the relief requested in the plaintiff's complaint because it would be unfair to hold the defaulting defendant to a higher liability than that of which he had notice in the complaint that was served on him.

In addition to allowing defenses against the plaintiff's claims, many jurisdictions allow the defendant to raise *counterclaims* (also known as *countersuits*), in which the defendant levels a claim against the plaintiff. The specifics of the counterclaim might be filed as part of the defendant's answer or as a separate document. If a defendant files a counterclaim, it and the original complaint will be tried concurrently, with the final judgment stipulating a decision on each side's claims.

Preservation of Evidence

Most civil litigations concerning fraud involve many documents, tangible items, or digital information that might serve as evidence. Each jurisdiction has rules for how potential evidence should be handled.

Generally, common law jurisdictions impose a duty on parties in civil litigation to take affirmative steps to preserve relevant evidence, and this duty might arise prior to the commencement of litigation. For litigation occurring in common law courts, the duty to preserve relevant evidence typically arises when the litigation in question is reasonably anticipated. For instance, if a company receives a letter from a vendor that alleges a credible allegation of fraud and a threat to sue, the company's duty to preserve evidence has most likely arisen.

In contrast, civil law countries tend to have a more narrow scope of what evidence is required for litigation. Typically, the issue of when to take affirmative steps to preserve evidence is established by the court, meaning the court dictates what evidence must be preserved and produced by the parties or others with relevant information. Due to privacy requirements in many civil law jurisdictions, retaining personal information (a very broad class of information regarding individuals) for longer than necessary might be illegal without a court order. Some civil law jurisdictions allow a party to apply for a court order to preserve evidence prior to a lawsuit being filed.

The duty to preserve evidence can be a confusing concept, especially in the context of litigation between parties in different countries or parties with information stored in foreign countries. For instance, the United States and other countries require parties to issue *litigation holds* within their organization when litigation is anticipated, which freezes the regular destruction of documents and information. However, if the litigation hold is followed regarding information stored in countries with strong data privacy laws—particularly members of the European Union—there is the potential for a criminal violation of such laws. Therefore, fraud examiners should consult with legal counsel on how to preserve evidence gathered during an examination.

Gathering Evidence

After the parties submit pleadings to the court, the evidence-gathering process begins. The system for collecting evidence varies from country to country, especially along the lines of

adversarial processes (generally common law systems) and inquisitorial processes (generally civil law systems).

Common Law Systems

After statements of claim and defense are filed in common law jurisdictions, each party is entitled to pretrial discovery. *Discovery* refers to the formal process whereby the parties collect evidence and learn the details of the opposing side's case, and pretrial discovery is intended to clarify the claim against the defendant, and to permit each side to examine the evidence that will be used in court by the other side.

In most common law jurisdictions, each party must file an *affidavit of documents*, or *affidavit of records*, which lists and describes all documents in its possession that are relevant to any matter at issue in the case. The party filing the affidavit must allow the other party to inspect or copy any such documents. If any of the documents are privileged, the privilege should be asserted in the affidavit of documents. If requested, the judge will examine the documents to determine if the privilege applies. Some of the more common privileges include:

- *Litigation privilege.* This privilege protects communications or documents prepared in anticipation of litigation.
- *Attorney-client or solicitor-client privilege.* This privilege protects information provided by the client to the solicitor which is necessary in order to obtain legal advice.
- *Settlement negotiations.* Pretrial settlement negotiations are also privileged.

Some jurisdictions also allow the parties to make a request for documents or records, in which they ask another party to turn over a specific document or other record.

A party may be examined or questioned by the other party either orally or by written questions. In Canada, this procedure is referred to as *examination for discovery*; in the United States, an oral examination for discovery is referred to as a *deposition* and a written examination is referred to as an *interrogatory*. However, other common law jurisdictions might not allow for pretrial oral discovery, although written pretrial discovery is still available.

An oral examination, or deposition, is sworn testimony given by a party or witness upon questioning by counsel for one of the parties before trial and outside of court, usually in a lawyer's office. Opposing counsel and a stenographer, who administers the oath and transcribes the testimony, also are present. An oral examination may be used to obtain evidence about the party's own or the opponent's case, or to preserve testimony for trial.

Often, a party has the option of an oral or a written examination, but not both without court approval. In some jurisdictions, however, discovery by interrogatories can be conducted without forfeiting a party's right to an oral examination.

In contrast, a written examination for discovery, or interrogatory, is simply a list of questions that the party, usually through a lawyer, is required to answer in writing. Written examinations are less expensive than oral examinations, but they are usually not as productive. Some parties will try to provide as little information as possible but still give a "truthful" answer. Moreover, counsel often finds ways to avoid answering questions or to provide minimal information.

Generally, the collection of oral or written testimony in the pretrial stage does not remove the need for such testimony to be presented during trial. A witness in a pretrial oral examination would also need to testify at trial, barring some exception to the rules.

Civil Law Systems

One of the most significant differences between the adversarial process of most common law jurisdictions and the inquisitorial process of most civil law jurisdictions is the way in which evidence is collected. Again, adversarial processes are largely driven by the parties to a suit, whereas in inquisitorial processes, the judge is the driving force. In other words, instead of the parties seeking evidence from each other, the judge seeks evidence from the parties and other sources.

In the inquisitorial process commonly found in civil law jurisdictions, the evidence is gathered contemporaneously with the trial, as opposed to the common law method of having the parties gather evidence over time and enter it into the record all at once during the trial stage. Civil law legal systems tend to value documentary and written evidence over oral testimony. When witnesses give testimony, the judge orchestrates the questioning instead of the parties. The judge is also responsible for collecting documents and physical evidence.

Many civil law systems have *professional secrecy obligations*, which require members of certain professions to maintain the confidentiality of information obtained from clients in the course of those services. This obligation is similar to the attorney-client privilege, and legal representatives of the parties generally may refuse to provide testimony or produce documents covered by the secrecy obligation.

While the parties' attorneys or advocates are still involved in the evidence-gathering process, they play a more advisory role, such as formulating questions for the judges to ask and making recommendations on how to interpret the evidence. The judge orchestrates the proceedings by calling witnesses and eliciting testimony, as well as collecting documents and physical evidence.

Rather than keep a verbatim record of witness testimony, the judge makes a synopsis of the evidence that will later be used in the decision-making portion of the trial. Typically, the trial record consists of the judge's summaries of evidence, as opposed to every document or item of evidence submitted. However, key documents or particularly important statements might be included. The parties also work to ensure that the judge accurately creates the trial record and argue to frame it in a way that represents their interests.

Civil Trials in Common Law Jurisdictions

The trial process in common law jurisdictions can most easily be divided into two phases: the pretrial stage and the trial stage. Beyond discovery that occurs in the pretrial stage, much of what occurs in the trial stage depends on the results of the pretrial process.

Pretrial Stage

Civil cases often involve pretrial motions in which the parties ask the court to rule on a number of issues that relate to how the trial will be conducted.

A common pretrial motion that occurs during, or at the conclusion of, the discovery process asks the court to decide the case without a trial, based on the evidence contained in the complaint and answer. In several common law jurisdictions, this motion is referred to as a *motion for summary judgment*. This motion will be granted if the court determines that the pleadings and proof clearly demonstrate that there is no genuine material issue of fact involved in the proceedings and that the moving party is entitled to judgment as a matter of law. Motions for summary judgment generally are not favored by the court, as they terminate the proceedings before trial and the moving party bears a heavy burden to demonstrate that there are indeed no circumstances, factually or legally, under which the opposing party could possibly be entitled to relief. If the granting of a motion for summary judgment disposes of all the issues between the parties, the case ends, although the opposing party may appeal. If the motion is denied, the case proceeds to trial.

Other pretrial motions may involve requests:

- Seeking an order to secure assets before trial and prevent the defendant from disposing of the assets while the lawsuit is pending
- Asking the court to seize and take custody of property that is subject to the dispute
- Seeking an order preventing a defendant or a third person in possession of assets claimed by the plaintiff from transferring, dissipating, wasting, damaging, spending, concealing, or otherwise hindering the plaintiff's claimed interest in the property
- Requesting the court to rule that evidence is inadmissible, prohibiting opposing counsel from referring to or offering the evidence during trial
- Requesting the court to dismiss the charges based on a defect in the complaint
- Seeking a change of venue for the proceedings due to improper procedure, unfair prejudice, or similar reason

Trial Stage

The purpose of a civil trial is to determine whether there is some basis upon which the plaintiff is entitled to a remedy from the defendant and, if so, what the appropriate remedy might be. To achieve this purpose, the jury (or in cases tried without a jury, the judge) must listen to both sides and determine the facts of the case. When juries are used, the requirements are typically less stringent than in criminal trials. For instance, it is common for the minimum number of jurors to be lower for civil cases. Additionally, civil trials might not require a unanimous verdict from the jurors in some situations.

Generally, in a civil suit in common law jurisdictions, the plaintiff must prove that it is more probable than not that the defendant is liable. This standard is sometimes referred to as the *preponderance of evidence* in common law jurisdictions. The plaintiff does not have to prove liability beyond a reasonable doubt, as in a criminal case.

In the adversarial process present in most common law jurisdictions, the trial begins with the plaintiff presenting the evidence against the defendant. The plaintiff calls witnesses to testify as to facts, and present documents, photographs, or other kinds of evidence. The defendant may then cross-examine the plaintiff's witnesses to test their evidence. Once the plaintiff has presented his case, the defendant can present his own evidence, which may include calling witnesses, and the plaintiff can cross-examine the defendant's witnesses.

Expert testimony is another common facet of trials—especially for technical cases like white-collar crimes. In adversarial settings, civil parties may call expert witnesses to give their

opinion on matters thought to be too technical for the judge or average juror to understand. Fraud examiners and accountants may be used as experts in cases to compute and testify to damages. In most trials, each side will produce a qualified expert who disagrees categorically with everything the expert for the other side says. Because the jury usually learns through cross-examination that each expert has been paid for preparation and trial time—and because jurors generally have a difficult time understanding and evaluating expert testimony—such testimony may have little effect on the outcome of the trial.

Throughout the trial, the judge must ensure that all of the evidence presented and, in adversarial proceedings, that all of the questions asked are relevant to the case. For example, in most situations, the judge will not allow *hearsay evidence*—testimony based on what a witness heard from another person that is offered to prove that the assertion made by the other person is true—because such evidence lacks reliability.

At the conclusion of the trial, both the plaintiff and the defendant present a summary of their arguments, and the judge or jury must then consider the evidence presented and make a decision that is based on what the evidence shows to be most probable.

Civil Trials in Civil Law Jurisdictions

Civil cases in civil law jurisdictions vary considerably compared to common law civil cases. The most obvious difference is that civil law trials are a continual series of meetings and written correspondences, rather than a single event, as in common law systems. Throughout the series, evidence is introduced and evaluated by the court, and motions are submitted and decided on by the judge. The division between pretrial and trial stages found in common law civil trials, therefore, does not apply in the typical civil law setting.

The standard of proof in civil law jurisdictions typically does not change in criminal and civil trials; it is often described as the inner conviction of the judge, sometimes called the *conviction intime* standard. This standard requires stronger evidence than the common law *preponderance of evidence* standard, but not as much as the common law *beyond a reasonable doubt* standard.

The judge chooses an expert (usually only one per issue) to give testimony on a subject and make expert findings on behalf of the court. The idea is that court-appointed experts are less biased than those that are hired by the parties. Some civil law jurisdictions allow (or require) the parties to provide expert witnesses to provide input for the court's appointed expert. The

court has the discretion to reject or accept the appointed expert's findings, but in practice the court usually accepts them.

Throughout the trial, the judge is evaluating evidence and recording it in the trial record. The record is generally a summary of the evidence, rather than a word-for-word transcript of the proceedings. At the final hearing, the judge rules on the admissibility and relevance of the evidence in the record and presents it. This final hearing is usually the closest singular meeting resembling the trial stage in common law jurisdictions. After presenting the evidence in court, the judge, jury, or judge panel (depending on the jurisdiction and type of case) rules on the issues in the case.

Civil Appeals

Generally, both sides may appeal from an adverse verdict, either as to liability or damages.

In common law systems, the appellate court is largely limited to reviewing the legal decision of the trial court, rather than the factual determination of the judge or jury. The appeals court may reverse and remand for a new trial on some or all of the issues, order that a certain portion of the awarded damages be remitted, or enter final judgment, if legal grounds are clear, in favor of either party.

In most civil law systems, the appellate court may review issues of both law and fact, meaning it may obtain additional witness testimony, gather new documentary evidence, obtain new expert opinions, and so forth. The appellate court may reverse, affirm, remand for additional proceedings, and (in some jurisdictions) modify the trial court's decision.

Decisions and Remedies in Civil Cases

If the defendant in a civil case is found to have done nothing wrong, the judge will dismiss the case, but if the defendant is found liable, the plaintiff is entitled to some sort of remedy. In general, the term *remedy* refers to any process, procedure, or consequence of a legal wrong by which a victim can be redressed for his loss. Thus, if the defendant is found liable in a civil case, the remedy to which the plaintiff is entitled must be considered.

Legal Remedies

The remedy to which the plaintiff is entitled, however, depends upon a number of factors, such as the relief sought, the facts, and the authority given to the court to grant specific

relief. There are various types of civil remedies, but the following three are most common: monetary remedies (damages), declaratory remedies, and equitable remedies.

Damages are remedies for the victim's recovery of money from the defendant because of, and as compensation, reimbursement, or reparation for, the defendant's legal offense. Damages are the remedy most commonly available to the successful plaintiff, and the main purpose of damages is to compensate the plaintiff for the loss caused by the defendant.

The amount of damages is normally fixed by the judge or jury that decided the case, unless a statute proscribes a particular amount. In fixing damages, the judge or jury will take into account the out-of-pocket expenses incurred by the plaintiff and, where the law permits such recovery, an additional lump sum to compensate the plaintiff for the loss suffered and the loss that might be suffered in the future as a result of the wrongdoing of the defendant. Although the judge or jury may take into consideration the amount demanded by the plaintiff in the originating document, they are not required to award that amount: they are free to award substantially less than the amount claimed.

In some jurisdictions, a court may occasionally award *punitive* or *exemplary* damages in addition to those that would ordinarily be payable. Such damages are usually awarded when they are made available by statute or, in most jurisdictions, when the judge or jury feel that the conduct of the defendant was so reprehensible that an increased award is required to express the disapproval of the community. Punitive damages tend to be available in common law systems, although a few civil law countries allow them in very limited circumstances.

Declaratory remedies are those in which the court states or declares the rights of the parties. For example, when a court interprets a will or a contract, its decision is declaratory in nature. Similarly, the decision of a court as to the ownership of personal property or land is also declaratory.

Equitable remedies are remedies used when the legal remedy by itself would be inadequate compensation for the wrong suffered. That is, equitable remedies are used when the plaintiff has no adequate remedy at law (i.e., damages are inadequate). One of the primary equitable remedies is the *injunction*, which is a court order by which a party is required to perform, or is restrained from performing, a specific act.

Fidelity Insurance

Given the prevalence of fraud, and given the fact that it is difficult to fully recover losses from fraud, many businesses have fidelity insurance that covers fraud losses. Fidelity insurance (also known as *crime insurance* and *employee dishonesty insurance*) is an often-overlooked method of recovery for losses due to internal fraud. *Fidelity insurance* is a type of insurance under which the insured entity is covered against losses caused by the dishonest or fraudulent acts of its employees.

Dishonest or fraudulent acts typically are defined as those acts committed with the intent to:

- Cause the insured to sustain a loss.
- Obtain a financial benefit for the employee, or for any third party intended by the employee, other than his proper compensation.

Fidelity insurance is likely to cover internal fraud or theft. Typically, fidelity insurance will provide coverage in cases of employee theft, forgery, fund transfer fraud, computer fraud, money order fraud, counterfeit currency fraud, credit card fraud, and so on.

It is often helpful for organizations to have fidelity insurance, since general liability insurance and many other policies will not cover damages from intentional acts like internal fraud.

As with any other insurance agreement, fidelity policies have deductibles (a reserved amount that is subtracted from the total loss claimed), policy limits (a limit to the amount the insurance company will indemnify the insured for a given loss), , and certain exclusions.

To collect on a fidelity insurance policy, the insured must submit a sworn proof of loss claim within specified time limits, together with supporting evidence of liability and the amount of loss. Submitting a timely proof of loss is the responsibility of the insured; the carrier will not conduct nor assist in any investigation efforts to obtain proof of a loss, and the carrier will not reimburse the investigative or legal costs that the insured incurred in making a claim.

Most policies have express subrogation provisions providing that if the insurance company pays a claim, it acquires the rights of the insured to sue the wrongdoer. Policyholders are prohibited from interfering with these rights in any way at the risk of jeopardizing coverage, such as releasing the wrongdoer from liability. Therefore, no settlement agreements or releases should be executed with a dishonest employee or any confederate unless the insurance company consents.

MENU

Alternative Dispute Resolution

A growing trend in civil litigation is to allow or encourage parties to an action to resolve their disputes without the necessity of a trial. *Alternative dispute resolution* is the term used to refer to these processes. In fact, not many cases actually go to trial; most are settled out of court or go though some kind of alternative dispute resolution.

Alternative dispute resolution has certain advantages over litigation. It helps preserve existing business relations between the parties, it provides more flexible remedies, and often, but not always, it is less costly.

Alternative dispute resolution in fraud cases usually involves one of two types of methods: mediation or arbitration.

Mediation

Mediation is the process whereby an impartial third person assists the parties in reaching a resolution of the dispute. The mediator does not decide who should win, but instead works with the parties to reach a mutually agreeable settlement. Any mediation agreement will be enforced as a binding contract.

Arbitration

Arbitration is the process whereby a dispute is submitted to an impartial third person (known as an *arbitrator*) who then decides the outcome of the case (i.e., which party should win). The arbitrator acts as a judge or jury by deciding the case on its merits. Arbitration can be either binding or nonbinding. If the arbitration is binding, then the decision of the arbitrator is final, and the parties cannot later submit their dispute to a judge or jury for determination. Conversely, if the arbitration is nonbinding, the arbitrator's determination is not binding upon the parties.

Today, many contracts contain arbitration clauses providing that if a dispute arises between the parties to the contract, both parties agree to submit their claims to binding arbitration rather than filing suit. Additionally, parties might agree to have the laws of a particular jurisdiction apply during the arbitration, and these provisions are often enforceable.

BASIC PRINCIPLES OF EVIDENCE

Definition of Evidence

In general, evidence consists of anything that can be used to prove something. In a legal sense, *evidence* means an assertion of fact, opinion, belief, or knowledge, whether material or not, and whether admissible or not.

Evidence refers to an intricate set of principles, developed and refined over hundreds of years, that is designed to ensure that only relevant and probative evidence is admitted in court proceedings, and that irrelevant, unreliable, and prejudicial evidence is excluded so that cases can be fairly and expeditiously decided.

Every aspect of trying a case—from filing the complaint through discovery, into the presentation of witnesses and exhibits—is affected by rules of evidence. This body of law covers not just what counts as evidence, but how that evidence is gathered, handled, and presented.

In every jurisdiction, the law of evidence governs the admissibility of evidence in legal proceedings. The law of evidence, however, varies between countries and legal systems. Common law legal systems have separate rules of evidence that regulate the admission and evaluation of evidence by courts. For example, evidence in U.S. federal courts is governed by the Federal Rules of Evidence (FRE). These rules set out what can and cannot be introduced during a dispute. In the late 1960s, a U.S. Supreme Court panel began codifying centuries of common law into the FRE. What had previously been a far-flung set of precedents, buried in local jurisdictions and lengthy appellate court decisions, was gathered into a singular body of information. The FRE became law in 1975. Likewise, in Canada, the Canada Evidence Act regulates the rules of evidence in court proceedings under federal law. Civil law legal systems, however, do not have a separate code of evidence law.

The rules of evidence can be complex, and counsel should be contacted if an important question of evidence arises in the course of a fraud examination. Additionally, rules of evidence vary by jurisdiction, even within the same country. For example, in the United States, state courts have different rules for the admissibility of evidence than do federal courts. The following are some general principles regarding evidence; however, fraud examiners should always review the rules for their area.

Three Basic Forms of Evidence

Evidence can be anything perceptible by the five senses, which is invoked in the process of arguing a case. Documents, spoken recollections, data of various sorts, and physical objects are all potentially evidence. Put differently, evidence is simply anything that relates to the proving or disproving of a fact that is of consequence to a case. With the known universe available for court inspection, legal authorities have narrowed the field by setting up categories to evaluate evidentiary significance.

There are three basic forms, as distinguished from types, of evidence: testimonial, real, and demonstrative. *Testimonial evidence* refers to the oral statements made by witnesses under oath. In general, there are two types of testimonial witnesses: lay witnesses and expert witnesses. A *lay witness* (or *fact witness*) is a nonexpert witness who must testify from personal knowledge about a matter at issue. An *expert witness* is a person who, by reason of education, training, skill, or experience, is qualified to render an opinion or otherwise testify in areas relevant to resolution of a legal dispute.

Real evidence refers to physical objects that played a part in the issues being litigated. The term includes both documentary evidence—such as canceled checks, invoices, ledgers, and letters—as well as other types of physical evidence. Therefore, a printer in a case involving questioned documents is clearly real evidence, as is a tape recording since members of the court can experience the sounds firsthand.

Demonstrative evidence is a tangible item that illustrates some material proposition (e.g., a map, a chart, or a summary). It differs from real evidence in that demonstrative evidence was not part of the underlying event; it was created specifically for the trial. Its purpose is to provide a visual aid for the fact finder. Nonetheless, demonstrative evidence is evidence and can be considered by the fact finder in reaching a verdict.

Direct Versus Circumstantial Evidence

There are two basic types of admissible evidence: direct evidence and circumstantial evidence. *Direct evidence* is evidence that tends to prove or disprove a fact in issue directly, such as eyewitness testimony or a confession. *Circumstantial evidence* is evidence that tends to prove or disprove facts in issue indirectly, by inference. Many fraud cases are proved entirely by circumstantial evidence, or by a combination of circumstantial and direct evidence, but seldom by direct evidence alone. The most difficult element to prove in many fraud cases—

fraudulent intent—is usually proved circumstantially, and necessarily so, because direct proof of the defendant's state of mind, absent a confession or the testimony of a co-conspirator, is impossible.

The distinction between direct and circumstantial evidence, however, is more significant in common law systems than in civil law systems; in trials held in civil law systems, the court weighs all relevant evidence, regardless of type, to reach its decision.

Admissibility of Evidence

Not all evidence is admissible. To be admissible, evidence must satisfy certain requirements. But because civil law systems do not rely on juries like common law systems, there is a relative lack of restrictions on the admissibility of evidence in civil law systems. Thus, there are far fewer limitations on the admissibility of evidence in civil law systems than in common law systems.

In common law systems using *adversarial processes*—those in which the litigating parties drive the discovery process—questions involving the admissibility of evidence occur when one party objects to another party's offer of evidence. If a judge sustains an objection, the evidence is not admitted. If, however, the judge overrules the objection, the evidence is admitted and can be considered by the fact finder.

Relevant

The admissibility of evidence largely depends on the discretion of the presiding judge, but a basic requirement of admissibility in both common and civil law systems is that evidence must be relevant. To be admissible in common law systems, evidence must be relevant to material issues in dispute. In civil law systems, evidence is admitted if the presiding judge determines it is relevant.

For example, in the United States, a common law country, the general rule is that all relevant evidence is admissible. Rule 401 of the Federal Rules of Evidence defines *relevant evidence* as evidence "having any tendency to make the existence of any fact that is of consequence to determination of the action more probable or less probable than it would be without the evidence."

Evidence is *relevant* if it tends to make some fact at issue more or less likely than it would be without the evidence. The facts in issue, of course, vary according to the case, but generally can be said to be those that tend to prove the essential elements of the offense or claim, as well as related matters such as motive, opportunity, identity of the parties, and credibility.

Whether a particular piece of evidence is relevant or not depends on what the evidence is offered to prove. An item of evidence might be relevant and admissible if offered to prove one thing, but not relevant and inadmissible if offered to prove something else. For example, evidence of other crimes, wrongs, or acts committed by the defendant would not be admissible if offered to prove that the defendant is generally a bad person, and therefore is likely to have committed the crime with which he is charged. However, evidence would be admissible if offered to prove motive, intent, identity, absence of mistake, or modus operandi, if such factors are at issue. If evidence of other wrongs or acts is admitted, the judge will instruct the jury that they may consider the evidence only as it relates to the narrow issue for which it was admitted, and may not consider it for any other purpose.

Also, in common law systems using adversarial processes, the fact that an item of evidence is relevant does not automatically mean that it will be admitted. Relevant evidence still might be excluded if it is unduly prejudicial, threatens to confuse or mislead the jury, threatens to cause unnecessary delay or waste of time, or is merely cumulative. Thus, evidence of drug addiction technically might be relevant to prove motive for embezzlement or fraud, but the judge still might exclude the evidence if he believes that its probative value is outweighed by the danger of prejudice to the defendant. Relevant evidence also might be excluded if it is subject to certain privileges as noted below. Evidence of other crimes and acts, as discussed above, that are otherwise relevant also might be excluded for the same reason.

Relevant evidence can be either inculpatory or exculpatory. *Inculpatory evidence* is evidence that serves to establish that an individual is guilty or at fault. *Exculpatory evidence* is evidence that tends to clear an individual from fault or guilt. Evidence that is neither exculpatory nor inculpatory is likely irrelevant.

Authentic

Authentic evidence is evidence that accurately represents the fact or situation it is offered to prove or disprove. The authenticity of evidence is an important concept in civil law and common law systems.

Authenticity in Civil Law Systems

Civil law systems, in contrast to common law systems, do not impose a requirement of authenticity for the admission of evidence. But even so, authentication is relevant in civil law systems because it affects the evidential value or weight the fact finder should give to evidence. That is, in civil law systems, authenticity is a factor to be considered by the fact finder in deciding, in light of all the evidence presented at trial, just how much weight to give the evidence. If, for example, a relevant item of evidence is not authentic, it will not be reliable, and, therefore, it will not be helpful to the fact finder in ascertaining the truth. Consequently, the fact finder will give it less weight than authenticated evidence. Conversely, an item of evidence deemed relevant and authentic will be reliable, and, therefore, it can be used by the fact finder to ascertain the truth.

Authenticity in Common Law Systems

In common law systems using adversarial processes, evidence will not be admissible unless it is established as authentic. If a piece of real evidence cannot be authenticated, it will not be admitted, even if it is relevant.

Admissibility of Testimonial Evidence

The rules around the admissibility of testimonial evidence in civil law jurisdictions are more lenient than in common law jurisdictions. Generally, in civil law jurisdictions, testimonial evidence is admitted if the presiding judge decides it is relevant.

In contrast, to be admissible in common law countries, testimony generally must be relevant and based on:

- Fact, not speculation or opinion (unless the witness is testifying as an expert)
- Direct knowledge, not hearsay

Very generally, a witness has direct knowledge if he:

- Performed the act or participated in it
- Saw the act being performed
- Heard about the act from the defendant (or in some circumstances, from a co-conspirator)

Special Rules Concerning the Admission of Evidence in Adversarial Proceedings

Common law systems that use adversarial processes have several rules that restrict the admission of evidence. These rules are not present in civil law systems that use inquisitorial proceedings.

In common law systems, special rules exclude certain forms of evidence that lack reliability. The most common of these rules are:

- The rule of authentication
- The rule against character evidence
- The rule against opinion testimony
- The best-evidence rule
- The rule against hearsay

The Rule of Authentication

In common law systems using adversarial processes, exhibits are inadmissible unless they are relevant and established as authentic. *Exhibits* are the tangible objects presented as evidence. Therefore, both real evidence and demonstrative evidence are entered into the record as exhibits. Exhibits include documents such as contracts, letters, and receipts, as well as photographs, X-rays, baseball bats, knives, fountain pens, and computer files. In short, almost anything that is not testimony is an exhibit. Testimony is what people say. Exhibits are the "props."

Questions concerning the admissibility of exhibits are determined by the trial judge in common law systems using adversarial processes.

But again, to be admissible at trial, evidence, other than testimonial evidence, must be properly authenticated; that is, the party offering the item must produce some evidence (e.g., testimony from a person with firsthand knowledge) to show it is, in fact, what the party says it is and to show it is in the same condition as when it was seized. If an exhibit cannot be authenticated, it will not be admitted even if it is plainly relevant.

The authentication requirement serves to ensure that evidence is what it purports to be and is genuine, not a forgery.

Although testimonial evidence does not have to be authenticated to be admissible, the courts in common law systems have a sort of "credibility test" for witnesses. The witness must

demonstrate that the knowledge he is communicating is believable and was gained by his personal experience.

There are a number of techniques that can be used to authenticate evidence, but they vary depending on the type of evidence. Often, evidence is authenticated by the testimony of a witness who knows about the item's chain of custody, the testimony of a witness with knowledge that the item is what it is claimed to be, by reference to the item's distinctive characteristics, and so on. Additionally, certain documents are self-authenticating and may be received into evidence without independent proof of authenticity. For example, in the United States, business records are self-authenticating if they were generated or maintained in the usual course of business.

Authenticating Typical Exhibits

Below are some of the issues that might be encountered in proving to a judge that particular types of exhibits are authentic.

DEMONSTRATIVE EVIDENCE

Again, *demonstrative evidence* refers to a tangible item that illustrates some material proposition. It differs from real evidence in that demonstrative evidence is not part of the underlying event; it is created specifically for the trial. Its purpose is to provide a visual aid for the jury.

An exhibit used for purely "illustrative purposes" is a type of demonstrative evidence. Demonstrative evidence includes charts, graphs, and summaries that help to simplify complicated evidence for the jury. In complex fraud cases, such evidence is extremely useful, but it must be simple and easy to understand.

Demonstrative evidence is admissible if the court decides that it presents a fair and balanced summary or picture of the evidence and is not unduly prejudicial. If offered for its truth value (and not just to illustrate a point), demonstrative evidence must be authenticated to show that the evidence is in fact what it is claimed to be.

Also, demonstrative evidence must be made available to the other party, and the court may order that the information used to create the exhibit be produced in court.

DIAGRAMS

A *diagram* is a schematic or technical drawing that is used to help make something easier to understand. A diagram (on paper or some other tangible display) can be admitted as evidence with no more foundation than the assent of a witness (e.g., "Is this a fair representation of the suite where you work?") It does not have to be true to scale or particularly detailed. A diagram can be prepared before trial, during trial, or prepped outside the court and finished during questioning. If a party objects to the admission of a diagram, the offering party may need to establish that it is reliable. Diagrams can be used in tandem with photos or other representational evidence, or as assistance in demonstrations to the jury.

WRITINGS

In general, authentication of a writing consists of establishing who authored the document. Depending on the document and situation, this is done in one of several ways: (1) the author testifies and claims authorship; (2) a witness testifies to seeing the author write the document; (3) with handwritten letters, a witness verifies the author's penmanship; (4) with typed or machine-written documents, the witness verifies the author's signature; (5) a witness testifies that the contents of the document point decisively to the author. These and many other document issues may require the participation of a documents expert.

BUSINESS RECORDS AND OTHER DOCUMENTS

Business records can encompass a broad range of documents, from all sorts of organizations, including corporations, small businesses, nonprofit operations, and community groups. Like other evidence, a party offering business records must provide testimony that the exhibit is the business record in question. For proper authentication, the party offering the evidence should be able to establish the following two things:

- The content of the document is complete and unaltered.
- The document originated from the named place of origination.

Certain documents, such as business records, are self-authenticating and may be received into evidence without independent proof of authenticity. For example, in the United States, business records are self-authenticating if a custodian or other qualified person certifies that the records meet the following requirements:

- The records were prepared reasonably near the time of the event they describe.
- The records were made by, or based on information transmitted from, a person with knowledge.

- The document was prepared as a usual part of doing business (i.e., it was not prepared specifically for litigation).

Business records and other documents are also vulnerable to hearsay objections. Put differently, offering the contents of business records to establish the truth of their contents can constitute hearsay. Thus, such materials can be barred as unreliable out-of-court statements unless a trustworthy foundation is established. If, however, there is certification that complies with the self-authenticating rules listed previously, the records will not only be self-authenticating, but the records' contents will be admissible to prove the truth of the contents as an exception to the rule against hearsay.

GOVERNMENT DOCUMENTS

The requirements for government documents are the same as for other business records. The distinction between government and business records arose because of narrow interpretations of the law that separated nonprofit from for-profit enterprises. Today, most records, regardless of origin, are called business records.

PHONE RECORDS

To be admitted into evidence, phone records must meet the business records authentication test.

DIGITAL RECORDS

Courts typically accept digital files and documents as evidence. In fact, courts themselves are using more digital resources because many aspects of litigation can now be conducted electronically.

Generally, to be admissible, digital records must meet the same authentication standards as hard copy records (i.e., to show that the item is what the proponent claims). Thus, to prove that a particular electronic record is authentic, those offering the evidence must demonstrate that the original document was not modified after its creation. But courts have recognized that the authentication of digital records may require greater scrutiny because such records can easily be altered after creation.

In fact, courts are still figuring out how to deal with digital evidence, and there is still disagreement regarding how to authenticate digital records. If digital evidence needs to be seized, it is vital that fraud examiners engage the services of a trained computer forensic

technician. A properly trained technician should know the proper procedures to follow to ensure that the files can be authenticated.

Nevertheless, the most likely methods of authenticating digital records are:

- Testimony from a witness with personal knowledge (e.g., an authenticating witness attests to the process by which the digital records are created, acquired, maintained, and preserved)
- Circumstantial evidence of distinctive characteristics (e.g., a person's business habit is consistent with the document)
- Certified copies of business records (e.g., digital records are accompanied by a custodian's written certification)

Digital evidence comes in several forms, including email, texts, instant messages, website data, and digital photographs. And different forms of electronic evidence may require different authentication approaches. Therefore, it is helpful to examine a few common forms.

EMAIL

Unlike traditional business letters written on formal letterhead, emails are more prone to authenticity issues and may be more difficult to authenticate. Email authenticity issues usually arise because email systems are unreliable and inherently unsecure, making emails susceptible to alteration. Moreover, emails can lack reliability because the identities of senders can be corrupted through unauthorized access and use.

Even so, there are numerous ways email can be authenticated, including:

- Witness with personal knowledge (e.g., a witness testifies that he recognizes a copy of an email that he received or drafted)
- Comparison with authenticated examples (e.g., if one email has been properly authenticated, a second email could be authenticated by comparing it with the first)
- Circumstantial evidence of distinctive characteristics (e.g., the presence of a party's name and email address or the presence of metadata)
- Trade inscriptions purporting to have been affixed in the course of business and indicating ownership, control, or origin (e.g., an automatic business signature at the end of the email)
- Certified copies of business records (e.g., email is accompanied by a written certification by its custodian)

TEXT AND INSTANT MESSAGES

As the use of text and instant messages continues to grow, parties are offering these types of records as evidence in an increasing number of cases. The most likely methods to authenticate text and instant messages are:

- Witness with personal knowledge (e.g., a witness testifies that he recognizes a copy of messages that he received or drafted)
- Circumstantial evidence of distinctive characteristics (e.g., the use of the defendant's name in the text messages and the subject matter of the messages)

WEBSITE DATA

As with all evidence, the proponent of website evidence must be prepared to establish that the evidence is authentic. In some courts, authenticity can be established by the testimony of a witness. Like any other demonstrative exhibit, parties can authenticate a website with the testimony of a witness who verifies that the exhibit at issue accurately reflects what he observed after logging on to the site and reviewing what was there.

Alternately, the proponent may be able to authenticate a website by providing testimony from the webmaster or someone with personal knowledge to show that the data was posted by the person to whom the information is attributed. For example, if website data is attributed to the website owner, the webmaster can testify that a particular file or content was entered on a site at a specific time. This is similar to authenticating writings by showing that the item was written by the person to whom it is attributed.

A growing number of people are using social networking sites like LinkedIn, Facebook, and Twitter, and as a result, the legal use of information obtained from social media sites has increased. Many users don't give much thought to what they post online. And because most of the information that gets posted online becomes a permanent record somewhere, investigators, attorneys, and employers are increasingly mining these sites for information, photos, and videos that can become evidence in civil and criminal litigation.

The standard for authenticating evidence from social media sites is no different than for any other types of evidence—there must be sufficient evidence to support a finding that the evidence is what the proponent claims.

Because evidence posted on social media sites typically comes from third parties, who sometimes use pseudonyms, attributing this type of evidence to a certain person can be challenging.

Finally, some website data may be self-authenticated. To review, self-authenticating evidence may be received into evidence without independent proof of authenticity. The types of website evidence that may fall under this category include government material that appears on official government websites or business-related material that appears on an organization's website.

PHOTOGRAPHS

Concerning the admissibility of photographs, it is necessary to establish their fidelity to the object they claim to represent. This means that the offering party must prove that the picture is unaltered and shows what the proponent claims it shows. Generally it is enough to have a witness familiar with the object or space in a photo to corroborate it (e.g., "Yes, that's the hallway running between our two buildings."). The matter gets more complicated when a photo is controversial. This can require technical specifications for proper foundation.

In some unusual situations, a photo may reveal information that no witness can corroborate. There has been at least one instance where the background of a photo showed a stabbing that took place in a crowd. No one, not even the photographer, saw the stabbing at the time. In unusual situations where a photo communicates evidence not substantiated elsewhere, the foundation of the photograph will need more strength—including technical details on the camera, the film, who took the shot, why and where, and so on.

The exceptions make photos seem more legally fraught than they are. In fact, photos usually are admitted with little objection. Moreover, photos do not even have to be contemporary with the crime or grievance to which they pertain. If a photograph is established as accurate in its portrayal, it can be shot after the original act.

General Points About Exhibits

In adversarial processes, either side can enter exhibits into the record, given the proper foundation. Once admitted, the evidence is available for use by either side. It does not matter who entered the item into evidence; either side can use it during questioning.
It also does not matter when exhibits are admitted. They may be introduced into evidence

during direct examination: opposing counsel is allowed to inspect the exhibit and then the witness confirms the exhibit.

Additionally, exhibits are marked for identification before they are offered into evidence. Marking an exhibit identifies it for the record so that it will be recognizable to anyone who subsequently reads the transcript of the proceedings. Exhibits generally are marked sequentially and identified according to the party who offered them (e.g., Plaintiff's Exhibit 1).

Furthermore, when everyone agrees that an exhibit is authentic and admissible, it can be directly entered into the record, without foundational review, by *stipulation*—an agreement between the parties that relates to a matter in the trial proceedings.

Both sides to a lawsuit can stipulate to certain basic facts and narrow the line of dispute to a few issues or allegations. Stipulations generally are used only for objective facts that are easily proved or disproved. For instance, in an embezzlement case, both sides might stipulate the fact that the employee worked at the company, his dates of employment, and his title.

Objections to Exhibits

The fact that an item of evidence is relevant and authentic does not, however, automatically mean that it will be admitted. If the evidence violates some other rule of evidence—such as the rules against hearsay, prejudice, or relevance—it will likely be barred.

If, during trial, a party wishes to dispute the admissibility of an exhibit, the party will say, "objection," and the judge will rule on the objection. If the judge overrules the objection, the evidence will be admitted, but if the judge sustains the objection, the evidence will be excluded. Also, in deciding on the admissibility of exhibits, judges can decide to admit the material just as it is, admit it with alterations (e.g., expurgating parts of a text or obscuring certain images), or deny the admission altogether.

In some instances, the judge's ruling on an objection requires a separate hearing to consider the issue.

Fraud trials can be bogged down with lengthy challenges due to the sometimes large volumes of documents offered as evidence.

The Rule Against Character Evidence

In civil and criminal trials in common law systems, there is strong policy against character evidence. *Character evidence* (sometimes called *propensity evidence*) is testimony or exhibits that purport to establish a "trait of character" or propensity to behave in a particular way, such as carefulness, honesty, violence, or cowardice.

There are several reasons why common law rules exclude character evidence. If used inappropriately, character evidence has the potential to be unreliable and unfair. Also, if character evidence is admitted, the jury might draw conclusions about the general propensity of the individual who is the subject of the evidence. Similarly, juries might afford character evidence too much weight, or they might try to punish a defendant for his bad character. Additionally, character evidence is subjective—one person's "gruff" is another viewer's "aggressive." Moreover, the introduction of character evidence might involve time-consuming ventures into matters that are collateral to the matters at issue.

Additionally, character is not an absolute indicator of behavior. That is, it is pretty common to remark how "out of character" somebody's actions were in a given situation. So there is always a chance someone was acting out of character, making the behavioral propensity (if there was one) useless in the legal exchange.

Finally, testimony about character has a reckless potential to be mistakenly founded, misled, or concocted. It is always possible to "misjudge" someone, especially if we only know the person in limited circumstances like work or a social club. Moreover, it is exceedingly easy to fabricate incidents about character and, for shrewd talkers, to manipulate perceptions of personality. To prove a fraud case, the party bringing the action must show that the defendant committed the act in question. There is too great a danger of prejudicing the jury if you allow testimony about the defendant just being a bad person. Whether he is a bad person or not ought to have no bearing on whether or not he committed the act in question.

In general, character evidence is not admissible in criminal cases, and it is only rarely admissible in civil ones. The general rule in criminal cases provides that evidence of a defendant's bad character is not admissible at trial. For example, under this rule, the government cannot offer evidence of a defendant's prior crimes or other bad acts to prove the defendant's bad character.

There are, however, some instances where character evidence may be admitted in criminal trials. Some of the exceptions for use of character evidence in criminal cases include:

- The accused may offer evidence of his good character, in which case the prosecution may introduce evidence of the accused's bad character.
- Character evidence may be admissible to reflect on the credibility of a witness.

Again, evidence of other crimes, wrongs, or acts is not usually admissible to prove the character of a person. For example, Rule 404(b) of the U.S. Federal Rules of Evidence states that evidence of a defendant's earlier crimes, wrongs, or acts is not admissible to show the defendant's character in order to show that he acted in conformity with that character. That is, under such rules, such evidence is not admissible to prove that the defendant is generally a bad person and therefore is likely to have committed the crime with which he is charged. For example, if a defendant is charged with stealing money from his employer's safe, the prosecution would not be permitted to offer evidence that the defendant had previously stolen money from another employer to show the defendant had a propensity to steal.

However, there are some uses of character evidence that may be admissible because they are offered for a purpose other than showing character. In criminal cases, character evidence generally may be used to:

- Show the accused's knowledge, intent, or motive for the crime.
- Prove the existence of a larger plan of which the charged crime is a part.
- Show the accused's preparation to commit the charged crime.
- Show the accused's ability and means of committing the crime (possession of a weapon, tool, or skill used in the commission of the act).
- Show the accused's opportunity to commit the crime.
- Show threats or expressions of ill will by the accused.
- Link the accused to physical evidence at the scene.
- Show the accused's conduct and comments during arrest.
- Show the accused's attempt to conceal his identity.
- Show the accused's attempt to destroy evidence.
- Present valid confessions.

Conversely, civil law systems do not rely on juries like common law systems, and because of this, the laws of evidence in most civil law systems do not have rules designed to prevent improperly influencing an inexperienced fact finder. Therefore, most civil law systems do not prohibit the use of character evidence.

The Rule Against Opinion Testimony

During trial in adversarial proceedings, most evidence is introduced through the testimony of witnesses. Evidence on which the jury can make factual determinations must be introduced in the form of admissible testimony or documentary evidence by lay or fact (i.e., nonexpert) witnesses.

The rules of evidence, however, limit the testimony of *lay witnesses*—nonexpert witnesses who testify from personal knowledge about a matter at issue. Generally, lay witnesses are only allowed to testify about what they have actually experienced firsthand and their factual observations. Thus, lay witnesses provide a report on what they know and must keep their opinions and conclusions to themselves.

Despite the general rule, there are exceptions that allow some nonexpert witnesses' opinions into the record. Lay witnesses may give opinions if the statement is "rationally based" on their own perceptions, and if the opinion is helpful to a clear understanding of their testimony or the determination of a fact.

EXAMPLE

An employee at a securities firm blows the whistle on his superiors for a high-level stock fraud, and in response, the government initiates a secret investigation into the matter and ultimately brings criminal charges against the employee's superiors. At trial, defense suggests the investigation was an invasion of privacy. Prosecutors are justifying their secret eight-month investigation on the basis of the whistleblower's tip. The prosecution will offer into evidence the whistleblower's "opinion" that his superiors were engaged in fraud to show that the government was justified in conducting its investigation. Under these facts, the opinion is admissible. But the opinion testimony is not allowed to show that management is guilty of fraud; instead, it is admissible to show what prompted the investigation.

In general, lay witnesses in common law countries generally may give opinions if their statements pass a three-part test:

- The witness must have direct personal knowledge of the facts to which the opinion pertains.
- The opinion must be of the common, everyday sort (i.e., does not involve specialized knowledge or tests).
- The opinion is not part of a legal judgment, reserved for the jury or judge to decide.

Opinions from lay witnesses must be based on personal experience and have some bearing on the *facts* (as opposed to the *judgment*) of the case. This distinction is further refined in situations involving hearsay and personal judgment (discussed below).

In contrast to lay witnesses, expert witnesses are allowed to give opinion testimony because experts are hired to render a professional opinion. Experts possess education, training, skill, or experience in drawing conclusions from certain types of data or information that lay witnesses do not possess. Expert testimony, however, may be excluded if it embraces a legal conclusion. Therefore, expert opinions addressing guilt or innocence will likely be excluded in criminal cases.

The Best-Evidence Rule

Sometimes testimony may be excluded in common law systems because of the *best-evidence rule*, which prohibits a party from orally testifying about the contents of a document without producing the document itself or proving to the judge that there is a valid reason for being unable to do so. This rule, however, only applies when an original or copy is being used to prove the contents of a writing, and it does not demand that a party produce the very best evidence to prove a fact in dispute.

Also known as the *original-writing rule*, the best-evidence rule provides that when a witness testifies about the contents of a document, at least a fair copy of the original must be available for inspection. If there is no original, a copy of the proven authentic document will do, but the court must be assured that the copies are reliable and accurate. If the document is lost—no original, no copies—the judge will have to be convinced that there is good reason to forgo the exhibit and admit the testimony.

The original purpose of the rule was to prevent altered evidence from being admitted as evidence, but most modern commentators state that the primary purpose of the rule is to ensure that the most accurate written version of evidence is admitted at trial.

Fraud examiners can use copies in preparing their case reports, but at trial, the original must be produced if it is available. Thus, when public records are involved in a fraud examination, examiners should always obtain certified copies.

The best-evidence rule applies in the United States, but to accommodate electronic evidence, some common law countries, including England and Australia, abolished the best-evidence rule.

The Rule Against Hearsay

Many countries with common law systems restrict the admission of hearsay statements at trial. Simply put, hearsay refers to a statement that repeats what some other person said while outside of court. More specifically, *hearsay* is "a statement, other than one made … at the trial or hearing, offered in evidence to prove the truth of the matter asserted." Basically, hearsay involves the following elements:

- A *statement* (anything intended to be an assertion; statements can be oral, written, or nonverbal conduct, such as nodding a head)
- *That is made outside the court's supervision* (statements made at trial or during deposition are not hearsay because they are made during court proceedings, but a statement made at work or at a crime scene is outside the court's supervision and could be hearsay if the other elements are also present)
- *That is offered to prove the truth of the matter asserted* (a party is offering a statement to prove the truth of the matter asserted if the party is trying to prove that the assertion made by the declarant [the person who made the out-of-court statement] is true)

Under the general rule, hearsay is not admissible in court, but this rule is subject to numerous exceptions. Excluding hearsay on one level means witnesses cannot say, "He said … she said." Each person testifies to his own experience. The general rule against hearsay is designed to protect the credibility and condition of testimony and to preserve each side's right to cross-examine witnesses.

Each witness in the trial will be questioned about personal, firsthand encounters. Unless their statements satisfy one of the exceptions discussed below, witnesses will speak only about things they have experienced themselves. If possible, evidence should be presented in the courtroom so that the jury can determine the weight to give each piece of evidence.

The hearsay rule often creates admissibility issues for digital evidence because such evidence is often made out of court and offered to prove the truth of the matter asserted.

Exceptions to the Hearsay Rule

The general rule against hearsay is full of exceptions—ways to get information into the record—that accounts for the rule's infamy in courtroom dramas and in real courtrooms. Some categories of statements may be exempt because they are not considered hearsay, and there are many circumstances in which evidence, although hearsay, is admissible.

Note that these are general types of exceptions, and each country that excludes hearsay has its own list. Fraud examiners should check the applicable laws for hearsay exceptions.

THE TRUTH OF THE STATEMENT IS NOT AT ISSUE

Although the general rule against hearsay provides that out-of-court statements offered to prove the truth of an assertion are not admissible, it does not apply to out-of-court statements that are offered for some other purpose. That is, the general rule against hearsay only applies if the statement is being offered to prove the truth of the matter contained in the statement. Therefore, if the statement is offered for some other purpose, it technically is not hearsay. An out-of-court statement can be admitted if it (1) is relevant to some aspect of the proceedings *and* (2) is not offered for the truth of its contents. Such statements are most often used to show a person's knowledge or state of mind at a particular time.

EXAMPLE

Patrick got into an altercation with Dwyer on August 19, 20X1, and on September 1, 20X1, Patrick filed a civil suit against Dwyer, alleging that Dwyer broke his jaw during the altercation.

The suit goes to trial, and during the trial, it is established that the fight occurred at 8:30 p.m. and that it lasted about five minutes.

In his defense, Dwyer calls Walter to the stand, and Walter testifies that at 9:30 that night, Patrick called him and made the following clearly-enunciated statement: "Walter, I hereby forgive the money you owe me."

Walter's testimony relates to an out-of-court statement, but it is not hearsay because it is not offered to prove the truth of the matter asserted (i.e., that Patrick forgave the loan he made to Walter). Instead, the statement is being offered to prove that Patrick was speaking clearly at 9:30 p.m., which would mean that Patrick's jaw was unbroken after his altercation with Dwyer. Walter's testimony relates to his own firsthand perception of how Patrick's voice

sounded. Therefore, this statement is not hearsay, and it is admissible to show that Patrick was speaking clearly at 9:30 p.m.

ADMISSIONS BY AN ADVERSE PARTY

Generally, the statement of an adverse party is not hearsay. Such statements, called *admissions,* can be very powerful evidence. More specifically, an *admission* is an out-of-court statement or conduct by a party to the lawsuit that tends to support the other side's position or diminish the declarant's own position. Thus, anything spoken or written by a party to a lawsuit can be entered into the record, provided that the statement can be corroborated and is relevant. Each side can use its adversary's out-of-court statements as evidence.

For example, during your investigation of the case prior to trial, you interviewed the defendant. During the interview, he tells you that he falsified invoices. Later he denies making the statement. If you take the stand and tell the jury that the defendant told you he falsified invoices, technically that statement is hearsay. But because the statement is an admission, it will be admitted under this exception to the rule.

An admission is not necessarily an outright confession. A witness may testify that a bank officer told her, "I have ways of getting loans approved that no one else knows about." The statement alone does not prove loan fraud against the officer, but it does establish, by his own admission, his stated intent to subvert the security controls of the institution.

In cases involving corporations, large groups, or government agencies, any statement made by a member of the organization is potentially an admission. But to qualify as an admission, the person who made the statement has to be directly authorized to speak for the organization or perform a job related to the issue under discussion. For example, an agent employed by Jefferson Realtors who says, "You've been defrauded here" to an aggrieved client has made an admission on behalf of the company. A janitor at Jefferson Realtors, however, cannot make the same admission because janitorial duties are not related to the formation of contracts, and it is not likely that the janitor is authorized to make corporate declarations. Additionally, because an agent makes contracts on the company's behalf, a statement made by an agent of Jefferson Realtors is an admission even if the agent is not the official spokesperson for Jefferson's legal affairs.

FORMER TESTIMONY UNDER OATH

Testimony given by the declarant at another hearing is admissible if the party against whom the testimony is now offered had an opportunity and motive to examine the witness in circumstances similar to those of the present trial.

BUSINESS AND GOVERNMENT RECORDS

We commonly think of invoices, receipts, and official documents as the final legal word, but like statements made outside of court, business and government records are hearsay; they are prepared outside the courtroom. A special exception for these materials, however, makes them admissible if they are provided with a legal foundation. The admissibility of such records rests on two questions:

- Have they been prepared during "regularly conducted business activity"?
- Are they verifiably trustworthy?

If both questions can be answered in the affirmative, then the records are admissible. Thus, the business-records exception to the rule against hearsay provides that, although business records are hearsay (prepared outside the courtroom), such records are admissible under a hearsay exception if they are prepared during regularly conducted business activity and are verifiably trustworthy.

Materials prepared specifically for trial are not admissible as business records. Anything that casts doubt on the veracity of these documents can bar them. In situations where the charge involves altered documents, the materials are admitted to prove the charge of alteration—not for their truth-value—so the hearsay rule does not apply.

Computerized records have had no trouble being accepted as evidence. Generally, the hearsay exception for business records applies to such records (i.e., they are admissible as long as the records have been compiled as a regular facet of doing business).

STATEMENT AGAINST INTEREST

A statement against interest is a hearsay exception that is grounded on the theory that people do not ordinarily make harmful or damaging statements about themselves. A *statement against interest* is a statement that was, at the time of its making, contrary to the declarant's interests and would not have been made unless the declarant believed it was true. So, a statement against interest exception allows someone to testify to a statement by another person that reveals something damaging to the person who made the statement.

Generally, to be admissible under this exception, the statement must meet three requirements:

- The declarant must be unavailable to testify.
- The statement must have been against important interests of the declarant when made.
- Corroborating circumstances must clearly establish the trustworthiness of the statement.

In prosecuting a tax evasion charge, for example, prosecutors may present a financial statement used by the defendant to obtain a loan; this is a statement against interest because the document declares a higher net worth than the defendant now claims to have.

ABSENCE OF AN ENTRY IN BUSINESS RECORDS

Evidence that a matter is not included in the memoranda or reports kept in the regular course of business may be admissible to prove that a certain event did not occur if the matter was one about which a memorandum or report regularly was made and preserved. However, this does not hold true if the source of information or the circumstances indicate a lack of trustworthiness.

RECORDED RECOLLECTIONS

A memorandum or record may be admissible if it concerns a matter that the witness once had knowledge of but now has forgotten; was made or adopted by the witness when the matter was fresh in memory; and is shown to be accurate. Such memoranda or records also may be shown to a witness who has temporarily forgotten the events to refresh the witness's recollection and allow the testimony to be more complete or accurate.

PRESENT SENSE IMPRESSIONS

Courts assume statements that are made during or immediately after significant events or conditions and that describe or explain the events or conditions are reliable, so present sense impressions are admissible. For example, a witness can report that he first suspected fraud at Securities Plus by noting that his superior said, "Oh my God! This can't be happening!" when he was informed that there would be an audit. In a similar example, Mr. Whistler notices Jenny Moore, a coworker, in John Smith's office and overhears her say, "Oh, here are some bid sheets in the trash can." If the government prosecutes Smith for bid rigging, which is demonstrated by the bid sheets, Mr. Whistler can testify about Moore's statement as a present sense impression because the words described the scene before her.

EXCITED UTTERANCES

There is also a hearsay exception for *excited utterances* (i.e., statements relating to a startling event or condition made while the declarant was under the stress of its excitement). Unlike statements of present sense impressions, excited utterances require an occurrence that is startling enough to produce excitement. In the Mr. Whistler scenario, for example, Moore's statements might qualify as an excited utterance if she discovered the bid sheets after months of searching for incriminating evidence and told Whistler, while jumping up and down in excitement, "I've found the evidence I've been waiting for a long time!" Here, the successful conclusion of the search was sufficiently exciting.

THEN-EXISTING MENTAL, EMOTIONAL, OR PHYSICAL CONDITION

Statements of the declarant's then-existing state of mind, emotion, or physical condition are also admissible as exceptions to the hearsay rule. Generally, evidence rules list state of mind, emotion, sensation, or physical condition, pain, and bodily health as acceptable subject matters, along with extremely personalized thought processes such as intent, plan, motive, design, and mental feeling.

Defense attorneys at a fraud trial sometimes use arguments about what their client *intended*, or the *confusion* and *stress* the person was suffering. For instance, the defendant was seen shredding documents, and he was overheard to say, "They'll never prove anything now." The statement may be admitted to show the defendant's state of mind at the time he was shredding the documents. It also shows that the defendant acted with the intent to destroy the documents. Hearsay statements that help establish this intention are admissible as exceptions.

STATEMENTS FOR PURPOSES OF MEDICAL DIAGNOSIS OR TREATMENT

Anything first communicated during a medical examination is admissible as a hearsay exception. This includes medical history, symptoms, pain, and the general character of the medical condition. These statements do not even have to have been made by the patient. They can involve someone (parent or spouse) accompanying the patient.

PRINTED MATTER, LEARNED TREATISES, AND REFRESHER WRITINGS

Written materials that add to the court's knowledge of an issue are excluded from the general rule against hearsay. This exception frequently applies to the testimony of expert witnesses who often use published material in their work.

Printed materials that support technical or professional assertions, such as commodity market reports, stock market quotes, mortality tables, cost of living indexes, etc., are admissible if they are "generally used and relied upon by the public or by persons in particular occupations."

Often, rules of evidence create a hearsay exception for *learned treatises*, providing that an authoritative work is admissible to either support or attack the opinion of an expert witness if the work is established as a reliable authority. However, some courts limit the rule. In these jurisdictions, specialized "treatises, periodicals, or pamphlets" can be referenced only during cross-examination. In a world of proliferating and sometimes contradictory sources of information, just what counts as a learned treatise and what is a fringe group's manifesto is not immediately clear.

Also, courts may permit testifying witnesses to refresh or revive their memory by referring to a writing or anything else if the witnesses will thereafter be able to testify without depending on the terms of the writing. For example, Whistler, who is serving as a witness at a fraud trial, wants to see some notes he wrote two years ago to make sure he got the numbers right in his testimony. He is allowed to consult the notes and continue with his testimony. The text of the notes used to refresh the witness's memory is also admissible, but only if the *opposing* attorney requests the admission.

OTHER EXCEPTIONS

There are other miscellaneous exceptions to the general rule against hearsay, and these include exceptions for things like *dying declarations* and *ancient documents*. For those instances not specified in any rule, there remains the judge's discretion: Anything the judge deems *trustworthy* for the purposes of its presentation is admissible. This is the cornerstone of the rule. Hearsay is excluded in the first place because it supposedly lacks trustworthiness. However, other kinds of hearsay that do not fall within any specific hearsay exceptions may be admissible if they meet the same standards of trustworthiness as required for the listed exceptions.

Hearsay in Civil Law Systems

Civil law systems do not have any rules corresponding to the common law rules against hearsay due to the fact that judges play a more active role in determining the facts in inquisitorial systems. For example, in German courts, hearsay is admissible, and it is up to the court to determine whether or not the hearsay evidence is convincing. The common law

rules against hearsay are founded on the concern that juries might give inappropriate weight to unreliable hearsay evidence, but because judges play a more active role in determining the facts in inquisitorial systems, the concerns that gave rise to the rules against hearsay in common law systems are not present in civil law systems. Accordingly, hearsay evidence is more freely admitted in civil law systems than in common law systems.

Chain of Custody

If evidence is subject to change over time, or is susceptible to alteration, the offering party might need to establish that the evidence has not been altered or changed from the time it was collected through its production in court. This is done by establishing a chain of custody. Thus, the chain of custody can be an important factor in establishing authenticity.

The *chain of custody* is both a process and a document that memorializes (1) who has had possession of an object and (2) what they have done with it; it is simply a means of establishing that there has not been a material change or alteration to a piece of evidence.

Thus, establishing the chain of custody for an item of evidence demonstrates its authenticity, and it shows that the item has not been altered or changed from the time it was collected through production in court.

In general, establishing the chain of custody consists of documenting each person who had control or custody of the evidence; how and when it was received; how it was maintained or stored while in each person's possession; what changes, if any, it underwent in that person's custody; and how it left that person's custody. The end result is a chain of testimony that accounts for the movement and location of physical evidence from the time it is obtained to the time it is proffered at trial. The goal is to show that access to the evidence was limited to those who testified in the chain of custody and thereby demonstrate that the evidence has not been materially altered.

Gaps in the chain of custody (e.g., when it is not clear what occurred with a set of records) or outright mishandling (e.g., a group of questioned documents was not properly sealed) can dishevel a case but not wreck it outright. Courts have found in some cases that even though there have been mistakes in the chain of custody, the mistake affects the "weight," though not the "admissibility," of evidence. That is to say, the evidence will still be allowed into the record, but it is accompanied by a forthright description of any improprieties that have

occurred in the chain of custody. The jury and judge are supposed to consider the improprieties when they deliberate, "weighing" the case for guilt or innocence.

In fraud cases, the array of physical evidence, all the paper documents, audio and video recordings, and information-processing equipment, such as computers, demands close monitoring in the chain of custody.

The following are some general guidelines that will help examiners demonstrate the chain of custody. They will also help examiners in authenticating obtained evidence:

- If records are received via mail or courier-receipted delivery, keep copies of the postmarked envelope or the delivery receipts.
- If a cover letter is included, make sure you keep it.
- If the cover letter or transmittal letter includes a list of the documents, check the package immediately to ensure all documents are there. If something is missing, make a note in the file and notify the sender immediately.
- If you receive documents in person, create a memo stating the date and time the documents were received, who gave you the documents, where that individual obtained the documents, and a complete list of the documents received.
- If you obtained the documents yourself from the original source (desk, file cabinet, etc.), create a memo describing the date, time, *exact* location of where the documents were found, and a complete list of the documents obtained.
- Keep the originals of these memos or delivery receipts in the case file and keep a copy with the documents (it will be much easier to identify where the documents came from if you have the information with the documents).

Additionally, because digital evidence can be easily altered or destroyed, a chain of custody must be maintained for all electronic evidence gathered and analyzed in an investigation. At a minimum, the following chain of custody procedures should be followed:

- Identify each item that contains relevant information.
- Document each item, who it was received from, who authorized its removal, the location of the item, and the date and time the item was received.
- Maintain a continuous record of the item's custody as it changes hands.

Impeachment

In common law systems using adversarial processes, evidence usually is introduced during direct examination of a witness. In adversarial processes, there is another side to testimony: cross-examination. (Inquisitorial processes do not allow cross-examinations). Under the evidence rules in adversarial systems, the adverse party is usually entitled to offer evidence to impeach the testimony or credibility of a witness. *Impeachment* is the practice of bringing out matters that attack a witness's credibility.

It is important to note, however, that because cross-examination is absent from inquisitorial processes, impeachment is not an issue for civil law systems using inquisitorial processes.

There are numerous ways an attorney might impeach a witness, but the most common ways include efforts to show that the witness:

- Is influenced by bias or self-interest
- Has an impaired ability to observe
- Made prior inconsistent statements
- Has been convicted of a felony or equivalent crime
- Has a reputation for untruthfulness

Impeachment by *bias* shows that the witness has reason, or at least opportunity, to skew the evidence against one of the parties in the litigation. To impeach a witness for bias, opposing counsel will, during cross-examination, ask questions to bring up any pecuniary interest the witness has in the case, any connection the witness might have to any matter or litigant, and any other information that will make the witness appear to have some interest in favoring one party over another.

Another way to impeach witnesses is to show that their *ability to observe was impaired*. Matters of observance include the ability to see, hear, smell, or feel some item in question.

Nothing overturns a witness's statements like *inconsistency*. Opposing lawyers will always confront any witness on cross-examination with any apparent inconsistencies between the trial testimony and statements, testimony, or information given by the witness on other occasions.

In some common law systems, a witness's credibility may be challenged, though not automatically impeached, by showing that the person has been convicted of a felony crime.

For example, under Rule 609 of the U.S. Federal Rules of Evidence, evidence that a witness has been convicted of a crime may be offered to attack the witness's character for truthfulness if the crime was punishable by death or imprisonment in excess of one year or if the crime, regardless of the punishment, involved dishonesty or a false statement. In short, Rule 609 offers a few basic rules for introducing evidence of prior crimes to impeach a witness. First, convictions for acts involving dishonesty, such as perjury, false statement, or criminal fraud, are admissible to impeach a witness's testimony. So, if a witness has been convicted of a misdemeanor not involving dishonesty or a false statement, the prior conviction cannot be used for impeachment. Second, evidence of felony convictions can be used to impeach a witness, but evidence of any prior conviction is presumably inadmissible if the conviction is more than ten years old.

Finally, any witness may be impeached by proof of *reputation for untruthfulness*.

Generally, impeachment is complete when a witness admits the impeaching matter; if the witness does not admit it, then opposing counsel is usually required to prove the impeachment. If, however, the subject of the matter of the impeachment is *collateral*—those non-material matters that affect the credibility of a witness and do not tend to prove or disprove a substantive issue in the case—the impeaching counsel must accept the witness's answer even if it is false. So, when a witness is asked about a collateral matter for the purposes of proving impeachment, the witness's answer ends the inquiry, and opposing counsel cannot offer extrinsic evidence to prove collateral impeaching matters.

Certified Fraud Examiners should keep in mind that the above methods of impeachment may be used not only on the defendant and defense witnesses, but also on witnesses for the prosecution. Inquiries should be made before trial to determine if a prosecution or defense witness is subject to impeachment, and, if so, appropriate steps should be taken.

Privileges

Introduction

There are evidentiary privileges that protect certain types of evidence from being discovered or produced during trial. Generally, if a privilege applies to information, the court and the parties seeking the information are denied access to it, and judges and juries must disregard any evidence they do actually hear if it is deemed privileged afterward.

The privileges available and the requirements for each vary substantially by jurisdiction. Generally, the United States and other countries with common law systems offer broader protection with privileges than those countries with civil law systems.

Civil law jurisdictions have doctrines that serve the same function as privileges in common law jurisdictions—doctrines that exclude relevant evidence from being discovered or produced during trial—even if such doctrines are not classified as privileges. For example, many civil law systems have general professional privileges that prohibit the admission of communications made through the exercise of certain professional duties.

Some of the more common privileges are discussed below.

Legal Professional Privileges

Legal professional privileges are rules of evidence that preclude disclosure of confidential communications between professional legal advisors (e.g., solicitor, barrister, attorney, etc.) and their clients. These privileges are designed to encourage open and honest communications, and they go by many names. In the United States, the legal professional privilege is known as the *attorney-client privilege*; in the United Kingdom, it is known as the *legal advice privilege*; in Canada, it is known as the *solicitor-client privilege*; and in the European community, it is known as the *legal professional privilege*.

The requirements for the application of these privileges vary among jurisdictions, but generally, the following elements must be present for communications to be protected:

- A communication between a legal professional and a client
- The communication was made to seek or give legal advice
- The parties intended the communications to be confidential (i.e., the communications must not be disclosed to third parties such as vendors, customers, auditors, or governmental officials)

To be protected under a legal professional privilege, it is not necessary that the communication take place after a lawsuit has been filed.

Legal professional privileges, however, are not absolute; they are subject to waiver. Because these privileges only protect confidential communications, the protection they provide will be waived for communications disclosed to third parties who have little or nothing to do

with the client's pursuit of legal representation because such disclosures demonstrate a lack of confidentiality.

Generally, waiver occurs when the client, who holds the privilege, voluntarily discloses (or consents to or encourages someone else disclosing) any significant part of the privileged communications. Although the client holds the privilege, the privilege can be waived by the client's attorney or a third party—someone who is neither the attorney nor the client.

The legal professional privilege can be waived in various ways, including:

- The client testifies about confidential communications.
- The attorney testifies about confidential communications at the client's command or request.
- The client puts confidential communications in question.
- The client, the attorney, or a third party carelessly or inadvertently discloses confidential communications to an outside party (which sometimes results in waiver).

Although legal professional privileges only apply to confidential communications between a lawyer and his client, in most jurisdictions, the protection afforded by these privileges extends to communications with third-party consultants hired to help provide legal advice to the client (e.g., fraud examiners, accountants, bankers, or other experts). Thus, waiver does not occur when an attorney shares privileged information with an outside consultant hired in a role that concerns the client's pursuit of legal representation and when the communication was made for the purpose of effectuating legal representation for the client.

The U.S. Attorney-Client Privilege

The attorney-client privilege precludes disclosure of communications between an attorney and client, but only if all of the following conditions are met:

- The client retained the attorney to provide legal advice (i.e., there must be an attorney-client relationship)
- And thereafter the client communicated with the attorney on a confidential basis, and
- The privilege has not been waived

The attorney-client privilege applies to individuals as well as corporations or other business entities. In the context of an investigation of a company, communications generally will be protected under the attorney-client privilege if the following elements are present:

- The communications were made by corporate employees to counsel.

- The communications were made at the direction of corporate superiors in order for the company to obtain legal advice from counsel.
- The employees were aware that the communications were being made in order for the company to obtain legal advice.
- The information needed was not available from upper management.
- The communications concerned matters within the scope of the employees' corporate duties.
- The communications were confidential when made and were kept confidential by the company.

To be protected under the attorney-client privileges, a communication must be made to obtain legal advice. Thus, a general counsel's participation in an investigation conducted by management does not automatically create an attorney-client privilege. The key element is that the attorney (whether in-house counsel or outside counsel) is conducting the investigation for the purpose of providing legal advice to the company. The privilege generally extends to information gathered by investigators acting at the direction of the attorney.

Also, to qualify for the privilege, there must be intent to keep the communications confidential (i.e., the communications must not be disclosed to third parties such as vendors, customers, auditors, governmental officials, etc.).

The attorney-client privilege prevents disclosure of the communications—the letters, memos, or contents of telephone calls—between the attorney and client, not of the underlying facts or documentary evidence in the case. A client may not refuse to produce documents or other relevant evidence merely because such evidence was previously given to the attorney.

Similarly, the attorney-client privilege does not prevent disclosure of communications that relate to business rather than legal advice. Corporate counsel is often consulted to give advice on matters related to business conduct rather than legal issues. Such communications would be discoverable.

Finally, the attorney-client privilege may not be asserted if the communication involved the attempted or actual commission of a present crime or fraud. The attorney does not have to be a participant in the fraud for the waiver to apply.

The attorney-client privilege is not absolute; it is subject to waiver. Generally, waiver occurs when the client, who holds the privilege, voluntarily discloses (or consents to, or encourages, someone else disclosing) any significant part of the privileged communications to an outside party who has little or nothing to do with the client's pursuit of legal representation. Even inadvertent disclosure can result in a waiver of privilege.

And like other legal professional privileges, the attorney-client privilege extends to communications with third-party consultants hired to help provide legal advice to the client (e.g., fraud examiners, accountants, bankers, or other experts). Accordingly, fraud examiners involved in investigations conducted at the direction of counsel must take special care to ensure that the attorney-client privilege is not waived by giving documents or communicating information to anyone outside the investigation team, including members of law enforcement. Generally, disclosure of a written fraud investigation report to a third party constitutes a waiver of privilege. Also, if confidential information gathered during an investigation is shared with law enforcement, then the privilege may be waived not only as to the information given, but also as to any other information relating to the same subject matter.

For example, if an investigator submits a copy of his report to the prosecutor who initiates criminal proceedings based on the findings in the report, the criminal defendant may be able to require the investigator to provide all the documents he used in writing the report. In such an instance, the investigator may be considered to have waived the privilege.

The Legal Advice Privilege in the United Kingdom

Because the United Kingdom is also a common law jurisdiction, its legal advice privilege shares many aspects of the attorney-client privilege in the United States. The legal advice privilege prevents the disclosure of confidential communications between a lawyer and his client that are in connection with giving legal advice.

The legal advice privilege applies to every communication between a lawyer and his client whether or not the communication was made in contemplation of litigation.

The Solicitor-Client Privilege in Canada

The solicitor-client privilege protects information a client provides to his solicitor that is necessary to obtain legal advice. For the solicitor-client privilege to apply, all of the following three requirements must be met:

- There is a communication between a legal professional and a client.
- The communication was made to seek or give legal advice.
- The parties intended the communications to be confidential.

Attorney Work Product and Litigation Privileges

Litigation privileges and other similar evidentiary protections, such as the U.S. attorney work-product doctrine, protect materials that are prepared in anticipation of litigation.

The U.S. Attorney Work-Product Doctrine

The U.S. attorney work-product doctrine protects materials from discovery that are prepared in anticipation of litigation.

The attorney work-product doctrine is embodied in Rule 26(b)(3) of the Federal Rules of Civil Procedure and under comparable state rules. It protects documents and tangible things that are prepared in anticipation of litigation. The protection, however, is conditional in part: The opposing party may obtain access to otherwise protected investigative documents and things through pretrial discovery if it can show *substantial need* for the protected information and that the information cannot be obtained from another source. However, the attorney's mental impressions, opinions, and strategies concerning the litigation are absolutely privileged and cannot be discovered even with a showing of substantial need.

The protection offered by this doctrine extends to not only information and documents prepared by a party or the party's attorneys, but also by third-party consultants and examiners hired by the attorneys. For instance, communications with the attorney and any work or analysis done by an expert with whom the attorney has consulted is protected as work product, although that protection will be waived if the expert is called to testify as an expert witness at trial.

Work-product protection applies only to documents and things *prepared in anticipation of litigation or for trial*. Thus, documents and tangible things prepared in the course of an in-house or other pre-litigation investigation, even if at the direction of an attorney, may not be privileged if they were not prepared in anticipation of litigation. Just because there is a possibility of future litigation does not mean that the investigation is in anticipation thereof. Litigation must be actually planned and the work for which protection is sought must have been undertaken for the specific purpose of preparing for that litigation. But if the work to

be protected was done in anticipation of litigation, then it does not matter in most jurisdictions that no lawsuit has been filed yet.

The work-product doctrine protects documents and things prepared in anticipation of litigation from compelled disclosure, but it does not render the facts themselves confidential, privileged, or non-discoverable. Thus, while reports, interview notes, and transcripts might not be discoverable under the doctrine, the facts learned may be discoverable. Similarly, the work-product doctrine does not prevent discovery of the identity of witnesses and the existence of interview notes, tapes, or transcripts.

Moreover, the extent to which interview notes, transcripts, and other factual reports prepared in anticipation of litigation are actually protected from discovery by a party opponent may vary between jurisdictions and may depend on the facts and circumstances of a given case.

Like the attorney-client privilege, work-product protection can be waived.

The Litigation Privilege

The *litigation privilege*, which is present in the United Kingdom and Canada, is roughly comparable to the U.S. attorney work-product doctrine. The litigation privilege prevents the disclosure of communications made, and documents prepared, for the purpose of litigation. The privilege, like the work-product doctrine in the United States, may extend to communications of, and documents created by, third-party agents (e.g., consultants, fraud examiners, etc.) in preparation for litigation.

The litigation privilege arises once litigation is reasonably anticipated. Accordingly, communication is only privileged under the litigation privilege if litigation was contemplated at the time the communication was created. Therefore, the privilege does not cover documents that came into existence before litigation was contemplated.

General Professional Privileges in Civil Law Jurisdictions

Many civil law systems have general professional privileges that prohibit the admission of communications made through the exercise of certain professional duties. That is, general professional privileges apply to certain kinds of communications made during the course of professional relationships. In France, for example, the Penal Code provides for penalties if professional confidences are broken.

Self-Evaluation Privilege

The *self-evaluation privilege* (also referred to as the *self-critical privilege*) may provide some protection for the work product of an investigation conducted by an organization. This privilege is based on the need to encourage voluntary internal reviews and compliance programs. It will protect the work product of an organization's investigation if the organization can demonstrate that it is attempting to police itself in an area of public interest, and it can show that disclosure of its work product would prejudice its efforts to police itself.

Normally, for this privilege to apply, the information must be prepared by the organization with the expectation that it would be kept confidential, and the information must have remained confidential.

The self-evaluation privilege may apply even in the absence of anticipated litigation, and it does not require the participation of a lawyer.

The privilege is a relatively new concept and is not recognized in all jurisdictions. It is much weaker than the legal professional and litigation privileges.

Marital Privilege

In many jurisdictions, the *marital privilege* (also called the *spousal privilege*) protects communications between husbands and wives, and it is designed to encourage harmony between spouses. The marital privilege, however, differs between countries.

In the United States, there are two forms of the marital privilege: (1) the confidential communications privilege, and (2) the adverse testimony privilege. The *confidential communications privilege* protects the contents of confidential communications between spouses during their marriage, and it enables either spouse to prevent the other from testifying about a confidential communication made during marriage. The *adverse testimony privilege* protects spouses from being compelled to testify against each other while they are married. Usually, the confidential communications privilege continues after the termination of the marriage; the adverse testimony privilege does not.

Many European jurisdictions, including Switzerland, the Netherlands, and Italy, have spousal communication privileges that prevent spouses from being forced to testify against each other.

Spousal communications, however, are not privileged in England and Wales, but Section 80 of the Police and Criminal Evidence Act 1984 gives spouses or civil partners of criminal defendants protection against being compelled to testify by the prosecution, except in limited circumstances.

Parent-Child Privilege

Many European jurisdictions recognize a privilege that prevents parents and children from testifying against each other, but no such privilege is widely recognized in the United States.

Similarly, there is no privilege that permits a person not to testify against other family members, although, as a matter of policy, many law enforcement agencies will not compel testimony from immediate family members.

Law Enforcement Privilege to Withhold the Identity of an Informant

In some jurisdictions, law enforcement agencies may legitimately withhold the identity of an informant unless disclosure is necessary to ensure that the defendant receives a fair trial. In such circumstances, the prosecution has to decide whether to forego prosecution or disclose the identity of the informant. In the private sector, there generally is no equivalent privilege. Certified Fraud Examiners or others who are investigating on behalf of a private client may be compelled by court order to disclose the identity of an informant or any other witness. This possibility should be disclosed to potential witnesses who may request confidentiality.

Accountant-Client Privilege

Some jurisdictions may have an *accountant-client privilege* that protects the communications between an accountant and client, although most common law jurisdictions do not recognize any such privilege. Even so, English law recognizes a limited accountant-client privilege, and in the United States, a few states have a weak accountant-client privilege that allows an accountant to resist production of a client's work papers or documents. No such privilege is recognized under U.S. federal law, and the state privileges may be overcome by a showing of need or by the service of a subpoena.

Other Privileges

There are a number of other privileges that are less likely to be asserted in fraud actions, including the *priest-penitent* and *physician-patient* privileges.

Judicial Treatment of Privileges from Foreign Jurisdictions

The rise of global markets and multijurisdictional transactions has resulted in an increase in disputes that span multiple jurisdictions, and as the above discussion on privileges demonstrates, the privileges that are available vary substantially by jurisdiction. There are no standardized rules and, in some cases, privileges might conflict. For example, the litigants in a cross-border dispute might be required to disclose information in one jurisdiction that is privileged in another jurisdiction. Accordingly, privilege law is a key source of uncertainty for litigants in cross-border disputes.

Generally, individuals involved in cross-border litigation should not expect to have the privilege laws from their own jurisdiction applied when engaged in litigation abroad. There are several reasons for this. First, courts are more inclined to apply their own privilege law because they are more familiar with local law than the laws of foreign jurisdictions. Second, characterizations and conceptualizations of privileges vary among different countries. For instance, common law jurisdictions typically view privileges as the right of the client, but civil law jurisdictions do not. In civil law jurisdictions, communications are protected by secrecy laws that require confidentiality.

TESTIFYING

Introduction

Testimonial evidence is evidence presented in the form of statements made during a legal proceeding, such as a trial, an administrative hearing, or a deposition. All testimonial evidence has specific requirements governing its admissibility that depend on the type of witness and the manner in which the witness is testifying. The judge or administrator applies these requirements to determine who can testify and what they can testify about.

Witness testimony, however, differs in adversarial and inquisitorial jurisdictions. Again, adversarial jurisdictions (which are typically common law countries) are those that use judicial processes in which the parties to a proceeding drive the discovery process (the search for evidence), and inquisitorial jurisdictions are those that use judicial processes that place the primary responsibility of discovering evidence on the presiding judge. In adversarial systems, a large amount of litigation is conducted using oral evidence, with witnesses offering testimony, being examined in direct examination by their representatives, and, in turn, cross-examined by opposing counsel. Conversely, in inquisitorial systems, the examining judge interrogates witnesses, and it is up to the judge to decide the value of witness testimony. Furthermore, adversarial systems give more weight to testimonial evidence than inquisitorial systems, and cross-examination of witnesses is virtually non-existent in inquisitorial systems.

Certified Fraud Examiners, accountants, and auditors often are called upon to provide testimony in criminal and civil prosecutions where their services can be used to support investigations of matters such as financial frauds, embezzlements, misapplication of funds, bankruptcy fraud, improper accounting practices, and tax fraud. Fraud examiners may also be used as defense witnesses or to support the defendant's counsel on matters that involve accounting or audit issues.

There are two basic kinds of testimony. The first is *lay testimony* (sometimes called *factual testimony*), where witnesses testify about what they have experienced firsthand and their factual observations. The second kind is *expert testimony*, where a person who, by reason of education, training, skill, or experience, is qualified to render an expert opinion regarding certain issues at hand. Typically, a fraud examiner who worked on a case will be capable of providing lay testimony based on observations made during the investigation. When a trial involves issues that are complex or unfamiliar to most people, as is common in incidents of

fraud, expert testimony is appropriate to help the fact finder understand these issues. The type of testimony provided by the fraud examiner depends on both his role in the case and whether he is qualified to provide expert testimony. If a fraud examiner who participated in the investigation also qualifies as an expert regarding a relevant issue, he might provide both lay and expert testimony. Alternatively, the witness might solely be used either to present factual evidence or to provide a particular expert opinion based on the facts.

Many of the considerations for providing testimony are the same, regardless of whether it is factual or opinion-based. However, there are also some important distinctions, which are discussed throughout this chapter.

Considerations for Testifying as a Lay Witness

A *lay witness* (or *fact witness*) is anyone who provides nonexpert testimony in a legal proceeding. Before testimony begins, fraud examiners serving as fact witnesses will need to lay the proper groundwork. That is, to be an effective fact witness, fraud examiners must investigate, prepare, and disclose.

There are basic competency requirements for all witnesses. For fact witnesses, competency relates to the witness's capacity for observation, recollection, and communication. As will be discussed later in this chapter, there are heightened capacity requirements for those who are presented to give opinion evidence—either lay opinions or expert opinions.

Information Versus Evidence

Witnesses—particularly those involved in an investigative process—must appreciate the difference between information and evidence. Information consists of all facts, documents, observations, statements, or other indications of what happened. Evidence is information that is presented at trial, under the supervision of the judge, to prove or disprove an alleged fact at issue (i.e., to convince the judge or jury of the truth or falsity of the fact at issue).

The effective fraud examiner must not let concerns about the admissibility of investigative information or "leads" limit the scope or tenacity of the examination. Even if information is not in and of itself admissible, such information might lead to the discovery of admissible evidence.

Similarly, the effective witness does not get bogged down or excluded simply because the underlying information is inadmissible in court. Sometimes admissibility depends on the form of the information or prior disclosures; other times, it depends on whether specified procedures were followed. Therefore, all witnesses should work closely with their lawyers to make sure that all important information can be presented as evidence.

Sources of Lay Testimony

The rules of evidence, which govern the admissibility of evidence in court, prefer factual testimony based on firsthand knowledge (i.e., testimony on matters that the witness has perceived through one of the senses). There are several permissible sources for factual testimony:

- Observations
- Information collected during investigations
- Calculations and summaries
- Research
- Opinions (typically limited in scope)

Testimony derived from personal involvement in any of the sources enumerated in this list will generally be more effective and more easily admitted than all other types. Even if a witness is admitted as an expert, maximum exposure and reliance on direct rather than derivative information will increase the likelihood that the witness's statements will be admitted as evidence.

Use of Summaries

Whenever one party wishes to introduce an item of evidence, the other side is typically entitled to inspect such evidence. Nonetheless, when certain items of evidence are so voluminous that they cannot be conveniently examined in court, some jurisdictions allow the contents thereof to be presented in the form of a chart, summary, or calculation. When this occurs, the original documents (or duplicates) should be made available for examination or copying by other parties at a reasonable time and place, and the court may order that the underlying documentation be produced in court.

Opinions by Lay Witnesses

As a general matter, fact witnesses can only testify about the things they have personally observed and cannot give opinions or conclusions. However, some jurisdictions might allow some types of opinions from fact witnesses. For instance, under state and federal law in the

United States, a fact witness might be allowed to testify in the form of an opinion when such opinion is: (1) rationally based on the perception of the witness (i.e., one that a normal person would form from those perceptions) and (2) helpful to a clear understanding of the witness's testimony or the determination of a fact in issue.

Lay witnesses are commonly allowed to testify as to:

- The appearance of persons or things
- Identity
- The manner of conduct
- Competency of a person
- Degrees of light or darkness
- Sound, size, weight, or distance
- State of mind, including intent

EXAMPLE

Steven Dalton is called to testify as a lay witness in the fraud case against his boss, Frank James. As a lay, or fact, witness, Dalton, can say that he found his boss frightening. Often, James tromped up and down the office hallways yelling at subordinates. Dalton can also say that James kept the bottom right-hand drawer of his desk locked and that he became extremely irritated if anyone asked him what was in it. But as a fact witness, Dalton cannot offer opinions about James's psychological state or how he believes that James's desk contained information about a fraud scheme in which he thinks James was involved. Dalton must limit his testimony to those things he's actually seen, heard, and otherwise experienced.

EXAMPLE

Most courts would allow the owner of a business to testify as to the value or projected profits of his company without qualifying the owner as an accountant, appraiser, or similar expert. Such opinion testimony by a fact witness is not admitted because the witness possesses the broad range of experience, training, or specialized knowledge of an expert, but rather because he possesses particularized knowledge—as to his specific company—by virtue of his position in that company.

Generally, lay witnesses are restricted from providing expert opinions. In the United States, for example, Federal Rule of Evidence 701 prohibits lay witnesses from providing opinions based on scientific, technical, or other specialized knowledge. Under the rule, the distinction

between lay and expert testimony is that a permissible lay opinion "results from a process of reasoning familiar in everyday life" while expert testimony "results from a process of reasoning which can be mastered only by specialists in the field." Note that FRE 701 does not bar an expert from testifying as a lay witness; the same witness can provide both lay and expert testimony in a single case.

Considerations for Testifying as an Expert

Litigation involving fraud is often complex, and the parties or the court might seek the help of experts. Experts can serve one of two roles in the trial process: testifying expert or consulting expert. *Testifying expert* witnesses give opinion testimony when specialized knowledge is needed to help the fact finder understand evidence or determine a fact in issue. Conversely, *consulting experts* typically do not testify at trial. Instead, they are hired to provide technical assistance to the attorney in preparing the case. In adversarial processes, both testifying and consulting experts play an ongoing part with the litigation team for both sides. In inquisitorial processes, however, the court hires the expert to testify on technical issues.

Although experts serve one of two roles, they can perform various functions throughout the litigation process. Lawyers often count on testifying experts to help crystallize the judge or jury's understanding of the case. In his book, *Effective Expert Witnessing*, author Jack V. Matson lists the four main functions of all expert testimony and offers advice on fulfilling each assigned duty:

- *Establish the facts*. You must first develop a strategy to collect and examine the documentation in the case. The discovery process, which is a mechanism for full disclosure of all knowledge pertinent to the case, usually yields a vast amount of paper, which the expert then must sift through to make a preliminary classification of relevance.
- *Interpret the facts*. Tie together cause and effect relationships with the data and the facts for the technical basis of your case. Do not be fooled by correlation that seemingly links cause and effect but holds no theoretical justification.
- *Comment on the opposing expert's facts and opinions*. If engaged in an adversarial proceeding, develop a good understanding of the opposing experts by reviewing their educational background and experience. Read their publications. Probe for weaknesses that your side might exploit. Oftentimes, trials become a battle of the experts. Prepare for the battle with as much intelligence as you can muster. Take apart the opposition's expert report, which represents the other side's best case, piece by piece. Your attorney needs to know the most intimate details about the facts and opinions contained in that report.

- *Define the professional standards in the particular area of your opponent's expertise*. One of the most critically important ways an expert is used in trial is to define the "standard of care" exercised by fellow professionals in the field. *Standard of care* has been traditionally defined based on judgment normally exercised by professionals in good standing. Additionally, the professional must be informed or aware of current practices and promulgation. Obsolete practices are now considered by the court to be negligent practices. Thus, professionals must exercise reasonable, informed judgment in carrying out their duties. You, as the expert, will be called upon to define the professional standard.

Depending on the rules of the jurisdiction, the expert witness may be called by the court (i.e., the judge) or the parties. If called by the prosecution or plaintiff, fraud examiners might testify to their findings, and if called by the defense, they might testify regarding opinions expressed by the prosecution's or plaintiff's expert—to create doubt in the fact finder's mind about the credibility or weight to be given to that expert.

Alternatively, an expert might be called upon to give an opinion different from that reached by an equally credible expert called by the court or on the other side. This might be due to different interpretations of the facts of the case. In some instances, given equally plausible alternatives, the case might be decided on which expert witness was the most credible.

Additionally, effective expert witnesses frequently share certain characteristics. Credibility is one such feature. To become a "credible" expert witness, one must be a member in good standing of the profession and usually be recognized as an authority in that profession or some specialized aspect of practice within it.

Similarly, an expert witness in the area of accounting must have a thorough knowledge not only of generally accepted accounting principles, but also of current promulgations. The expert's expertise often might involve special knowledge of a specific industry. In this case, the expert should be aware of recent developments and any important issues within that area.

The expert also must be analytical and be able to work with incomplete data. The expert, however, might not always be able to recognize when data is incomplete. As a result, the expert might make assumptions that will then be open for interpretation or attack. If all data

have not been made available to the expert, then a party might be able to offer alternate scenarios that are more plausible under the circumstances, thus discrediting the expert.

Accepting the Role of a Testifying Expert

Serving as a testifying expert is a difficult task, but it can be a rewarding experience. Before accepting a role that could potentially require testifying as an expert, the examiner must be capable of doing so and confident that the testimony will be helpful.

Ideal expert witnesses need to be respected experts in their fields and continue learning throughout their careers. For Certified Fraud Examiners, that means completing Continuing Professional Education (CPE), regularly reading publications in the specific field, and actively seeking new developments. Fraud schemes and the investigation and prevention measures associated with them are always evolving, so the ideal expert will stay on top of these issues.

Additionally, a fraud examiner needs to confirm that the requested testifying role is within the scope of his skills. For example, a fraud examiner might have a long history in securities fraud, but that does not mean that he is qualified to testify in a case that will require appraising assets. Experts must reject work outside of their scope for the interests of the retaining parties and their own careers.

When an expert is asked by a party to provide expert testimony, it is usually easy to see what that party wants the expert's testimony to be—whatever will most help the party win. An expert must make sure that his analysis is objective and not shaped by the retaining party's will.

Asking the right questions of the retaining party in the beginning is necessary to avoid becoming an expert witness in a case in which the expert should not be involved. The types of questions necessary depend on the case, but in general, the expert should ask:

- Who are all of the parties and potential parties to the litigation?
- Who are the other attorneys for all of the parties?
- Who are the other experts in the case?
- What are the basic facts of the case?
- What is the scope of subject matter the party is requesting expertise for?
- Is the party seeking a consulting or testifying witness (discussed later in this chapter)?
- Are there any known or potential conflicts of interest?

- What court or administrative body will hear the case and what procedural rules should the expert know about?
- How will communications work (e.g., will the clients be contacted directly)?

Conflicts of Interest

When retained, experts must quickly determine if any conflicts of interest exist—or even appear to exist—in a particular case because a conflict might preclude participation. A *conflict of interest* exists when an expert's ability to objectively evaluate and present an issue for a client will be impaired by any current, prior, or future relationship with parties to the litigation. Prior or ongoing relationships might suggest to others that the expert cannot provide undivided loyalty to the cause and the client. Whether a relationship causes a conflict of interest depends on the facts. Simply meeting a person does not necessarily cause a conflict, but a close personal or business relationship is more likely to give the perception of a conflict.

There are several actions an expert can take to determine if any conflicts of interest exist. For example, before an engagement an expert can ask for the names of all parties involved, and then review the names with his associates to disclose any connections, however remote.

Compensation (whether from the parties or from the court) for expert testimony services is standard, and it is not generally considered a conflict of interest. The amount of compensation can be brought up at trial, so the payment should not be above normal.

Penalties for consulting or acting as an expert in a conflict of interest include expert disqualification, attorney disqualification, and inadmissibility of expert testimony.

Divergences in Adversarial and Inquisitorial Jurisdictions

While most jurisdictions have procedures for admitting expert testimony in judicial proceedings, adversarial and inquisitorial jurisdictions tend to take different approaches. The biggest difference is the party retaining the expert.

Adversarial jurisdictions (which are typically common law countries such as the United States) usually allow the parties to litigation to retain experts to either consult or testify in proceedings, meaning the parties pay the experts directly. Each party might obtain its own expert, and it is common to have competing expert testimony in a proceeding. The parties are given an opportunity to both question their own expert in front of the judge or jury, as

well as cross-examine the other party's expert to potentially reveal weaknesses in that expert's methods or analysis. The fact finder (i.e., the judge or jury) must weigh these competing expert opinions.

In most inquisitorial jurisdictions (which are typically civil law countries), the court hires its own expert witnesses for technical issues that require guidance. This expert provides the court with information, and the judge has the discretion to determine whether to apply the expert's testimony when deciding issues. Unlike in adversarial jurisdictions, in inquisitorial jurisdictions, it is primarily the judge's responsibility to elicit the testimony from the expert. However, the parties' representatives can ask the expert questions, and in some cases can challenge the expert's qualifications or testimony. In some inquisitorial jurisdictions, the parties might also be able to (or be required to) make experts available for the court-appointed expert to question. Therefore, while not procedurally the same, expert witnesses in both adversarial and inquisitorial systems must be prepared to have their testimony withstand the scrutiny of the opposing party's legal counsel or the court-appointed expert.

While a jurisdiction's classification of being either adversarial or inquisitorial tends to determine its procedures for admitting expert testimony, this is not always the case. For example, Spain is a civil law country with an overall inquisitorial system, but it takes the adversarial approach of letting the parties obtain their own experts.

There are various other differences between adversarial and inquisitorial jurisdictions discussed throughout this chapter.

Pretrial Preparation in Adversarial Proceedings

Pretrial preparation remains key to becoming a successful expert witness, and success often depends on full inquiry and thorough investigation. In adversarial proceedings, the discovery process occurs in the pretrial stage, and an expert may provide assistance during this phase of litigation. An expert may help by composing discovery requests or answers. A financial expert is often expected to educate a lawyer on the types of documents typically available for certain cases.

Many times, financial crime experts must search through extremely large numbers of documents or computer files to determine whether evidence of fraudulent intent or behavior exists. The parties might overwhelm the other side with paper or electronic documents to

hide or trivialize vital documentation. Because an efficient search saves time and money, successful experts develop an early strategy to achieve their goals within a specific period.

When testifying as an expert, it is often useful to obtain a list of all other witnesses, including other testifying experts. This is important so that the expert is not surprised by the existence of other experts or reports. One can then determine if it is necessary to be present for the testimony of those witnesses and can obtain the necessary court approval. If other experts will be present, then it becomes incumbent upon the expert witness to examine the other experts' reports and assess whether they contain reasonable points that might affect the credibility of the expert witness's report.

Experts who are testifying need to be keenly aware that their communications with counsel or the judge will often get turned over to the parties. The best approach is to assume that each communication regarding the case will be heard or read by all parties to the litigation.

Discoverability of Expert's Reports

At some point during litigation, parties have a chance to examine an expert's opinions and underlying rationales. Caution is the by-word for expert witnesses at every step of the legal process. Reports and supporting documents used by experts might have to be disclosed to the opposing side in adversarial processes, and the parties in inquisitorial processes might also have a chance to review such documents. Therefore, experts should be cautious about what records they have. Fraud examiners should always consult with the party or court retaining them concerning the information in the report and the documents used to prepare the report.

Keeping Good Files

The best way to protect the confidentiality of information is to keep good files. Dan Poynter, the author of *The Expert Witness Handbook*, reports that experts routinely "reduce their files to useful reports only" once they have been officially engaged as a witness for trial.[1] No one is recommending that files be *sanitized*, Poynter adds, just *updated*. The difference may be subject to abuse, but it is simple: Any materials that serve as the basis for an expert's opinion must be in the file. Notes, documents, or tests that serve as background or represent unfruitful lines of investigation do not have to be included and probably should not be. The lawyer trying the case doesn't want an expert having to answer about dead ends

[1] Dan Poynter, *The Expert Witness Handbook* (Santa Barbara: Para Publishing, 1997), p. 82.

or exploratory jaunts; a shrewd cross-examiner can turn a hastily scribbled hypothetical into just enough "reasonable doubt" to raise concern regarding the accuracy of an expert's testimony. So, in the best-case scenario, an expert presents to the court an opinion and its basis—nothing more, nothing less.

Qualifying to Testify as an Expert Witness

Before an individual can testify as an expert, the proposed witness must be qualified as an expert. But what constitutes expert status? Generally, the term *expert witness* refers to someone whose education and professional credentials establish his knowledge of a particular set of practices.

The process for qualifying as an expert varies by country, but there are some common approaches in adversarial and inquisitorial jurisdictions.

Qualifying to Testify as an Expert in Adversarial Jurisdictions

Parties introduce expert witnesses, so they are tasked with proving that an expert witness is qualified to give such testimony. As with introducing exhibits in trial, counsel must lay a foundation for the expert's testimony. This means showing that by formal education, advanced study, or experience, the witness is sufficiently knowledgeable on the subject at hand. That is, a witness must be qualified to testify as an expert. The foundation may be established during the pretrial stage or during direct examination.

Generally, before allowing an expert to testify before the jury, the judge will make three determinations:

- Is the person qualified as an expert witness?
- Will the expertise of the witness assist the jury in understanding the evidence or determining a fact at issue? In other words, is the proposed testimony relevant to the facts of the case?
- Is the testimony reliable?

Qualification Requirement

Before admitting expert testimony, the judge must determine that the expert is a qualified practitioner. This element addresses whether the individual is qualified to assist the trier of fact.

The process of evaluating whether an expert is qualified mainly centers on the candidate's formal education and work experience—whether that includes 30 years in law enforcement or ten years in a large accounting firm. But there is no standard educational requirement for expert testimony; a witness with no formal education may be qualified based on training or experience. Some other factors that may be considered include the candidate's:

- Awards and honors
- Licensing or certification
- Technical training
- Published books and journal articles
- Positions in professional associations, societies, and organizations

In addition to being qualified as an expert, the expert's qualifications must be relevant to the particular issue(s) in the case at hand.

But the important thing to remember is that a person can be qualified as an expert based on either special training or experience. A person does not have to be a CFE to testify as an expert on fraud prevention, detection, or investigation techniques if that person has sufficient practical experience in those techniques. The CFE designation is important because it serves as recognition of the special skills that those holding the designation have demonstrated to become a CFE. A professional designation does not, however, automatically qualify someone as an expert for purposes of testifying in court.

Although designations are important, it is most helpful to have prior experience as an expert with litigation or criminal matters. This is primarily because of what is learned during the experience of testifying.

Further, it often is helpful to have been accepted as an expert in other cases thereby easing current acceptance. A danger exists, however, if a witness serves as an expert on behalf of litigants in many cases because he could appear to be a "professional witness."

To establish the candidate's expertise, the counsel introducing the expert witness often will read the expert's qualifications or ask specific questions to establish the witness's credentials. Smart defense lawyers are not likely to challenge the credentials of experts, assuming they meet at least minimum standards of professional competence. To do so may give these experts an opportunity to fully highlight their professional credentials and perhaps make a

greater impression on the jury or judge, thus adding more weight to their testimony. Although expert qualifications are not often contested, it does happen.

Relevant and Reliable Requirement

After determining that a witness is a qualified expert, the trial judge must determine that the testimony being offered by the expert is relevant to the facts of the case and reliable. These two questions focus on what opinions the expert will actually testify to in court.

Relevant testimony will assist the jury in understanding the evidence or determining a fact at issue. To be relevant, the proposed testimony must be sufficiently related to the facts of the case so that it will aid the jury in resolving a factual dispute." That is, the testimony must have a tendency to make the existence of any fact more probable than it would be without the evidence. Testimony is not relevant if the jury can make its own determination without expert testimony.

To be reliable, the testimony must be based on sufficient facts and data, and it must be the product of reliable methodology that has been reliably applied to the facts of the case. This ensures that an expert's opinions are not mere speculation.

Accordingly, fraud examiners should be sure to fully cover the rationale for their assumptions and determine whether the assumptions are supported by the facts.

When preparing an expert report or testimony, examiners should keep in mind the principles set forth above. Fraud examiners should document their conclusions, how they reached those conclusions, what evidence they based the conclusions on, and what professional techniques or knowledge they used. Additionally, it is a good idea for expert witnesses to keep a list of professional books or journals that advocate or sanction whatever principles they used in drawing their conclusions.

Qualifying to Testify as an Expert in Inquisitorial Jurisdictions

The primary experts in inquisitorial jurisdictions are usually appointed and presented by the judge, rather than the parties. Like in adversarial jurisdictions, the judge makes the final determination of whether an expert is qualified. However, most inquisitorial jurisdictions have more standardized requirements.

Many jurisdictions (through the courts, chambers of commerce, or other organizations) maintain lists of experts in particular fields from which the courts may choose for the case at hand. These experts are qualified if they meet national standards, such as being certified in a particular field (e.g., an accounting certification). Some jurisdictions allow judges to look outside of the lists for experts. Due to the maintenance of expert lists and the relatively low perceived bias of experts in inquisitorial jurisdictions, it is acceptable for expert witnesses to offer their services in court more often than in adversarial jurisdictions.

After being initially selected by the judge, expert witnesses are usually required to submit a report to the court and are subject to questioning by the parties to the litigation. The parties' representatives may ask questions concerning the expert's qualifications, potential biases, and report, but are generally more limited in the scope of questioning than parties in adversarial proceedings. The judge has already reviewed the witness by this point and there are generally more specific requirements in inquisitorial systems, so there is a lower perceived need to allow parties to challenge the expert.

Preparing to Testify

The majority of cases filed will not go to trial; most civil cases are resolved through a *settlement agreement* (a voluntary agreement resolving part or all of a dispute), and, in common law countries, most criminal cases result in a *plea bargain* (a negotiation whereby a criminal defendant agrees to plead guilty to a lesser charge). Therefore, most witnesses' experience in testifying comes through having their depositions taken.

Depositions

In many countries, depositions are available as a means of gathering testimonial evidence. A *deposition* is sworn testimony given by a party or witness upon questioning by counsel for one of the parties before trial and outside of court. A deposition serves as a powerful discovery device that may be used to compel anyone associated with the case to give oral testimony under oath. Although the subject cannot decline to testify in a deposition, he may be allowed to specify a convenient time and place for the deposition. In addition, a deposition may be recorded by a court reporter, camera, or a voice recorder.

For skilled investigators, depositions provide an opportunity to hear the other side's case aloud, but the opposition may set ulterior goals as well, including:

- Learn new information or confirm existing facts.

- Appraise the subject's ability as a witness.
- Lock the subject into a hard-to-defend position.
- Create a written record for future impeachment.

Before testifying at a deposition or at trial, the witness should ensure that required graphic displays are ready and available and that the witness has a complete understanding of the report and other relevant issues. Many witnesses have been discredited in depositions or at trial because they could not explain details of a report, such as how a particular calculation was made. The witness should ensure that he agrees with counsel as to the sequence of evidence and the strategy for presenting it.

At pre-testimony meetings, it is appropriate to discuss the expert's qualifications (if applicable) to ensure that they are current, to discuss the strengths and weaknesses of the case, and to discuss and agree on what parts of the fraud examiner's reports, if any, are to be entered as exhibits.

Additionally, witnesses should pore over the written transcription of the deposition afterward to ensure accuracy, immediately correcting any omissions or errors, whether made by the witness or the stenographer. In the case of expert testimony, experts should notify their retaining party if their opinion changes after a deposition. If the expert is present at the deposition of an opposing expert, the expert may be asked to summarize his impressions afterward and note any gray areas that call for further inquiry.

Appearance and Composure

The appearance of the witness often lends itself to an assessment of his credibility. It is recommended that witnesses wear conservative business attire, be well groomed, and be neatly dressed.

It is also important that the witness maintain a professional demeanor. In the witness box, the witness should maintain a poised, alert appearance, stand firmly, and be ready to take the oath. The witness should not smile gratuitously at the judge, jury, or the lawyers. Also, it is important that the witness keep control of his hands to avoid fidgeting. The witness should maintain eye contact with the questioner as much as possible; he should not stare off into space, at the floor, or at the ceiling.

Because the judge will be taking notes during the testimony, witnesses should speak slowly to ensure that the judge does not fall behind.

The witness should direct his answers to the questioner, and his voice should be strong, clear, and audible. Thus, before answering each question, the witness should pause before answering and carefully consider the answer; he should also respond in a slow and deliberate manner.

Dos and Don'ts

There are other considerations in being a credible witness. Some tips are:

- Exude a confident attitude.
- Maintain professional pride and integrity throughout.
- Tell the truth; be honest and avoid bias.
- Use simple rather than complex terms, and refrain from using professional jargon where possible.
- Explain complex concepts in a layperson's terms.
- Be friendly and polite to all parties present.
- Be alert.
- Correct any misstatements as soon as they are detected.
- Listen carefully and answer the specific questions—do not go off on tangents or volunteer more than the question requires.
- Do not verbally fence with the questioner.
- Do not try to be humorous or hip.
- Be calm and deliberate in responding to questions—think before you speak.
- Plan your testimony in advance and know your material thoroughly.
- Use graphs, charts, and other visual aids if they help to clarify a point.
- Do not read from notes if you can avoid it (the opposition lawyer will probably demand to see such notes, and the witness will then look like he rehearsed his testimony).
- Prepare your material completely. If you have documents to introduce, have them organized so that you can quickly retrieve them when asked to do so.
- Do not "hem and haw" or stammer; recover your composure when a tough or complex question is posed.
- Ask for a question to be repeated or clarified if not fully comprehended.
- If an answer is not known, say so; do not guess.
- Do not invent and do not inflate.
- In cross-examination, do not respond too quickly because counsel might wish to object to the question.
- Do not be evasive.

Several other things should also be avoided. These range from conspicuous activities like drinking five cups of coffee immediately before testifying to small physical mannerisms that might affect your appearance. These mannerisms, which might be as simple as rubbing one's hands together continually, looking down at one's hands, fidgeting on the stand, or jingling coins in a pocket, could become irritating to the judge or jury.

In depositions and at trial, the judge or the opposition might drill a witness about his report, credentials, methodology, and conclusions pertaining to the case. If a witness is being questioned critically, then the witness often answers tersely, giving only a straight "yes" or "no." For inquiries that require more, witnesses should respond directly and precisely and refrain from volunteering any information.

Direct Examination

Direct examination is the initial questioning of a witness by the party that called the witness (in adversarial jurisdictions) or the judge (in inquisitorial jurisdictions). Most of the time, direct examination is a nonconfrontational questioning aimed at exposing the facts and issues of the case. It is usually not as treacherous as cross-examination—where opposing parties challenge the witness's testimony—but still requires a good strategy for answering questions, knowledge of the case, and self-awareness.

Direct Examination for Lay Witnesses

When a fraud examiner testifies as a fact witness, the direct examination generally proceeds from setting a background—who the witness is and the person's relation to the case—to establishing the witness's personal knowledge of the relevant material. Nonexpert witnesses must have some firsthand mental or sensory impression on which to base testimony. They generally can't discuss things they've only heard about or surmised. Conversations may be admissible, but only if details can be fully established, such as who participated, where and when the conversation took place, and so on. To be allowed, a conversation has to show relevance to the proceedings. Note, however, that inquisitorial jurisdictions tend to be less restrictive as to what testimony is allowed than adversarial jurisdictions.

As with an interview, the questions put to a witness can be broadly categorized as open or closed. Open questions ask for a detailed response: "What was it about the ledgers that made you call them 'irregular' in your report?" The witness offers a summary of the irregularities in his own words. A closed question, conversely, asks for a direct answer: "Did you remark that

the ledgers were in an 'irregular' state?" Closed questions are usually answered with yes or no, unless they're aimed at extracting some particular piece of information. For example, the attorney might ask, "What was the word you used to describe the state of the ledgers?" The witness then replies, "I called them 'irregular.'" A combination of open and closed questions is often used during direct examination.

Direct Examination for Expert Witnesses

Expert witnesses, like lay witnesses, are subject to direct examination, but the direct examination of an expert witness will differ somewhat from that of lay witnesses.

Adversarial Versus Inquisitorial Direct Examinations

Recall that most expert witnesses in adversarial proceedings are chosen by the parties to the litigation (although adversarial courts may also appoint independent experts), while judges in inquisitorial courts typically appoint their own experts to evaluate technical matters. These relationships largely impact the dynamic of providing expert testimony in direct examinations.

In adversarial systems, the expert and the retaining party are "allies" in the sense that legal counsel will attempt to paint the expert's testimony in the best light during direct examination and will try to correct any issues in the expert's testimony that the opposing party raises. Additionally, the party retaining the expert might try to prepare the expert for the types of questions that will likely be asked. However, it is important that the expert never allow his opinion or best judgment to be supplanted by that of the retaining party. The expert must maintain objectivity, despite the obvious shared interest.

Most inquisitorial systems have a different dynamic, where the primary experts are appointed by the court. Expert witnesses in inquisitorial jurisdictions are subject to various examinations, and might have to conduct their own examinations of witnesses. Usually, all of the expert's activities related to the case are controlled by the judge, who determines the scope of the expert's analysis, the expert's authority to access certain items of evidence, whom the expert can interview, and several other functions. Because some jurisdictions allow parties to submit testimony or evidence from their own experts in addition to the court-appointed expert, the latter might need to interview the parties' experts. The expert should carefully follow the judge's instructions, especially since the instructions are usually made available to the parties of the proceeding.

The expert's findings are often requested in written form, but the expert might also have to answer oral questions from the judge and the parties' legal counsel.

In some ways, the expert's job in an inquisitorial system is easier than in adversarial systems because there is less assumption that the expert is biased toward one of the parties. However, the expert might have broader investigative responsibilities, depending on the judge's orders.

The same rules of integrity and professionalism for experts apply equally in both adversarial and inquisitorial proceedings.

Expert Reports

Experts typically create written reports regarding their analysis of the case. In adversarial processes, these reports are written in the pretrial stage and presented during direct examination by the party who retained the expert.

In inquisitorial processes, written reports are generally the only form of expert testimony presented, but the expert might also provide oral testimony. If there is oral testimony, the judge performs the direct examination. Because experts are hired for their opinions, they are often not subject to the usual restrictions about statements of judgment. Experts also have other leeway not given to ordinary witnesses. They may rely on documents or exchanges that would otherwise be inadmissible as hearsay. This allows them to use articles, academic papers, professional texts, and consultations in rendering their opinions of the case. These materials are typically admissible as long as they were used by the expert in developing his opinion.

Question and Presentation Style

Expert witnesses present their findings in various ways, such as narrative questions, hypotheticals, specialized materials, and special exhibits. Experts are commonly asked to answer *narrative questions,* which are broad, open-ended questions that allow experts to present their opinions in their own words with minimal prompting. Fraud cases, with their divergent paths of activity and intrigue, can require complex summarizing for the facts to make any sense. Average jurors and some judges have never considered how someone could manipulate store inventories to drive up the company's stock price and then make a profit on the phony surge. The expert witness in cases dealing with such issues often will begin testimony by recounting the narrative background of a case, the tests and experiments that

were performed during the investigation, and a summary of the findings based on his professional expertise.

For example, during a direct examination, the judge or counsel for the party presenting the expert witness might ask open questions, such as, "Could you please tell us about the background of this case?" or "What procedures did you perform in your examination?"

Compound (two-part) and hostile questions do not generally occur in this process. Additionally, leading questions are generally not allowed during direct examination (e.g., "The results were negative, weren't they?").

Expert witnesses also are typically allowed to demonstrate their findings by using *hypotheticals*, which are fictional situations, analogous to the act in question, that clarify and highlight particular aspects of the dispute. But to be effective, hypotheticals must be constructed exquisitely. Appeals courts have been adamant that the facts of the case being tried have to be reflected directly in the hypothetical situation; there must be no exaggeration or obscuring in the presentation.

Publications and Exhibits

Experts sometimes use specialized materials in reaching and communicating their opinions, but generally, such materials must be used and relied on by people in the expert's relevant field. Also, these materials may be produced as part of the trial.

Finally, experts may use special exhibits to demonstrate facts about the case or some aspect of their opinion. These exhibits may include charts, diagrams, annotated documents, or photos. If the exhibit is offered to prove a fact, it must satisfy the rules applicable to any other piece of evidence in the case. In demonstrating a professional opinion, the role of the exhibit must be clear and its applicability to the present case justified, if necessary.

General Direct Testimony Considerations

The purpose of direct examination is to draw out the evidence to prove or disprove issues in the case. Most likely, this will only be a reiteration of what previously has been discussed between the witness and counsel (in adversarial proceedings) or the judge (in inquisitorial proceedings) outside the courtroom. It is still very important, however, for the witness to refresh his memory beforehand by reference to all relevant facts and data considered for the case.

Direct examination is the most organized aspect of the trial; it is the stage in which the witness's credibility must be established with the judge or jury.

According to the concept of the primary memory, people remember best what they hear first and last during a presentation. This often is a useful idea to employ in giving or structuring evidence. Another noteworthy point is that the fact finder in a proceeding often has a limited attention span in a long trial; thus, it is often useful to use a "grab/give/conclude" method of presenting evidence.

To a witness, the interpretation of questions and the ability to listen are crucial skills. Even though the witness might already have gone through a mock direct examination, it is critical that each question be carefully evaluated again—the witness should reflect upon the questions asked and not anticipate them (they might have been changed, anyway, since the time of rehearsal).

The answers to all questions should be clear and concise, and, where complex terms are used, they should be clarified. Similarly, expert witnesses should explain complex concepts in a layperson's terms and avoid professional jargon because the fact finders might not be familiar with esoteric or technical terminology.

Witnesses should avoid, or limit, the use of notes (if allowed) as much as possible, and they should strive to maintain eye contact.

If an expert witness is to give an opinion, he should state the opinion with conviction.

Certain standards for fraud examiners that apply when they testify are found in the ACFE Code of Professional Ethics (see the Fraud Prevention and Deterrence section of the *Fraud Examiners Manual*). Specifically, fraud examiners are prohibited from expressing opinions as to the guilt or innocence of any person or party. This is not to say that the witness cannot testify to the badges, hallmarks, or characteristics of fraud found in the case. It also does not mean that the fraud examiner cannot testify that, based on the evidence, he believes the accused might have committed the offense. However, the ultimate guilt or innocence of any person or party is the sole responsibility of the fact finder (judge, jury, arbitrator, etc.). The fraud examiner typically will not be permitted to testify to the ultimate fact questions.

Cross-Examination

Cross-examination refers to the questioning of one side's witness by the opposing side, and it is truly the highlight of the adversarial court system. Cross-examination, however, is uncommon in inquisitorial systems, although some civil law jurisdictions allow counsel for the parties to question witnesses in limited circumstances.

Cross-examination is geared to allow opposing counsel or another questioning party either to clarify or to make points at the witness's expense. It generally is the most difficult part of the trial process for any witness. Questions during cross-examination might concern anything that might refute or embarrass the witness. During adversarial cross-examination, the witness's credibility will constantly be called into question. Inquisitorial cross-examination tends to be less confrontational, but even so, it is still important for witnesses to maintain poise and credibility in such situations.

Adversarial Cross-Examination

The goals of the opposing counsel during cross-examination are threefold. First, opposing counsel will seek to diminish the importance of the testimony presented by the witness. Second, opposing counsel will seek to have the witness testify in support of the opposing position by providing a series of assumptions. Third, opposing counsel will attack the witness's report or expert opinion (as applicable) itself to show the inadequacies, thereby discrediting the opinion, the report, and the witness.

The opposing counsel can attack or question anything that has been said or entered into court. This includes notes, working papers, affidavits, reports, and preliminary trial or discovery transcripts. Often, cross-examination creates an atmosphere of confrontation and contradiction.

When being cross-examined, the witness must not take attacks or attempts to discredit personally. Throughout the process, it is important for the witness to maintain pride and professional integrity.

Opposing counsel wants to reduce or limit the impact of the witness's evidence—it is natural for a witness to feel a certain amount of apprehension, and this might do a great deal to keep the witness alert. The witness often can take a clue as to the tempo and reaction of the jury or judge to the evidence being presented. Slight changes in style and presentation could be made accordingly.

In adversarial proceedings, the opposing counsel usually has a plan of cross-examination in mind, and a witness should be able to anticipate this direction to prevent falling into a trap. A danger to this, of course, is that the witness will spend as much time planning ahead as answering the questions and might not be giving appropriate attention to the immediate questions. Further, in attempting to anticipate a question, the witness might misunderstand what is actually asked.

Generally, a witness should not volunteer or freely give information.

Also, when providing an answer during cross-examination, it might be difficult to avoid getting trapped in various assumptions, what-if scenarios, and generalities presented by counsel. Opposing counsel might also pose overly complex questions in an attempt to convolute the witness's responses. If this occurs, or if asked a long or imprecise question, the witness should retrench by asking for a question to be rephrased in smaller components.

It is critical to never underestimate the expertise of the opposing counsel. Often, opposing counsel will be underplaying its understanding of the issues to lull the witness into a sense of security. This can lead the witness into a difficult situation. Opposing counsel's golden rule is to cross-examine only if it would benefit the case. So, opposing counsel usually knows the answers to the questions it poses.

In asking questions of the witness, opposing counsel generally either will ask short questions in plain words or will ask leading questions. A common tactic is to make a question seem like a yes or no question, even though it might require an explanation. It is important for the witness to answer succinctly when possible to avoid appearing argumentative.

The opposing counsel generally will evaluate answers and then take a specific approach that furthers the argument. Generally, the witness will not be allowed to explain or elaborate on the question, as that would allow the witness to alter the thrust of a carefully orchestrated cross-examination. Opposing counsel will continually question or evaluate how the last question and answer could be used against the witness.

Furthermore, opposing counsel often will prepare for cross-examination by researching the witness. For example, it is likely that counsel will read all of the witness's earlier testimony and publications. Opposing counsel also might speak to other lawyers as to the witness's

capabilities in court if the lawyers have had experience with the witness. If weaknesses are discovered, the questioning probably will be directed toward those weaknesses.

Opposing counsel also might attempt to take psychological control of a witness by:

- Using physical presence to intimidate
- Making nonstop eye contact
- Challenging the witness's space
- Asking questions at a fast pace to confuse the witness
- Not allowing the witness to explain or deviate from the exact question

Physical domination often is used by opposing counsel. Opposing counsel will quickly discover the response pattern of the witness and might take an aggressive stance to lead the witness to the point where he is unsure.

It is not the witness's job to argue with or challenge the person conducting questioning. The witness should simply try to get through the cross-examination in the most professional way possible. If the questioning party uses blatantly unfair practices, the judge or jury will take note, and such practices might hurt the opposing side's case. In no circumstances should the witness argue. In adversarial proceedings, the counsel who called the witness is tasked with objecting to improper questioning, so the witness should continue answering questions until an objection is made, and then follow the court's directions. In inquisitorial proceedings, the judge should intervene if questioning is improper.

Inquisitorial Cross-Examination

Cross-examination is unusual in inquisitorial systems. Given that most lay and expert witnesses in inquisitorial jurisdictions are called by the judge, the closest thing to cross-examination in inquisitorial systems occurs when the parties object to or examine the witness. In some jurisdictions, the parties typically do not ask questions directly, but may submit suggestions for inquiries to the judge. If parties are allowed to directly question witnesses, the questioning is usually less aggressive than in adversarial systems. Even so, the witness should be just as cautious in inquisitorial systems to preserve his credibility.

There are several considerations for experts in inquisitorial systems. Since the primary expert or experts are obtained by the court itself, they are generally seen as inherently less biased than experts in adversarial proceedings. Additionally, the selection of the expert is an extension of the court's authority and discretion. Therefore, for a party's legal counsel

to attack the expert's credibility in an adversarial way would be strategically unwise in most circumstances.

However, parties usually are allowed to raise objections to an expert if they believe the expert is biased. For example, the expert might have a relationship with one of the parties to the litigation. The parties are often allowed to question the expert's analysis or methods used. While this process is less confrontational, a poor performance can lead to the court rejecting the expert's testimony.

Additionally, fraud examiners might be asked to serve as experts for the parties to litigation. In this case, the judge or the court-appointed expert may question a party's expert. Party experts will have a perception of potential bias, so the questioning might involve similar tactics as those that occur in adversarial cross-examination.

Strategies to Discredit Witnesses

The questioning party might employ the following strategic methods to discredit a witness or to diminish the importance of a witness's testimony. These methods could be used alone or in conjunction with one another and are not an all-encompassing list. A party with adverse interests in cross-examination will quickly discover the witness's weak areas and employ any possible techniques to achieve its goal.

Note that some of these strategies are unavailable to opposing counsel or other questioning parties due to restrictions on the scope of questioning (this is especially true in inquisitorial jurisdictions).

Also, in some inquisitorial jurisdictions, lawyers cannot impeach a witness whom they know to be telling the truth because such impeachment arguably interferes with the court's pursuit of truth.

Myopic Vision

Myopic vision, a tactic primarily used against expert witnesses, entails getting the expert witness to admit to excessive time being spent on a specific matter, and then selecting an area to highlight in which the witness is unsure or has not done much work. This area might not be central to the issues in the case or to the conclusions reached. Then, the questioning party will make a large issue of it and prove that the witness's vision is myopic in that the work was limited in extent or scope, and, as such, substandard. At the same time, the questioning

party might reference the expert's fees to show that the party retaining the expert spent large sums to have this "obviously incomplete" work done.

Safety

The questioning party might seek to lull the witness into a feeling of false security by not attacking him at first, but then—after the witness feels safe—finding a small hole in the testimony that can be enlarged quickly. This approach is often characterized by being friendly and conciliatory, by which the fact finder is made sympathetic to the questioning party's cause. The questioning party also might attempt to achieve a certain amount of association with the witness that will make the witness want to help the questioning party to bring out information. Doing so may result in the witness giving information that otherwise would not have been given. With this additional information, it might be possible to find a chink or hole in the evidence and open it further.

Contradiction

In this type of attack, the questioning party seeks to impeach the witness by showing that the witness's testimony is contradictory or inconsistent. The questioning party might use leading questions to force the witness into a hard or contradictory position. Alternately, the questioning party can show that an expert's testimony contradicts documents or quotes from other articles written by experts in the field. If these documents or articles are in contradiction to the expert witness, then an admission can be obtained from the expert as to that contradiction. If a contradiction exists, the expert might be drawn into an argument as to who is the most appropriate or experienced person. A questioning party can also show that an expert witness has contradicted himself or his own article, and often, such attacks occur because the expert does not have a strong memory of the matter, or because of confusion resulting from the attack.

New Information

The questioning party may introduce new information of which the witness might not be aware. This normally is done to confuse the witness in the hope that the witness might contradict himself or show that an expert witness's existing testimony, assessment, report, or opinions are no longer valuable.

Support Opposing Side's Theory

This method is used against expert witnesses. In this approach, the questioning party recognizes an expert witness's qualifications and evidence, but he provides a different theory

that relies on an alternative interpretation of the facts and tries to get the expert to agree with the alternate theory. By obtaining the expert's agreement, the questioning party, in effect, makes the expert a witness for the other side. This technique is useful to obtain concessions from the witness that would damage his conclusions and, ultimately, his credibility.

Bias

The questioning party may seek to show that the witness is biased. *Bias* refers to partiality that prevents a witness from objectively considering an issue or situation. Often, this method draws the retaining party and the witness together to show possible collusion as to the evidence being presented, and hence, to demonstrate bias. Collusion and bias can be shown if the questioning party can determine that the retaining party had instructed the witness as to what to say or by limiting the witness's scope and thus his conclusions.

Attempts to show bias also can focus on the question of whether or not the witness was told by his client what to do and look for. With this approach, opposing counsel might attempt to show that the witness overlooked important documentation in an effort to assist his client.

Confrontation

The questioning party may seek to use confrontation to put the witness into a situation where he loses emotional control and shows anger. If a witness explodes when confronted by the questioning party, the witness's credibility normally disappears.

Sounding Board

The questioning party may seek to use the witness as a sounding board to reacquaint the judge or jury with the favorable aspects of the questioning party's theory. This technique often uses the "Is it not true?" and "Would you agree with me?" approach. Often, the questions cover basic premises of the case that both parties agree to. Constant, nonstop agreement is used to intimidate the witness. If the witness agrees with various questions raised by the questioning party, the judge or jury might interpret the agreement to mean that the witness generally concurs with the questioning party's position.

Witnesses should be cautious not to be lulled into agreeing with what the questioning party says after a barrage of "easy" questions. The questioning party might eventually try to trick the witness into agreeing with something that contradicts former testimony. At the same time, the witness should not resist agreeing with accurate assessments because doing so

makes him look combative and biased. It is important for witnesses to provide a thoughtful response to each question.

Willing to Say Anything for a Price

Under this method, which is used against expert witnesses, the questioning party portrays the witness as an individual who is willing to shape his opinion in favor of the side that paid him. The attack might indicate a lack of complete work and be correlated to the fee charged. This method often is related to *bias* and *myopic vision*. The questioning party might suggest that the witness, his report, or his opinion are, in fact, biased. This technique often builds to a conclusion in which the questioning party arrives at the idea that the expert's work was superficial and unprofessional, yet the expert received a great deal of money for this and other services provided to the client. These techniques seek to suggest that the testimony was purchased or that the witness was paid to overlook facts contradictory to the conclusions reached.

Terms of Engagement

This method is used against expert witnesses, and in this approach, the questioning party attacks the terms used to engage the witness. This technique normally is employed by obtaining the original engagement letter and examining the terms of engagement. With such information, questioning party can show that the expert witness intended to look only at various items in support of his client and glossed over alternative theories, generally to the detriment of the opposition. As such, the witness could be portrayed as partial.

Discrediting the Witness

The questioning party may seek to discredit the witness by proving that he is unworthy to be a credible witness to the court. This can often be accomplished by showing that the witness is currently or has previously been grossly biased, prejudiced, or corrupt; been convicted of criminal activities; been shown to engage in immoral activities; made inconsistent statements; acquired a reputation for a lack of veracity; or exaggerated his qualifications.

Discrediting also could consist of looking at the quality of the witness's educational background to reveal any other unusual activities that might bias the witness or exclude him from the court as an expert.

Personal Attacks

The questioning party may also make personal attacks against the witness to damage his credibility. The following are common areas of attack:

- The witness is unqualified.
- The witness displayed unprofessional behavior during the examination (e.g., asking personal or inappropriate questions during interviews).
- The witness had a conflict of interest.
- The witness was harassing (phone calls at home, threatening voice mails, etc.).

Failure to Follow the Standards of the Profession

Additionally, the questioning party may attempt to discredit expert witnesses by trying to show that they failed to follow the standards, best practices, or professional conduct rules set forth by their profession, such as the ACFE for fraud examiners or other professional bodies for accountants, attorneys, etc.

For fraud examiners, it is extremely important to be familiar with the tools and techniques set forth in the *Fraud Examiners Manual*. There have been cases where enterprising defense attorneys have obtained copies of the *Manual* and quizzed the fraud examiner about whether or not the methods set forth in the *Manual* were followed. Likewise, attorneys will often question fraud examiners about the ACFE Code of Professional Ethics, particularly regarding the prohibition against stating an opinion of guilt or innocence (which is discussed below).

It is important to understand that the *Fraud Examiners Manual* does not set forth standards. The *Manual* provides the fraud examiner with information, suggestions, and methods for conducting a fraud examination. An ACFE member is always required to follow the ACFE Code of Professional Ethics, but he is not required to follow what is set forth in the *Fraud Examiners Manual*.

However, if a fraud examiner deviates from the normal investigative methods set forth in the *Manual*, he should have an explanation as to why it was appropriate and explain that the *Manual* is only provided as guidance.

Expressing an Opinion on Guilt

As previously discussed, testifying expert witnesses give opinion testimony, which is based upon their specialized knowledge and experience about case issues, but experts may only give opinion testimony in areas that will aid the fact finders in reaching their verdict. Additionally, in some jurisdictions, experts may give opinion testimony on ultimate issues (i.e., the basic conclusions upon which the outcome of a case depends), but they cannot offer legal conclusions or educate the jury on the principles of law. However, there are some jurisdictions that do not allow expert opinions at all, and in such jurisdictions, experts are restricted to providing technical information.

Moreover, article five of the ACFE Code of Professional Ethics prohibits opinions regarding the guilt or innocence of any person or party. Determining whether a person is guilty or innocent of a crime is not a decision for fraud examiners; it is a decision that is reserved for a judge or jury. Article five states:

> *An ACFE member, in conducting examinations, will obtain evidence or other documentation to establish a reasonable basis for any opinion rendered. No opinion shall be expressed regarding the guilt or innocence of any person or party.*

This rule is a rule of prudence. Clearly, it is prudent for a fraud examiner to refrain from usurping the role of the judge or jury. In a courtroom, no good attorney would ask a fraud examiner for such a conclusion, and no alert judge would allow such testimony.

The fraud examiner's job is to present the evidence in his report. Such evidence might constitute a convincing case pointing to the guilt or innocence of a person. However, a clear line should be drawn between a report that essentially says "Here is the evidence," and one that steps over the line and says "He is the guilty (innocent) person." Nevertheless, there is a fine line between recommending action—forwarding the evidence to a law enforcement agency or filing a complaint or lawsuit—and giving an opinion on guilt or innocence. Fraud examiners might make such recommendations because they think the evidence is strong enough to support a case. They might even have a conclusion about whether the suspect committed a crime. The rule does not prohibit the fraud examiner, under the proper circumstances, from accusing the person under investigation. However, the ultimate decision of whether a person is "guilty" or "innocent" is for a judge or jury to determine. The fraud examiner is free to report the facts and the conclusions that can be drawn from those facts,

but the decision as to whether or not a person is guilty of a crime is a decision for the judge or jury.

Summary

In his book *Succeeding As an Expert Witness*, Harold A. Feder suggests that experts do the following while working on a particular case:

- Keep an open mind.
- Do not approach a case with predetermined conclusions as to causation, culpability, fault, or damage.
- Remember that attorneys and clients might present slanted facts, either accidentally or purposefully.
- Carefully follow one's own well-established investigative steps; develop forms, procedures, and processes that will ensure evidence is not overlooked.

One of the best things experts can do is to stay current about new developments in their field. It takes a concerted effort to stay on top of changes and advances in any industry, as well as the latest forensic investigation methods. To be a successful expert witness in any area of accounting, for instance, one must have a thorough knowledge of not only generally accepted accounting principles, but also current promulgation. For cases involving credit card fraud, one must have a basic understanding of his nation's electronic banking system. While active practice in one's field of expertise—in other words, experience—remains his single most valuable source of knowledge, other sources abound.

Actions that maintain and improve one's current credentials and make him a better expert witness, include:

- Pursuing continuing education and training opportunities
- Reading trade journals and publications
- Joining and participating in professional societies and associations
- Teaching, lecturing, and holding seminars
- Attending specialized seminars and workshops
- Writing for trade journals and publications
- Taking advanced computer courses

Experts can practice their oral delivery skills, and hence improve their credibility, by actively pursuing public speaking engagements and opportunities.

Similarly, to feel more comfortable on the legal stage, an expert witness might wish to visit his local courtroom to observe another financial expert giving testimony in similar cases.

INVESTIGATION

TABLE OF CONTENTS

PLANNING AND CONDUCTING A FRAUD EXAMINATION

MENU

PLANNING AND CONDUCTING A FRAUD EXAMINATION (CONT.)

ANALYZING DOCUMENTS

ANALYZING DOCUMENTS (CONT.)

INTERVIEW THEORY AND APPLICATION (CONT.)

MENU

INTERVIEW THEORY AND APPLICATION (CONT.)

INTERVIEW THEORY AND APPLICATION (CONT.)

INTERVIEWING SUSPECTS AND SIGNED STATEMENTS

MENU

INTERVIEWING SUSPECTS AND SIGNED STATEMENTS (CONT.)

COVERT EXAMINATIONS

MENU

SOURCES OF INFORMATION (CONT.)

MENU

SOURCES OF INFORMATION (CONT.)

DATA ANALYSIS AND REPORTING TOOLS

MENU

DATA ANALYSIS AND REPORTING TOOLS (CONT.)

DATA ANALYSIS AND REPORTING TOOLS (CONT.)

DIGITAL FORENSICS

MENU

DIGITAL FORENSICS (CONT.)

TRACING ILLICIT TRANSACTIONS

TRACING ILLICIT TRANSACTIONS (CONT.)

MENU

TRACING ILLICIT TRANSACTIONS (CONT.)

REPORT WRITING

MENU

REPORT WRITING (CONT.)

MENU

APPENDIX B: FRAUD EXAMINATION CHECKLIST

APPENDIX C: SAMPLE FORMS

APPENDIX D: ADDITIONAL INFORMATION SOURCES

PLANNING AND CONDUCTING A FRAUD EXAMINATION

Why Conduct a Fraud Examination?

There are many reasons why organizations choose to conduct fraud examinations. In particular, a properly executed fraud examination can address a number of organizational objectives, including:

- Identifying improper conduct
- Identifying the persons responsible for improper conduct
- Stopping fraud
- Sending a message throughout the organization that fraud will not be tolerated
- Determining the extent of potential liabilities or losses that might exist
- Helping to facilitate the recovery of losses
- Stopping future losses
- Mitigating other potential consequences
- Strengthening internal control weaknesses

In addition, in some instances, a fraud examination might be required by law. A duty to investigate can arise from statutes, regulations, contracts, or common law duties. For example, a corporation's directors and officers owe a common law duty of care to their organization and shareholders, and therefore, when suspicions of fraud arise, it might be necessary for them to conduct an investigation to ensure that they have full knowledge of such issues affecting the company. Likewise, some laws hold employers accountable for investigating employee complaints involving certain matters, such as retaliation, discrimination, harassment, and similar issues.

Tips

Fraud can be discovered in several ways, such as via a tip or complaint, an auditing procedure, monitoring, or chance. However, according to the ACFE 2014 *Report to the Nations,* more than 40 percent of all internal investigations originate with a tip from an employee, customer, or vendor. Management review and internal audit are each the impetus for about 15 percent of internal investigations, while the remainder are discovered through other means.

As tips are the most valuable resource for discovering internal fraud, companies should proactively seek them out by implementing easily accessible and anonymous (where

permitted by law) fraud reporting tools, such as a tip hotline or dedicated Web page. Additionally, these reporting programs should be designed to accept external tips from sources such as customers and vendors.

Not all tips are valid, and while it is important to consider the motives of individuals willing to supply information of this kind, all tips must be approached from the outset as if they will yield useful information. In many instances, the tipster provides information that is of value in commencing an internal fraud case. In such cases, the tipster observes or becomes aware of activity that is suspicious and feels a sense of obligation to report it.

What Fraud Examination Entails

The term *fraud examination* refers to a process of resolving allegations of fraud from inception to disposition, and it is the primary function of the anti-fraud professional. The fraud examination process encompasses a variety of tasks that might include:

- Obtaining evidence
- Reporting
- Testifying to findings
- Assisting in fraud detection and prevention

Obtaining Evidence

The value of a fraud examination rests on the credibility of the evidence obtained. Evidence of fraud usually takes the form of documents or statements by witnesses; therefore, fraud examiners must know how to properly and legally obtain documentary evidence and witness statements.

Reporting

Once evidence has been obtained and analyzed, and findings have been drawn from it, the fraud examiner must report the results to the designated individuals (e.g., management, the board, or the audit committee). A fraud examination report is a narration of the fraud examiner's specific activities, findings, and, if appropriate, recommendations.

Such communications are necessary so that those responsible can determine the appropriate course of action.

The results of an examination can be communicated in various ways. The appropriate method of communication will depend on the facts at issue, but most reports are communicated orally or in writing.

When communicating the results of a fraud examination, the fraud examiner is responsible for providing clear, accurate, and unbiased reports reflecting the fraud examination results. This need arises from the possibility that such results might end up being read or used by various groups of people, such as organization insiders, attorneys, defendants, plaintiffs, witnesses, juries, judges, the media, and so on.

Testifying to Findings

Often, fraud examiners are called upon to provide testimony and report their findings at a deposition, trial, or other legal proceeding. When providing testimony, fraud examiners must be truthful. They should also communicate in a clear and succinct manner.

Assisting in Fraud Detection and Prevention

Fraud examiners are not responsible for the prevention of fraud; such responsibilities belong to management or other appropriate authority. Nevertheless, fraud examiners are expected to actively pursue and recommend appropriate policies and procedures to prevent fraud.

Because of their education, experience, and training, Certified Fraud Examiners are uniquely qualified to assist organizations in the prevention and detection of fraud.

Fraud Examination and Forensic Accounting

Although fraud examination shares certain characteristics with forensic accounting, they are not the same discipline.

Forensic accounting is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation. The word *forensic* is defined by *Black's Law Dictionary* as "used in or suitable to courts of law or public debate." Therefore, *forensic accounting* is actually litigation support involving accounting.

Accordingly, most fraud examinations involve forensic accounting, but not all forensic accounting is fraud examination. For example, an individual hired to value the property in a

minority shareholder derivative suit would engage in forensic accounting even if the engagement does not involve fraud.

While fraud examinations can be conducted by either accountants or nonaccountants, forensic accounting work can only be performed by accountants. In addition, while forensic accounting is litigation support work that involves accounting, fraud examinations only involve anti-fraud matters.

Most fraud examinations will generally fall under the category of forensic accounting because the majority of fraud examinations, investigations, and reports regarding fraud are done with "an eye toward litigation." This is because fraud examiners are taught to conduct fraud examinations with the assumption that they will end in litigation.

Forensic accounting can include many professional services. Typically, forensic accountants perform assignments involving:

- Computer forensics
- Electronic discovery
- Bankruptcies, insolvencies, and reorganizations
- Workplace fraud investigations
- Calculations of economic losses
- Business valuations
- Professional negligence

Fraud Examination Methodology

Fraud examination is a methodology of resolving signs or allegations of fraud from inception to disposition. The fraud examination methodology establishes a uniform, legal process for resolving signs or allegations of fraud on a timely basis. It provides that fraud examinations should move in a linear order, from the general to the specific, gradually focusing on the perpetrator through an analysis of evidence.

Fraud examinations involve efforts to resolve allegations or signs of fraud when the full facts are unknown or unclear; therefore, fraud examinations seek to obtain facts and evidence to help establish what happened, identify the responsible party, and provide recommendations where applicable.

When conducting a fraud examination to resolve signs or allegations of fraud, the fraud examiner should assume litigation will follow, act on predication, approach cases from two perspectives, move from the general to the specific, and use the fraud theory approach.

Assume Litigation Will Follow

Each fraud examination should begin with the proposition that the case will end in litigation. Thus, when a fraud examiner begins a fraud examination, he must assume that the case will end in litigation, and this assumption must be maintained and considered throughout the entire examination. If the fraud examiner assumes that litigation will occur, he will conduct the examination in accordance with the proper rules of evidence and remain well within the guidelines established by the legal systems.

Act on Predication

Fraud examinations must adhere to the law; therefore, fraud examiners should not conduct or continue fraud examinations without proper predication. *Predication* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe that a fraud has occurred, is occurring, and/or will occur. In other words, predication is the basis upon which an examination, and each step taken during the examination, is commenced.

A fraud examiner acts on predication when he has a sufficient basis and legitimate reason to take each step in an examination.

Accordingly, fraud examiners should begin a fraud examination only when there are circumstances that suggest fraud has occurred, is occurring, and/or will occur, and they should not investigate beyond the available predication. If a fraud examiner cannot articulate a factual basis or good reason for an investigative step, he should not do it. Therefore, a fraud examiner should reevaluate the predication as the fraud examination proceeds. That is, as a fraud examination progresses and new information emerges, the fraud examiner should continually reevaluate whether there is adequate predication to take each additional step in the examination.

If a fraud examiner acts without predication, he might expose both himself and his client or employer to liability.

The requirement for predication, however, does not bar fraud examiners from accepting other forms of engagements in circumstances where predication is lacking. For example, a fraud examiner can conduct a fraud risk assessment for consulting purposes even if there is no reason to believe a fraud has occurred, is occurring, and/or will occur.

Approach from Two Perspectives

Fraud examiners should approach investigations into fraud matters from two perspectives: (1) by seeking to prove that fraud has occurred and (2) by seeking to prove that fraud has not occurred. To prove that a fraud *has* occurred, the fraud examiner must seek to prove that fraud has *not* occurred. The reverse is also true. To prove fraud *has not occurred*, the fraud examiner must seek to prove that fraud has occurred. The reasoning behind this two-perspective approach is that both sides of fraud must be examined because *under the law, proof of fraud must preclude any explanation other than guilt*.

Move from the General to the Specific

Fraud examinations commence when the full facts are unknown or unclear; therefore, they should proceed from the general to the specific. That is, fraud examinations should begin with general information that is known, starting at the periphery, and then move to the more specific details.

To illustrate, consider the order of interviews in fraud examinations. In most examinations, fraud examiners should start interviewing at the periphery of all possible interview candidates and move toward the witnesses who appear more involved in the matters that are the subject of the examination. Thus, the usual order of interviews is as follows:

- Neutral third-party witnesses, starting with the least knowledgeable and moving to those who are more knowledgeable about the matters at issue
- Parties suspected of complicity, starting with the least culpable and moving to the most culpable
- The primary suspect(s) of the examination

Use the Fraud Theory Approach

When conducting fraud examinations, fraud examiners should adhere to the fraud theory approach. The fraud theory approach is an investigative tool designed to help fraud examiners organize and direct examinations based on the information available at the time.

The fraud theory approach provides that, when conducting investigations into allegations or signs of fraud, the fraud examiner should make a hypothesis (or theory) of what might have occurred based on the known facts. Once the fraud examiner has created a hypothesis, he should test it through the acquisition of new information (or correcting and integrating known information) to determine whether the hypothesis is provable. If, after testing a hypothesis, the fraud examiner determines that it is not provable, he should continually revise and test his theory based on the known facts until it is provable, he concludes that no fraud is present, or he finds that the fraud cannot be proven.

Simply put, the fraud theory approach involves the following steps:

- Analyzing available data
- Creating a hypothesis
- Testing the hypothesis
- Refining and amending the hypothesis

The following internal fraud case study illustrates the concepts involved in the fraud examination process. Although the case study is based on an actual incident, the names and certain other facts have been changed for purposes of illustration.

LINDA REED COLLINS CASE STUDY

Linda Reed Collins is purchasing manager for Bailey Books Incorporated in St. Augustine, Florida. Bailey, with $226 million in annual sales, is one of the country's leading producers of textbooks for the college and university market, as well as technical manuals for the medical and dental professions.

Bailey's headquarters consists of 126 employees, plus numerous sales personnel in the field. Because of the competitive nature of the textbook business, the company's profit margins are quite thin. Bailey's purchases average about $75 million annually, consisting mostly of paper stock and covering used in the manufacturing process. The great majority of the manufacturing is done in Mexico through contracts with the Mexican government.

The purchasing function is principally handled by three purchasing agents. Linda Reed Collins is the purchasing manager and has two other buyers who report to her, plus another 18 clerical and support personnel.

Because Bailey Books is required by investors and lenders to have audited annual financial statements, Bailey employs a large regional CPA firm to conduct its annual audit and has a staff of five internal auditors.

All internal fraud matters within Bailey are referred to Loren D. Bridges, a Certified Fraud Examiner. Often, internal fraud issues at Bailey involve defalcations by Bailey's cashiers, but Bridges also receives a constant stream of complaints alleging misconduct by Bailey Books' salespeople and distributors.

On January 28, Bridges received a telephone call in which the caller, who was male, wanted to keep his identity hidden. The caller, however, claimed to have been a "long-term" supplier of books, sundries, and magazines to Bailey. The caller said that ever since Linda Collins took over as purchasing manager for Bailey several years ago, he has been systematically forced out of doing business with Bailey. Although Bridges queried the caller for additional information, the caller hung up the telephone.

Under the facts in this case study, there could be many legitimate reasons why a supplier to Bailey would feel unfairly treated. Linda Reed Collins could be engaged in fraud, as the caller claimed, or the caller could be someone who has a personal vendetta against Collins and wants to get her fired. That is, Bridges does not have enough information to know if the caller was forced out of doing business with Bailey or why this might have been the case. Because Bridges does not have all of the facts, he should investigate the matter using the fraud theory approach.

Analyzing Available Data

Under the fraud theory approach, Bridges should begin by analyzing the available data so he can create a preliminary hypothesis as to what has occurred.

Also, if those responsible determined that an audit of the entire purchasing function is warranted, the audit would be conducted at the time this determination is made. When conducting the audit, the internal auditors should keep in mind that there is a possibility that fraud might exist.

Creating a Hypothesis

Once Bridges has analyzed the available data, he should create a preliminary hypothesis as to what has occurred. The hypothesis should be a "worst-case" scenario. That is, based on the

caller's statements, Bridges should determine the worst possible outcome. Under these facts, the worst possible outcome would be that one of Bailey's purchasing agents has been accepting kickbacks to steer business to a particular vendor.

Fraud examiners can create hypotheses for any specific allegation (e.g., a bribery or kickback scheme, embezzlement, conflict of interest, or financial statement fraud).

Testing the Hypothesis

Once Bridges has created a hypothesis, he should test it through the acquisition of new information or by correcting and integrating known information.

Testing a hypothesis involves creating a what-if scenario. For example, in the facts of the Linda Reed Collins case study, Bridges hypothesizes that, based on the anonymous tip, a vendor is bribing a purchasing agent. He would test this hypothesis by looking for some or all of the following facts:

- A vendor is receiving an unusually large amount of business
- Purchases of high-priced, low quality goods or services over an extended period
- A purchasing agent has a personal relationship with a vendor
- A purchasing agent with the ability to steer business toward a favored vendor
- A purchasing agent's lifestyle suggests unexplained wealth or outside income

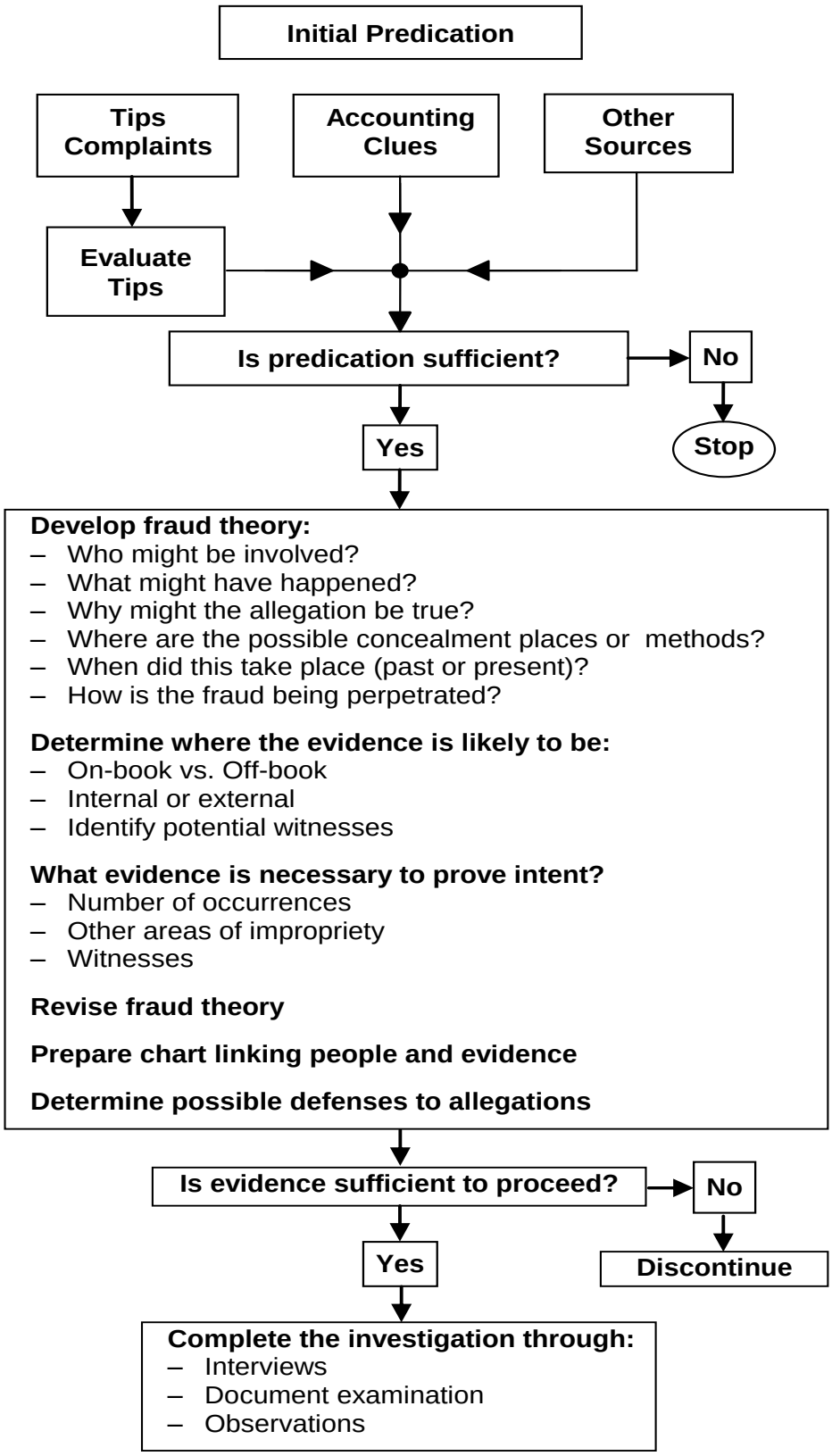
Bridges could readily look for facts indicating a bribery scheme. He could readily establish whether a vendor is receiving an unreasonably large proportion of Bailey Book's business when compared to similar vendors. Bridges could ascertain whether Bailey Books was paying too much for a particular product, such as paper, by simply calling other vendors and determining competitive pricing. Bridges could determine whether a vendor has a personal relationship with a purchasing agent by discreet observation or inquiry. Bridges could determine whether a particular purchasing agent had the ability to steer business toward a favored vendor by determining who is involved in the decision making process. Also, Bridges could learn about the agent's lifestyle by examining public documents such as real estate records and vehicle titles.

Refining and Amending the Hypothesis

If, after testing a hypothesis, the fraud examiner determines that it is not provable, the fraud examiner should continually revise and test it based on the known facts. For example, if Bridges tests his hypothesis that a vendor is bribing a purchasing agent of Bailey Books and

learns that the facts do not fit the presence of a bribery scheme, he should revise his hypothesis and retest it. (Obviously, if the fraud examiner tests his hypothesis and determines that the facts do not fit the presence of a bribery scheme, it could be that no fraud is present or that the fraud cannot be proven.)

The following flowchart sets forth how the fraud examination process is used to resolve signs or allegations of fraud.


Initial Predication
Tips Complaints
Accounting Clues
Other Sources
Evaluate Tips
Is predication sufficient?
No
Stop
Yes
Develop fraud theory:
– Who might be involved?
– What might have happened?
– Why might the allegation be true?
– Where are the possible concealment places or methods?
– When did this take place (past or present)?
– How is the fraud being perpetrated?
Determine where the evidence is likely to be:
– On-book vs. Off-book
– Internal or external
– Identify potential witnesses
What evidence is necessary to prove intent?
– Number of occurrences
– Other areas of impropriety
– Witnesses
Revise fraud theory
Prepare chart linking people and evidence
Determine possible defenses to allegations
Is evidence sufficient to proceed?
No
Discontinue
Yes
Complete the investigation through:
– Interviews
– Document examination
– Observations

Develop a Fraud Response Plan

When evidence of misconduct arises, management must respond in an appropriate and timely manner. During the initial response, time is critical. To help ensure that an organization responds to suspicious fraud-related activity efficiently, management should have a response plan in place that outlines how to respond to such issues.

A *fraud response plan* outlines the actions that members of an organization will take when suspicions of fraud have arisen. Because every fraud is different, the response plan should not outline how a fraud examination should be conducted. Instead, response plans should help organizations manage their responses and create environments to minimize risk and maximize the potential for success.

Additionally, a response plan will allow management to respond to suspected and detected incidents of fraud in a consistent and comprehensive manner. By having a response plan in place, management will send a message that it takes fraud seriously.

More specifically, the fraud response plan should guide the necessary action when potential fraud is reported or identified.

Also, a response plan should not be unduly complicated; for a response plan to work in high-pressure and time-sensitive situations, it must be simple to understand and administer.

While the appropriate response will vary based on the event, management should include a range of scenarios in the response plan.

Organizations without a fraud response plan might not be able to respond to issues properly, and will likely expend more resources and suffer greater harm than those that have such a plan in place. Conversely, having a response plan puts an organization in the best position to respond promptly and effectively.

This section explores the elements of a fraud response plan, which include:

- Reporting protocols
- A response team responsible for conducting an initial assessment
- Factors used to decide on the course of action
- Litigation hold procedures

- Principles for documenting the response plan
- A template or form to report fraud incidents

Reporting Protocols

One of the first steps when developing a response plan is to establish reporting protocols for tips, matters, allegations, and other indicators of improper activity. Reporting protocols are necessary to ensure that designated individuals are notified immediately to enable a prompt response.

Reporting protocols should outline notification principles and escalation triggers that vary depending on the nature and severity of the allegations. That is, they should indicate how to communicate the incidents to the appropriate level of management. For example, a fraud response plan might instruct employees to report suspicions of fraud to their manager (if possible), a designated human resources (HR) or compliance officer, or the head of audit and enforcement.

Next, the issue should be reported to the party or parties responsible for conducting an initial assessment to determine how to respond and whether a full investigation is necessary.

Additionally, organizations should provide multiple channels for reporting concerns about fraud.

A Response Team

No single person can effectively address every fraud-related issue. Therefore, the fraud response plan must identify key individuals who might be required to respond to a particular fraud. The response team members will vary depending on the facts and the potential severity of the suspected fraud, but the team might include:

- Legal counsel
- A representative of management
- A Certified Fraud Examiner
- The finance director
- General counsel
- A representative of internal audit
- Audit committee members
- A C-level executive

- Information technology (IT) personnel
- A representative of human resources (HR)

Factors Used to Decide on the Course of Action

Again, the response team should determine the appropriate course of action when fraud is suspected. In general, if an allegation of fraud-related misconduct arises, management should conduct an investigation, but there are other courses of action it might decide to take. To help decide the best course of action, management should identify a list of factors it will use to make this decision. Identifying such factors will help the response team determine whether to escalate an incident into an investigation.

Each organization will have different criteria for deciding whether allegations/suspicions qualify for a formal investigation, but common ones include:

- Credibility of the allegation
- Type of incident
- The subject of the allegation
- The business purpose of the activity at issue
- Seriousness or severity of the allegation
- Potential negative impact
- Likelihood that the incident will end up in court
- The ways in which prior, similar incidents were handled

Litigation Hold Procedures

If an organization does not already have litigation hold procedures in place, management should institute them immediately. A *litigation hold* refers to the steps an organization takes to notify employees to suspend the destruction of potentially relevant records when the duty to preserve information arises.

Litigation hold procedures are necessary to ensure that potentially responsive documents are not destroyed once evidence of misconduct arises. The failure to preserve relevant evidence could have several adverse consequences, including, but not limited to, the government's questioning of the integrity of any fraud investigation, monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defenses.

To establish litigation hold procedures, management should:

- Identify the scope of litigation hold procedures (i.e., the locations that the litigation hold procedures will cover).
- Examine how information moves through the organization.
- Determine how to identify relevant documents.
- Develop a process to ensure such information is preserved.

Litigation hold procedures should apply to individual communications (e.g., email, chat messages, voice recordings), data on shared devices (e.g., network folders), system backup files, and archived data.

In general, litigation hold policies should be developed so the organization can:

- Promptly notify employees who might possess relevant documents.
- Issue a preliminary hold order to all individuals and employees who might possess relevant information.
- Promptly notify information technology (IT) personnel and get their involvement if electronic data is at issue.
- Notify employees and IT personnel of their duty to preserve.
- Suspend any deletion protocols.
- Prohibit the destruction, loss, or alteration of any potentially relevant documents.
- Prohibit employees from destroying, hiding, or manipulating documents.
- Alert employees as to the risk to the company and the employees if they fail to heed the litigation hold request.

Moreover, establishing litigation hold procedures will help those involved in an investigation identify the relevant sources of information quickly, and it will help them understand the technology options available for searching, analyzing, and reviewing data.

Even though litigation holds should apply to both electronic data and physical documents, electronic data contains certain attributes that make executing a timely litigation hold more difficult. Specifically, electronic data might only be available for a temporary period, business practices are often designed to free up storage space by deleting this type of information, electronic data can reside in numerous locations, and identifying relevant electronic data within today's large and complex data systems can be challenging and costly.

Moreover, if an organization operates internationally, it is more difficult to execute a timely hold. In such cases, management should consider retaining an outside expert to help with the data search and preservation.

A key objective of a litigation hold is to stop any automatic document deletion programs or rules that might be in place.

Principles for Documenting the Response Plan

Management should establish principles for documenting information during each phase of a fraud investigation. The principles should be designed to record all information relevant to or created during each phase of a fraud investigation, including the initial response, that is used to support decision making.

A Fraud Incident Report Log

Management should also develop a fraud incident report log of all suspicions of fraud, including those not investigated, to serve as a record of the organization's response efforts. Once a suspicion of fraud arises, the issue should be recorded and detailed in the log, and as the issue progresses, the log should be modified. Ultimately, it should contain details of actions taken and conclusions reached.

The report log should include information on the following items:

- How the organization became aware of the suspected fraud, including the name of any complaining party
- The date the issue was raised or reported
- The nature of the suspected fraud
- Department or divisions involved
- Suspect employees or parties
- Actions taken

Initial Response to Suspicions or Allegations of Fraud

When responding to suspected and detected incidents of fraud, time is critical. Management and fraud examiners must be prepared to address a number of issues in a short amount of time, sometimes under stressful conditions.

This section explores the first steps that management and fraud examiners should take when a fraud-related incident becomes known, and it provides a list of tips for managing and organizing the process of responding to suspected and detected incidents of fraud.

Initially, when a suspicion or allegation of fraud arises, management must respond quickly. The failure to act quickly against suspicions of fraud could result in litigation, enhanced penalties, and enforcement actions by government regulators.

The appropriate response varies depending on the facts, such as the underlying evidence, who is implicated, how the evidence came about (e.g., internal sources, civil lawsuit, investigation by the government), and so on. But generally, when evidence of fraud arises, management should respond by engaging in the following actions:

- Activate the response team.
- Engage legal counsel, if necessary.
- Consider contacting the insurance providers.
- Address immediate concerns.
- Conduct an initial assessment.
- Document the initial response.

Activate the Response Team

When evidence of fraud arises, management must activate the fraud response team—the group of people tasked with responding to incidents of fraud. When activated, the response team should seek to answer the following questions:

- Is a formal investigation necessary?
- If a formal investigation is necessary, who will lead it?
- Is there a need for immediate police involvement?
- Is there an immediate need for legal assistance or advice?
- Is there a need for external support (e.g., forensics specialists)?
- Is there a need for additional support (e.g., access to IT facilities or a secure room, support from administration)?
- Is there a need to devise a media strategy to deal with the issue?
- Is there a need to report the issue to an external third party?
- Should the audit committee be informed?

Engage Legal Counsel

Because incidences of fraud are riddled with legal uncertainties, management should consult with internal and possibly external local legal counsel before making any decisions or taking any action concerning the suspected conduct. Typically, the general counsel should be made aware of any significant fraud that might result in legal action.

Consider Contacting the Insurance Provider

When evidence of fraud arises, it is generally impossible to know whether the incident will result in an insurance claim, but even so, many insurance policies require timely notice of potential claims. Therefore, an organization should consider putting its insurer on notice to preserve a potential insurance claim.

Address Immediate Concerns

Also, when evidence of fraud arises, management and the response team should address immediate concerns. Immediate concerns will vary, but they might include:

- Preserving relevant documents
- Identifying who should be informed

Preserving Relevant Documents

When evidence of fraud arises, management should seek to preserve all relevant documents, especially those that an employee might want to hide or destroy. In a fraud investigation context, the term *documents* typically refers to, but is not limited to, contracts, invoices, correspondence, memoranda, weekly reports, presentations, telephone messages, emails, reports, performance reviews, performance improvement plans, medical records, and other written or recorded material.

When evidence is misplaced, lost, or destroyed, it becomes more difficult to conduct an investigation. Thus, the response team and management must take action to preserve evidence as soon as the decision to investigate is made. There are a number of steps that management should take to preserve relevant documents. For one thing, management should work with legal counsel to issue a litigation hold to notify employees to suspend the destruction of potentially relevant records.

Furthermore, management should suspend the organization's record retention policy temporarily to avoid a piece of evidence accidentally being destroyed.

Also, management could lockdown access to emails or digital files that employees might want to conceal or destroy. Digital information can be found in virtually any type of media, and it is more fragile than tangible evidence. Therefore, employees can destroy this type of information if it is not protected properly. Often, when fraudsters become aware of an investigation, they try to destroy evidence in their computers or sabotage other evidence that could be used against them. Accordingly, it is a good idea to have IT personnel involved in this process each time the organization decides to conduct an investigation.

The failure to preserve documents could have several adverse consequences. First, the failure to preserve documents could cast doubt on the integrity of any fraud investigation. Second, documents destroyed when litigation is expected, or in progress, might result in obstruction charges or allegations of spoliation, which, if proven, could lead to the imposition of sanctions. *Spoliation* is broadly defined as the intentional or negligent destruction or alteration of documents relevant to litigation.

In today's digital environment, digital spoliation is a major concern for organizations involved in litigation. When compared to the spoliation of tangible documents, digital spoliation carries additional risks. Management often lacks sufficient knowledge of the inventory of digital information, and electronic data might only be available for an evanescent time. Additional concerns include business practices designed to free up storage space by deleting digital information and the fact that electronic data can reside in numerous locations, as well as the fact that identifying relevant electronic data within today's large and complex data systems can be challenging and costly.

Identifying Who Should Be Informed

Management and the response team should identify whom to inform. Depending on the facts, several departments should be interested in fraud, including legal, human resources, internal audit, security, risk management, and loss prevention. When responding to an allegation of fraud, it is important to consider the interests of each of these departments. This is necessary to ensure that designated employees are notified immediately to enable a prompt response. Information about incidences, however, should be shared only on a need-to-know basis.

Human resources (HR) personnel address issues involving unfair treatment, discrimination, harassment, substance abuse, or concerns about corporate policies. Therefore, the HR department should be informed of fraud that affects any such areas.

Both the HR and legal departments should be involved to ensure that the right people receive information in a timely manner. Also, other departments, such as loss prevention and risk management, audit, and security might need to be involved. Although the development of information distribution rules requires the participation of several departments, it is best to have these rules set before investigation protocols are in place.

Another department that needs to be involved is the information technology (IT) department. The IT department might need to be part of an investigation to safeguard data until it can be analyzed. IT personnel can also help identify what data are available and where, and they might be able to function as forensic investigators if licensed to do so.

Again, management must restrict access to certain pieces of information on a need-to-know basis.

Conduct an Initial Assessment to Determine the Appropriate Response

Usually, when an allegation of fraud arises, there are not enough known and verified facts to begin a formal investigation; therefore, management and the response team should conduct an initial assessment to determine if an investigation is needed and what steps, if any, are required to respond in an appropriate manner. This is perhaps the most critical question that management must answer when an allegation of fraud arises.

An initial assessment should be quick and, unless complications arise, completed within a few days. Ideally, action should be taken within three days of learning about an incident.

The initial assessment should be a limited fact-finding analysis focused on the specific allegation or incident. It does not require an investigation plan or report, unlike a formal investigation. Thus, the initial assessment should seek to:

- Determine if fraud occurred.
- Identify the status of the fraud (e.g., When did it begin? Was it internal or external? Is it still occurring? If it is no longer occurring, when did it stop?).
- Identify potential claims and offenses.

To conduct an initial assessment and determine the appropriate response, those responsible should take the following steps:

- Understand the context.

- Review any applicable policies and procedures.
- Investigate the allegations.
- Document the reasons for the decision.

Understand the Context

Next, those responsible should gain an understanding of all of the circumstances leading up to the current situation. Often, the context is necessary to determine the best approach to dealing with a tip or suspicion, and it can provide clues that are helpful in other areas. Efforts to understand the context should seek to obtain the initial facts and circumstances about:

- The manner in which the suspicions became known
- The date suspicions became known
- The areas to which the suspicions pertain
- The source of the information
- The allegations at issue

Review Any Applicable Policies and Procedures

Those involved in the initial assessment must also review any applicable internal controls and organizational policies, including any anti-fraud auditing and testing policies and procedures, to determine the best method and processes for continuing the investigation.

Investigate the Allegations

An initial assessment should be a limited, fact-finding analysis, and it should focus on investigating the specific allegation or incident. More specifically, to determine the appropriate response, the assessment should, if possible, seek to answer a number of questions, including:

- Is the allegation credible?
- Who is the subject of the allegation, and what is his relationship to the company?
- When did the alleged misconduct occur, and how often did it occur?
- What was the business purpose of the activity related to the allegation?
- How serious is the allegation?
- What levels of employees are alleged to be involved, if any, in the misconduct (i.e., officers, directors, or managers)?
- What individuals might have pertinent information about the matter that would tend to support or refute the complainant's position, and what facts do these individuals purportedly know?

- Did any third parties receive any direct or indirect benefit from the misconduct, and if so, who are they?
- If a third party is involved, is the third party a government official?
- How was the matter recorded on the company's books and records, if applicable?
- Can it be determined if the person in question acted with fraudulent intent?
- Is it possible that the issue might be larger than expected?
- Were there any whistleblowers, and if so, how should they be dealt with?
- What measures should the company take to document how the initial evidence of wrongdoing was handled?
- Is the government already involved, and if not, is it likely that the government will become involved?
- Is it likely that the matter will have significant negative impact on shareholder value?

These questions are important because the response should be proportional to the potential scale of the fraud in terms of its value, frequency, potential damage, the individuals involved, the number of people involved, and so on.

In addition, the decision as to the appropriate response might be influenced by other factors. As with any business decision, the cost of conducting the investigation must be considered, and management might also consider whether an investigation will interrupt business activity.

Generally, the investigation portion of the initial assessment will involve:

- Contacting the source, if the investigation was triggered by a report or complaint
- Interviewing key individuals
- Reviewing key evidence

CONTACTING THE SOURCE

If the evidence came in through a tip from an identified source, those responsible should contact the source to find out additional information and confirm the source's willingness to help throughout the investigation. When contacting the source, the interviewer should encourage the complainant to provide a narrative description of the report. After the source provides the narrative, the interviewer should ask clarifying questions and then summarize the key points.

An interview with the source should seek to determine:

- What does the individual know?
- How did the individual get the information?
- Who were the key individuals involved?
- When did the alleged events occur (e.g., dates, times, and locations)?
- What are the details (e.g., who, what, when, where, why, and how much) of the allegations?
- What are the dates (or period) of the key events?
- What evidence exists to corroborate the alleged events, where is the evidence located, and how can the evidence be accessed?
- What witnesses can corroborate the alleged events?
- Which individuals might have pertinent information about the matter that would tend to support or refute the complainant's position, and what facts do these individuals purportedly know?
- What was the motivation behind the alleged events?
- Why were the alleged actions improper?
- If the scheme is ongoing, do the subjects know of the complainant's report?
- What is the complainant's motivation for making the report (e.g., What prompted you to report this?)?

When interviewing the source, the interviewer should seek to determine if there is any reason to suspect the complainant's credibility. Also, if there are any weaknesses in the complainant's information, the interviewer should ask the complainant to explain what he expects the subject would say in defense of the allegations and ask the complainant to explain why such a response is not sufficient to dispose of the matter. Additionally, the interviewer should ask the source what he wants the organization to do about the complaint. The response to such an inquiry will help the team focus its efforts.

INTERVIEWING KEY INDIVIDUALS

Those responsible should interview key individuals for information about the suspicious conduct and the subject(s). Interviewing individuals with personal knowledge is critical.

Also, they should interview witnesses as early as possible because it will limit the harm arising from loss of memory, witnesses becoming unavailable, and inadvertent loss or destruction of key evidence.

REVIEWING THE EVIDENCE

Those responsible should review relevant documents and files, which might include personnel files, the organization's employee handbook, accounting records, vendor activity reports, budget reports, fixed asset records, expense reimbursements records, leasing documents, rental agreements, payroll records, purchasing requisitions, purchase contracts, inventory records, shipping/receiving reports, emails, telephone records, and so on.

Obtaining and reviewing these documents will assist in understanding the chronology of events and might put the responsible parties on notice as to certain strengths or weaknesses of the investigation.

Document the Reasons for the Decision

To avoid any real or perceived downplay of the matter's significance and to avoid any attempts at willful blindness, those responsible should document their actions and findings. In addition, management must document its decisions and the reasons behind them. Thus, if management decides against conducting an investigation, it must document the reasons why.

Again, management should document the organization's initial response in an incident report log that serves as a record of the organization's response efforts. Once a suspicion of fraud arises, the issue should be recorded and detailed in the log. As the issue progresses, the log should be modified and, ultimately, it should contain details of actions taken and conclusions reached.

The incident report log should contain all information relevant to or created during the initial response that is used to support management's decision making.

Planning and Conducting a Formal Investigation

Once it is determined that an allegation or issue will be investigated, those responsible must begin the formal investigation. Typically, the steps involved in this process include:

- Completing engagement letters/contracts
- Issuing advisory letters
- Assembling the fraud team
- Learning about the organization at issue
- Developing an investigation plan

Completing Engagement Letters/Contracts

Certified Fraud Examiners are sometimes hired for specific engagements, and in such cases, it might be preferable to document the engagement in a formal written contract or a client engagement letter. (In some circumstances, an oral understanding might be sufficient.)

Engagement contracts or retainer agreements are beneficial for various reasons. For one thing, they will maximize a fraud examiner's protection in the event of a client dispute or misunderstanding, making later disputes about the engagement's terms easier to resolve. For another thing, engagement contracts or retainer agreements will help manage client expectations by making the assignment's objectives clear. It is important to note, however, that although formal, written agreements might be preferable, they are not always practical.

Engagement letters should be written with certain standards in mind, and they should address a variety of items. Those items include, but are not limited to, the client's identity, the scope of the services, the timing of the work, deliverables, payment terms and fee structure, communication with the client, non-guarantee, governing law, jurisdiction, termination, and limitation of liability through indemnity clause.

There are two primary forms of engagement letters: the long form and the short form. The *long form* spells out the details of what examination techniques the fraud examiner intends to follow, while the *short form* does not. Examples of each type of engagement letter can be found in Appendix A (located in the Investigation section of the *Fraud Examiners Manual).*

Although engagement letters contain various items, they contain the following basic parts:

- Opening
- Body (long or short)
- Terms
- Indemnity clause
- Close

Opening

The opening paragraph should state the purpose of the engagement. It should be specific as to whether the letter is an engagement or a proposal letter.

Body

The body of the letter will follow either the long form or the short form.

THE LONG-FORM ENGAGEMENT LETTER

The long-form engagement letter is similar to an engagement letter prepared for specific-scope examinations performed by auditors. In the body of the long form, the fraud examiner describes the procedures in detail and limits the scope of an examination to the procedures defined. This form is not recommended for engagements that require the investigation of fraud allegations and a concluding opinion on the existence of fraud.

At the onset, the fraud examiner might not know what procedures will be necessary to resolve the allegation, and in such circumstances, it will be difficult to describe the anticipated procedures with any precision.

THE SHORT-FORM ENGAGEMENT LETTER

The short-form engagement letter outlines the general scope of the engagement. For example, it might describe that the services will include an investigation of a fraud allegation received over the hotline, by an anonymous tip, or by an audit anomaly.

The short form might also confirm whether the fraud examiner has access to any personnel or documentation deemed necessary to carry out the assignment. This type of engagement letter is best used for work that will ultimately require an opinion on a fraud allegation. Because the fraud examiner will not know the nature of the alleged fraud at the onset, it is best to avoid limiting the examination's scope.

Terms

The terms paragraph of an engagement letter should include the payment terms, fee structure, and the method of payment. The terms should include a retainer, if needed, and it should indicate how many hours of examination time the client initially agreed upon. Additionally, this section should describe the billing procedures and a statement regarding payment methods.

Also, the terms should address out-of-pocket expenses. If travel is required, for example, the terms should discuss the anticipated cost of travel and the number of trips.

This section should include things such as:

- The fraud examiner(s) assigned to the case
- The fraud examiner's hourly rate, if he bills at a flat rate

- If there is a retainer, the terms section should include a statement regarding the exhaustion of the retainer, what expenses will be reimbursed if there are unused retainer proceeds, and when and how such reimbursements will be refunded
- A policy regarding past due invoices and late fees, including finance charges if applicable
- Rates for any additional services or expenses that might be needed

Indemnity Clause

In letters of engagement, there should be an indemnity clause to protect the fraud examiner if the subject, a witness, or a third party sues the client and includes the fraud examiner as a party to the suit. The clause should not be boilerplate; it should be tailored to fit the particular terms of the engagement.

The indemnity must be broad enough to cover the fraud examiner's legal expenses, provide for independent counsel, and protect the fraud examiner from liability in case of an adverse finding, but it should also provide for the cost of time and expenses of the fraud examiner at the fraud examiner's usual hourly rate.

It can be extremely frustrating and expensive to spend days in court working on someone else's case with no retainer.

SAMPLE INDEMNITY CLAUSE

[Client company] agrees to indemnify and hold harmless [fraud examiner's company], its personnel, agents, subcontractors, and consultants from and against any and all claims, liabilities, cost, and expenses, including labor arbitration or related proceedings, (including without limitation, independent legal representation of [fraud examiner company]'s choice, attorney's fees, and the time of [fraud examiner's company] personnel, operatives, and consultants involved to defend or appear at any judicial or quasi-judicial proceedings), brought against, paid, or incurred by [fraud examiner's company] as a result of any of its services provided to [client company] in this project.

This includes, but is not limited to, any claims arising from violations of any laws relating to personal injury or property damage whatsoever suffered by [client company], its employees, or third parties. This provision shall survive the termination of this agreement.

Close

The closing section should conclude the letter. It should thank the addressee for the opportunity, and it should include the fraud examiner's contact information where he can be reached.

Also, the closing should include the date of agreement, client signature, printed name, client's contact information, and the fraud examiner's signature. The fraud examiner should ask the addressee to sign one copy and return it in a self-addressed stamped envelope.

Issuing Advisory Letters

An individual or organization can use an advisory letter to convey information intended to inform or opine about an issue relevant to a client or member-base. These letters include an auditor's formal opinion concerning a company's financial operations, an attorney's opinion regarding a particular point of law, or a fraud examiner's general findings as to the presence of fraud—or lack thereof. Several examples of fraud examination advisory letters can be found in Appendix A.

Assembling the Fraud Team

Fraud examinations usually require a cooperative effort among different disciplines; therefore, if members of management decide to investigate suspicions of fraud, they must determine who should lead and be involved in the investigation.

To determine this, management must identify the needed skills. Typically, fraud investigations require skills across different disciplines and industry sectors. Auditors, fraud examiners, managers, attorneys, security personnel, and others are frequently associated with fraud investigations.

Selecting the right team members is essential for an effective fraud examination. Accordingly, when choosing the participants in an investigation team, it is critical to identify those who can legitimately assist in the investigation and who have a legitimate interest in its outcome. These persons should be included on the investigation team, and all other personnel should be excluded from the team.

Also, when organizing the team, it is important to consider all of the implications that might arise from an investigation. These implications include the business, legal, human resources,

and operational factors that arise when an investigation commences. Addressing these potential issues up front will ensure that significant factors (e.g., the team members' abilities, the leading executives, and the assurance of independent action and reporting) are considered.

Furthermore, the team should comprise professionals with the skills needed to deal with various types of incidents. To acquire the appropriate level and mix of skills, the team should include internal resources (if available) and external resources, if needed or appropriate.

Typically, team members should have:

- Accounting and audit knowledge
- Knowledge of the industry
- Knowledge of the organization
- Knowledge of the law and the rules of evidence in the jurisdiction where the fraud occurred
- Knowledge about privacy issues in the jurisdiction where the fraud occurred and where the investigation will occur
- An understanding of psychology and motivational factors
- Interviewing skills, in the native language
- Communication skills
- Computer skills

A successful fraud examination, however, depends not only on the knowledge and skills of individual members, but also on the individual team members' characteristics that facilitate team interaction and functioning. These characteristics are especially critical for teams that require more coordination.

After identifying the necessary skills and characteristics, management must determine who possesses them and begin selecting the team. Each team will vary, depending on the goals, circumstances, and people involved.

Common Types of Professionals

A typical fraud examination team might include the following types of professionals:

- Certified Fraud Examiners (CFEs)
- Legal counsel
- Local international counsel

- Accountants or auditors (internal or external)
- Forensic accounting investigators
- Forensic technology experts
- Audit committee members
- Security personnel
- Human resources (HR) personnel
- A management representative
- Information technology (IT) personnel
- Computer forensic experts
- Data analytics specialists
- External consultants
- Industry specialists

CERTIFIED FRAUD EXAMINERS

Certified Fraud Examiners (CFEs) are trained to conduct complex fraud cases from inception to conclusion. A CFE has training in all aspects of a fraud examination and can therefore serve as a valuable "hinge" to the investigation team, tying together the financial examination and the more traditional investigative techniques.

LEGAL COUNSEL

It is crucial to have legal counsel involved in, and in most cases, "directing," fraud examinations, at least as far as the legal aspects of the process are concerned (e.g., reporting results, preserving confidentiality, avoiding lawsuits, or terminating employees for wrongful misconduct). This is because fraud examination can be a veritable hornet's nest of legal questions, and the team must have legal counsel on hand to sort out these questions. Otherwise, the investigating organization risks exposing itself to greater danger than the threat it is investigating.

In addition, by having an attorney directing the investigation, or overseeing an investigation conducted at the attorney's request, the company might be able to protect the confidentiality of its investigation under certain evidentiary privileges (e.g., the attorney-client privilege in the United States and the legal advice privilege in the United Kingdom) and similar forms of protection that shield certain types of evidence from being discovered or produced during trial.

LOCAL INTERNATIONAL COUNSEL

Management should obtain the help of local international counsel before beginning a fraud investigation involving work abroad.

Local international counsel is needed to address a number of issues that arise when working in foreign jurisdictions. For example, local counsel will be able to provide advice concerning applicable privileges. Likewise, consulting with local counsel can provide guidance as to whether local laws afford employees privacy rights that might interfere with the investigation.

ACCOUNTANTS OR AUDITORS (INTERNAL OR EXTERNAL)

Because accounting and audit knowledge is necessary to most fraud examinations, a team might include accountants or auditors, whether internal or external. Auditors can support the investigation with information on company procedures and controls. Internal auditors are often used to review internal documentary evidence, evaluate tips or complaints, estimate losses, and provide assistance in technical areas of the company's operations. Additionally, auditors can assess the probable level of complicity within the organization, and they can help design procedural methods to identify the perpetrators and help determine the extent of the fraud.

FORENSIC ACCOUNTING INVESTIGATORS

A forensic accountant can provide various services, including audits; accountant performance reviews; and examinations of financial documents for fraud, misconduct, or industry standard violations. Moreover, these experts can mine and analyze large amounts of data to identify potentially irregular transactions and high-risk relationships.

AUDIT COMMITTEE MEMBERS

As a result of the passage of the Sarbanes-Oxley Act in the United States and similar legislation in many other countries, audit committees are taking a more active role in internal investigations. This has occurred, in part, because such legislation mandates that audit committees for publicly traded companies be directly responsible for two key components of an effective fraud prevention program—outside audits and internal reporting mechanisms. Accordingly, a company's audit committee might actively oversee a fraud examination or require that the investigation team report directly to it.

SECURITY PERSONNEL

Security department investigators are often assigned the investigation's fieldwork responsibilities, including interviewing outside witnesses and obtaining public records and other documents from third parties.

HUMAN RESOURCES PERSONNEL

The human resources (HR) department should be consulted to ensure that the laws governing the rights of employees in the workplace are not violated. Such involvement will lessen the possibility of a wrongful discharge suit or other civil action by employees. Also, involving HR personnel can help provide access to the organization's policies and any employee information that might be needed. Moreover, HR can help the team understand office procedures, and if needed, it can help place suspect employees on paid leave if necessary.

Although the team might need advice from a human resources specialist, normally this person would not directly participate in the investigation.

MANAGEMENT REPRESENTATIVE

A representative of management or, in significant cases, the audit committee of the board of directors should be kept informed of the progress of the investigation and should be available to lend necessary assistance.

INFORMATION TECHNOLOGY PERSONNEL

If fraud occurs, it is likely that a computer was involved. If so, information technology (IT) department personnel might need to be part of an investigation to help identify what data is available and where it is located, as well as to help safeguard the data until it can be analyzed.

COMPUTER FORENSIC EXPERTS

When developing a fraud examination plan, management should determine whether a computer forensic expert is needed.

In today's world of increasing technologies, more and more information is created, stored, and disseminated electronically. Due to the sensitivity of digital evidence, the team should include a computer forensic expert if an investigation involves more than cursory analysis of electronic evidence. Moreover, with the majority of communication being conducted electronically, emails can be used as evidence in just about any case.

Computer forensic experts can uncover a large amount of data that relates to the use of a computer, what is or has been stored on it, and the details about the computer's users. Additionally, computer forensic experts might be able to recover evidence that a non-expert cannot. For example, if the target of an investigation tries to delete electronic evidence, a forensic expert might, depending on when and how the files were deleted, be able to recover the deleted files. Similarly, a forensic expert might be able to get around encrypted information.

Also, it is important to allow a trained examiner to conduct a proper seizure and examination of digital evidence to help ensure that the information can be used in a legal proceeding. Within the computer forensics field, there are several different types of special experts. Given the diversity of computer-related fraud, no person can be an expert in all aspects of computer technology.

Moreover, in cases involving litigation, a forensic expert can help parties draft interrogatories and requests for production designed to solicit relevant data, and they can help prepare and participate in depositions involving record custodians.

DATA ANALYTICS SPECIALISTS

As the volume of electronic records continues to grow, it is increasingly necessary for investigation teams to include data analytics specialists. These specialists are adept at searching, collecting, extracting, cleansing, analyzing, and modeling data. Thus, data analytics specialists can help manage costs, especially in larger, more complex investigations.

EXTERNAL CONSULTANTS

When conducting a fraud examination, fraud examiners should determine whether a technical specialist is needed for assistance.

Additionally, when the suspect employee is particularly powerful or popular, it might be useful to employ outside specialists who are relatively immune from company politics or threats of reprisals.

INDUSTRY SPECIALISTS

In some cases, it might be necessary to include an individual with deep industry knowledge. Industry specialists can help develop the investigation plan, evaluate technical documents, and identify potential misstatements by interviewees.

Dos and Don'ts for Selecting Team Members

The dos for selecting team members include:

- Consider the team's size.
- Check for conflicts of interest between internal and external team members.
- Ensure that there are no reporting issues (e.g., a team member feels pressure to report all details of the investigation to his direct manager, even though his manager does not have a need to know). Reporting issues can be prevented by establishing confidentiality rules in the beginning of the investigation.
- Select team members that fit the investigation's demands and objectives.
- Recruit team members with the skills needed to conduct the investigation.
- Recognize the unique knowledge, experience, and skills that each team member can contribute.
- Contemplate the ways that each potential member will fit into the team.
- Select people who will work well with other team members.

The don'ts for selecting team members include:

- Don't select team members based on friendship.
- Don't select team members to repay a favor.
- Don't select team members with negative attitudes.
- Don't overlook team members with untraditional knowledge that can contribute to the investigation (e.g., people with experience in a particular industry).
- Don't select members who might have personality conflicts with other members.
- Don't select members with a vested personal or corporate interest in the matter.
- Don't select members with a close personal or professional relationship with the subject or the complainant.
- Don't select members who lack restraint and a sense of discretion.

Identify the Investigation Leader

When evidence of fraud arises, management must designate someone to lead the investigation. A leader should have investigative experience and knowledge of legal and compliance requirements regarding the specific issues involved.

The investigation leader should be determined based upon the seriousness of the allegation. Management should consider whether to appoint an internal party (if available) or an external third party to lead and oversee the investigation.

The leader should be independent of the activity affected by the alleged fraud and have the means to recruit resources necessary to conduct the investigation, sufficient authority and access to gather any necessary information, and the ability to communicate with senior management.

Learning About the Organization at Issue

When tasked with conducting a fraud examination involving an organization, the team must become familiar with (if it isn't already) the organization, its industry, its competition, its market share, its financing structure, its vendors (suppliers), its customers, its methods of receipts (i.e., cash or on account) and disbursements, its procurement methods, its economic climate, its recordkeeping system, its policies and procedures, its organization chart and job responsibilities of key employees, and other matters that might be relevant to a fraud examination.

Understanding the entity will enable the team to assess the risks associated with the entity's particular operations.

Developing an Investigation Plan

Once it is determined that an allegation or issue will be investigated, those responsible should develop an investigation plan.

Each member of the team should be involved in the planning process. Letting each team member contribute to the planning process increases the likelihood that everyone will buy into the plan and results in a team approach that draws on each member's expertise.

The team should start planning early and update the plan throughout the investigation. Planning is not a one-time event; it is an ongoing process that requires constant attention, and the team must refine their plan as the facts and client's (or employer's) needs change.

Each fraud investigation is different, and no single plan can cover every situation. The facts and circumstances of each case should shape how an investigation is structured, what procedures are performed, and how those procedures are carried out. Nevertheless, it can help to have a standard set of items from which to begin the planning process.

In short, when developing an investigation plan, those responsible should:

- Review what is known and gain a basic understanding of key issues.
- Define the goals of the investigation.
- Identify whom to keep informed.
- Determine the scope of the investigation.
- Establish the investigation's timeframe.
- Address the need for law enforcement assistance.
- Define members' roles and assign tasks.
- Address operational issues.
- Outline the course of action.
- Adapt the necessary resources to conduct an investigation.
- Prepare the organization for the investigation.

Review What Is Known and Gain a Basic Understanding of Key Issues

The known information should serve as the basis for the plan. So, before writing the investigation plan, the fraud examiner must review what is known and gain a basic understanding of issues that are key to planning the investigation.

Typical questions to answer before beginning a fraud examination include:

- What period is under review?
- What is the timeframe?
- What are the deadlines?
- What is the nature of the suspected fraud?
- Where are the relevant locations?
- Who is the contact at the locations?
- Who are the targets?
- Does the issue predate any of the key players?
- Have any related fraud examinations ever been conducted at the relevant location?
- What other entities, departments, or regions might be involved?
- How long has the issue existed?
- What is the culture of the industry or department at issue?
- What other sites might be involved?
- Does the organization perform background checks of employees as a precondition of employment?
- Did the suspected fraud occur in an industry or location that has a history or culture of fraud?

- Has the organization been in compliance with reporting and regulatory requirements?
- What is the profitability of the unit or organization at issue in the investigation?
- Does the organization's level of growth make sense in light of its industry and peers?
- Has there been a recent acquisition, and if so, is former management still in place?
- Does the organization have a fraud policy?
- What type of report (written or oral) does the client expect?
- What is the budget?

After the fraud examiner obtains a basic understanding of the key issues, he can begin developing the investigation plan.

Define the Goals of the Investigation

An investigation must have goals or a purpose, which should be identified at the outset so the team members can achieve them. Goals also help keep the investigation focused and on task, and they can serve as an energizer, as long as they are specific, well defined, and measurable. A specific goal is more likely to be achieved than a general goal. If goals are not well defined, the team cannot expect to reach them, and goals must be realistic within the availability of resources, knowledge, and time. Measurable goals will allow the team to determine attainability, estimate a timeline, and know when the goals have been achieved.

Although the basic goal for most fraud investigations is to determine whether fraud occurred, and if so, who perpetrated it, fraud investigations might be designed to achieve a number of different goals, such as to:

- Prevent further loss or exposure to risk.
- Determine if there is any ongoing conduct of concern.
- Establish and secure evidence necessary for criminal or disciplinary action.
- Minimize and recover losses.
- Review the reasons for the incident, investigate the measures taken to prevent a recurrence, and determine any action needed to strengthen future responses to fraud.
- Help promote an anti-fraud culture by making it clear to employees and others that management pursues all cases vigorously and takes appropriate legal or disciplinary action where it is justified.
- Protect the company's legal privileges.

Identify Whom to Keep Informed

At the outset of a fraud examination, the investigation team and management must identify whom should be kept informed about the investigation. In general, as few people as necessary should be kept informed.

Factors to consider when determining whom should be kept informed include the severity of the incident under investigation, the suspect's role in the organization, and the tasks that will be required to conduct the investigation.

Determine the Scope of the Investigation

When planning an investigation, the stakeholders should identify the *scope* (the boundaries or extent of the investigation), which will vary depending on the facts and circumstances. An investigation, for example, might be limited to the subject matter, the department, or the geographic area at issue.

To determine the scope, those responsible should use the following guidelines:

- Consider the ultimate goals of the investigation.
- Develop a list of key issues raised in the initial assessment.
- Determine the level of discretion that is required.
- Determine if there are any constraints (e.g., time, resource, authority, procedural, legal, or practical). (Identifying such limitations helps ensure that the team can meet realistic objectives and develop alternative strategies.)
- Consider the quality of the organization's anti-fraud program and policies.
- Consider the organization's actual culture of compliance.
- Determine the extent to which mid- and senior-level management is involved in the suspected misconduct.
- Determine whether the issue is widespread or isolated to a particular area.
- Ascertain whether the suspected misconduct was prohibited by the organization's compliance program.
- Consider broadening the scope if the allegations indicate a failure in the organization's compliance program.
- Consider what the government expects.

Additionally, to determine the scope, the team and management should also consider how the issue became known (i.e., what prompted the investigation). Fraud issues can stem from a number of different sources, and different sources prompt different responses. If, for

example, the issue arose out of a government investigation, the company's investigation should closely examine the government's actions.

Establish the Investigation's Timeframe

When planning the investigation, the team must establish proper time parameters with start dates and due dates for tasks and deliverables. Also, the team should obtain the dates of upcoming earnings releases and audit committee meetings.

An established timeframe helps the team provide a quick and appropriate response, which can help the subject organization avoid future legal disputes and minimize adverse impact on employee morale.

In addition, time parameters will help the team members structure their plans, providing information to help develop concrete, short-range actions to reach the investigation's goals.

Address the Need for Law Enforcement Assistance

The planning stage of the investigation should also include efforts to consider the need for law enforcement assistance. That is, management must decide if the matter at issue is serious enough to call in the police or other law enforcement entities. Whether to seek assistance from law enforcement can be a difficult decision for organizations to make.

If, at the beginning of the investigation, management determines that it will make a formal referral to law enforcement or a prosecuting agency, then it must notify the authorities before the investigation commences to determine whether law enforcement personnel should participate in the examination.

Define Members' Roles and Assign Tasks

The team's authority levels, responsibilities for action, and reporting lines should be defined during the planning process. For efficient and effective coordination, all team members must be clear about their roles and responsibilities and the investigation's goals. Also, defining the members' roles and responsibilities gives them purpose and checkpoints for measuring success.

Conversely, failure to define roles and responsibilities can have an adverse impact on an investigation. Without clear roles, the team might waste time and money, gaps in

the investigation process might appear, or the investigation might lead to incomplete or faulty results.

That said, delineating the team members' roles is difficult because fraud investigations often are conducted in an unstable and high-pressure atmosphere that disrupts communication. Nevertheless, it needs to be a priority for management and individuals on the team.

In general, team members should understand:

- Their expected roles and responsibilities
- The expected roles and responsibilities of other team members
- The degree and source of any outside scrutiny
- Timing issues
- Expected form and timing of interim deliverables or final product
- Specific facts of the matter at issue
- Limitations on who can be involved in the investigation

Moreover, if the organization at the center of the investigation does not have a pre-established line of authority in its fraud policy or investigative protocols, the investigation plan should define the team's authority levels, responsibilities for action, and reporting lines. This allows for efficient and effective coordination.

Management should designate a primary contact person with whom the team can communicate on all matters that arise during the investigation. It is essential that the team reports to someone who will take action pursuant to the investigation's findings.

Address Operational Issues

During the planning process, management must consider any operational issues, which might include:

- Gathering facts abroad
- Recordkeeping practices abroad
- Record content and format differences
- Language translation
- Cultural differences
- International data privacy issues
- Differing conceptions of privacy and discovery

- Immigration regulations
- Safety concerns, especially for global assignments

Among the issues listed, international data privacy laws are of particular concern. Many foreign countries—and those in the European Union (EU) in particular—restrict or prohibit processing and transferring personal data. For example, the EU's directive on personal data protection (EU Directive), which has served as a model for the personal data protection laws of Argentina and Poland, essentially requires consent to use personal data and places limits on transmitting personal data to non-EU countries. Thus, the data privacy laws of other countries can significantly affect data collection, data use, and cross-border transfer.

Similarly, because recordkeeping practices in other countries differ, difficulties can arise when attempting to obtain information in foreign countries.

Outline the Course of Action (Case Plan)

Before beginning a fraud examination, the investigation team should develop a case plan to make sure it addresses every relevant issue. A case plan outlines the course of action the team members expect to take throughout the investigation, and establishing a case plan helps the team stay on track and focus on the key issues.

The case plan can encompass matters such as:

- The scope of the investigation
- The goals of the investigation
- Time parameters
- Resources needed
- Task assignments
- The overall approach to conducting the investigation

Also, the case plan should, among other things, outline how and in what order the team will proceed. Those responsible should organize an investigation by breaking it down into smaller, more manageable components. It is important, however, to avoid excessively breaking down an investigation, because doing so can lead to micromanagement or inefficient work management.

There are many ways to organize an investigation's components, but often, investigations are organized in the following ways:

- *Chronologically:* A chronological investigation is divided into time-based phases that, when completed, are marked as milestones. The phases are the broad steps needed to complete the investigation, and each phase contains tasks that define the actions needed to reach each milestone. The tasks should be assigned based on who is best suited to perform them. Milestones indicate the investigation's overall progress. This structure is best suited for investigations where time sequence is essential in organizing tasks.
- *By functional area:* This approach organizes investigations by functional areas needed to accomplish the investigation's goals. Thus, this approach focuses on the type of activities and processes that must be done under each functional area.
- *By team member:* This method of organization involves organizing the investigation's work by each member's area of expertise.
- *Hierarchically:* This approach organizes the members' roles and tasks hierarchically, from major undertakings to minor undertakings. Thus, the components are organized based on their relationship to each other.

Also, because the case plan should outline how and in what order the team will proceed, it should identify the information that is necessary to complete the investigation and include the investigative activities to be performed, such as:

- Documents and evidence that should be located, obtained, and examined
- A list of witnesses and subjects to interview and the preferred order of the interviews
- The date that a report of the investigation should be presented
- Matters that need supervisory review and approval

When developing the case plan, the team should consider:

- How to most efficiently achieve the goals of the investigation
- How to accomplish the goals of the investigation on a timely basis, with appropriate confidentiality and fairness to all parties
- How to ensure that the investigation's results are thorough, accurate, and documented appropriately
- How to ensure compliance with the law and the organization's policies and procedures

Moreover, the circumstances will change and new information will emerge during the course of an investigation, so the team and the plan must be adaptable.

Each stage of the investigation should be documented. Documenting the planning process will demonstrate advance thought and preparation, and will show thoroughness and help counter challenges that the investigation was inadequate.

It is helpful to prepare to-do lists or checklists for an investigation. For reference, a sample checklist is located in Appendix B. The sample checklist, however, is not intended to cover all aspects of the examination, but rather to provide the examination team with planning assistance.

Adapt the Necessary Resources

As with any special investigation or operation that requires advance preparation, the planning process in a fraud investigation must include efforts to adapt the resources needed to deal with the variety of issues that might occur during the course of the investigation. A successful fraud investigation requires support from management, the right supplies, adequate funding, and any other identified resources.

That is, the investigation team needs to have the tools necessary to complete the investigation. This is especially true if the relevant operations are in developing economies, remote locations, or areas with a higher risk of security-related incidents.

The necessary resources might include:

- Outside specialists
- Case management software
- Digital forensics tools (e.g., EnCase or Forensics Toolkit)
- Access to a commercial database

Also, every team member should have the contact information for those involved in the investigation.

Prepare the Organization for the Investigation

Before commencing a formal investigation (and especially before starting the evidence collection process), it might be necessary to prepare the subject organization for the investigation. Preparing an organization for an investigation involves such things as:

- Prepare the managers of the employees who will be involved in the investigation, especially if they do not know about the issue. Let them know that the subject and

witnesses might be busy at times during the investigation. The amount of information to share with a manager will depend on the circumstances.
- Notify key decision makers when the investigation is about to begin.
- Notify the organization's in-house or outside counsel when the investigation is about to begin.

But generally, it is not good practice to alert all of an organization's employees that an investigation will be taking place, nor should the investigation's purpose be explained to all employees.

Structure the Investigation to Preserve Confidentiality

Fraud investigations must be structured to preserve confidentiality. If confidentiality issues are not given attention from the outset of the investigation, the details of the investigation might become public, compromising the entire investigation. Additionally, if the details of the investigation do not remain confidential, employees will be reluctant to report future incidents, and if the suspicions giving rise to the investigation prove unsupported, the reputations of those suspected of misconduct might be irreparably damaged. Moreover, if an investigation stems from a complaint and the complaint becomes known, it is possible that the complainant could be retaliated against.

Accordingly, those responsible must structure the investigation to preserve confidentiality. Among other things, the team members should:
- Avoid alerting the suspected fraudster(s).
- Request participants' confidentiality.
- Guard case information.
- Consider conducting the investigation under any applicable evidentiary privileges.

Avoid Alerting the Suspected Fraudster(s)

When responding to a sign or allegation of fraud, those responsible must work to avoid alerting those suspected of fraud.

If the suspect is inadvertently informed of the investigation, a number of different adverse events might occur. For instance, the fraudster might attempt to destroy or alter evidence,

making it more difficult to conduct the investigation. When investigation details are leaked, concealment and destruction of evidence typically occurs at a faster rate.

Additionally, a forewarned suspect might attempt to flee, cut off contact with associates, or try to place the blame on somebody else.

Because unintentionally notifying the fraudster is a key concern in any investigation, the confidentiality of an internal investigation is critical. To avoid alerting those suspected of misconduct, it is important to have information about the person who is being investigated and what he can access. Also, to maintain confidentiality, determine in advance who should receive information about the investigation and reevaluate who should receive information as the investigation proceeds.

Here are some basic measures organizations and fraud examiners can take to avoid notifying suspected perpetrators who are under investigation:

- Know who is being investigated and what they can access.
- Limit the extent of any discussions.
- Only inform those who need to know.
- Inform employees of the consequences of a confidentiality breach.
- Work discreetly without disrupting the office's normal course of business so that employees do not know that an investigation is being performed.
- Work fast.
- Investigate during off hours.

Moreover, it is important for fraud examiners to be knowledgeable about the subject organization's guidelines or policies. Do the applicable guidelines or policies have a need-to-know clause and an all-access clause? Such clauses will allow the team to keep the details of the investigation confidential, and will provide the investigator with access to all the company systems so he can gather as much system evidence as possible without notifying any internal parties.

Finally, if the suspect is alerted, management should adjust the investigation and its timeline accordingly. This might mean interviewing the fraudster out of sequence from a normal investigation.

Request Participants' Confidentiality

To preserve the confidentiality of an investigation, management might (if legally permissible) remind participants to refrain from discussing investigation information with anyone or require participants to sign a confidentiality oath vowing not to divulge any information regarding the investigation.

Generally, an employer can ask employees to keep an investigation confidential when there are legitimate business justifications for making such requests. However, it is usually not wise for management to implement a blanket policy prohibiting employees from discussing employee investigations, because doing so could violate certain employee rights. Some countries, such as the United States, guarantee private-sector employees the right to organize and engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection. If an employer in such a jurisdiction has a routine policy or practice of asking employees not to discuss matters that are under investigation, the policy or practice might violate the employees' right to organize and engage in other concerted activities.

To illustrate, consider the law in the United States. The National Labor Relations Act (NLRA) is the primary labor law in the United States, and it affects an employer's ability to ask employees not to discuss matters that are under investigation.

On June 16, 2015, the U.S. National Labor Relations Board (NLRB), the entity that enforces the NLRA, expanded its interpretation of what constitutes protected "concerted activity" under Section 7 of the NLRA. Section 7 guarantees most private-sector employees the right to organize and "engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." In its decision, the NLRB ruled that an employer's routine policy or practice of asking employees not to discuss matters that are under investigation violates the NLRA, even where the employer did not threaten to take disciplinary action if employees breach confidentiality.

According to the NLRB, employee discussions may be restricted if the employer can show that it has "objectively reasonable grounds" for requiring confidentiality. The decision states that employers must proceed on a case-by-cases basis, determining whether confidentiality is necessary based on the circumstances of each case.

The NLRB provided the following suggestions for cases that would justify a legitimate business justification:

- Witnesses needed protection.
- Evidence was in danger of being destroyed.
- Testimony was in danger of being fabricated.
- There was a need to prevent a cover-up.

It is likely that the second, third, and fourth bullets would apply to most fraud investigations, so fraud examiners could probably request that employees keep their investigations confidential. Still, it appears that before making a request for confidentiality, fraud examiners should document the need for confidentiality.

Based on the NLRB's decision, U.S. employers should no longer have a blanket policy prohibiting employees from discussing employee investigations.

Guard Case Information

To help preserve confidentiality, the investigation team members should guard case information. Here are some recommended procedures for protecting case information:

- Store all confidential documents in locked file cabinets or rooms accessible only to those who have a business need to know.
- Protect all electronic information via firewalls, encryption, and passwords.
- Clear desks of any case information before stepping away.
- Lock computers when leaving workstations.
- Mark all case information, whether tangible or electronic, as confidential.
- Avoid talking about the investigation in public or in any place where other employees could hear the communications.
- Avoid using email or other electronic means (e.g., text messages or instant messages) to transmit confidential case information.

Consider Implementing Any Applicable Evidentiary Privileges

To prevent third parties, including the subject of the investigation, from having access to the investigative materials, management should consider conducting the investigation under any applicable evidentiary privilege that provides the right to keep certain information from being disclosed without permission.

If an evidentiary privilege applies to information, the general rule is that the court and the party seeking the information will be denied access to it, and the triers of fact must disregard

any evidence they do actually hear if it is deemed privileged afterward; however, legal jurisdictions vary on which communications are protected by such privileges.

Typically, the most relevant types of evidentiary privileges for keeping investigations confidential are legal professional privileges. These privileges protect the communications between a professional legal advisor (e.g., solicitor, barrister, or attorney) and his clients, and in some situations, fraud investigations can be structured so that they are afforded protection under such privileges. Generally, to receive protection under a legal professional privilege, an investigation must be conducted at the direction of, or under the supervision of, a legal professional.

In the United States, the legal professional privilege is known as the attorney-client privilege, and it protects against involuntary disclosure of communications between clients and their attorneys. The general rule is that the attorney-client privilege only applies to confidential communications (verbal or written) between a client and his attorney made for the purpose of giving or receiving legal advice, but courts have extended the privilege to include client communications with non-lawyers (e.g., fraud examiners) who are working under the direct supervision, direction, and control of the lawyer.

The U.S. attorney-client privilege, if properly implemented, provides some protection from discovery of internal reports by the subject of the investigation, the government, or third parties. The privilege might also assist in protecting the confidentiality of witnesses. It does not protect the underlying evidence or documents that do not meet the criteria outlined above, and it cannot be claimed retroactively to cover work done before counsel was involved.

In addition to legal professional privileges, litigation privileges and other similar evidentiary protections, such as the U.S. attorney work-product doctrine, can protect the confidentiality of investigations. These protections shield materials that are prepared in anticipation of litigation.

The U.S. attorney work-product doctrine, for example, protects tangible materials from discovery that are prepared in anticipation of litigation. To apply this doctrine, litigation must actually be planned, and the work for which protection is sought must have been undertaken for the specific purpose of preparing for that litigation. Also, the protection offered by this doctrine extends to not only information and documents prepared by a party

or the party's attorneys, but also to information and documents by third-party consultants and examiners hired by the attorneys. For instance, communications with the attorney and any work or analysis conducted by an expert with whom the attorney has consulted is privileged as work product, although that privilege will be waived if the expert is called to testify as an expert witness at trial.

For more information on evidentiary privileges, see the Law section of the *Fraud Examiners Manual*.

ANALYZING DOCUMENTS

The fraud examiner will usually obtain a great deal of documentary evidence when conducting fraud investigations. It is critical that the fraud examiner understand the relevance of this evidence and how it should be preserved and presented. Fraud examiners should always keep in mind that documents can either help or hurt a case, depending on which ones are presented and how they are presented. They should strive to make certain that all relevant documents are included and that all irrelevant documents are eliminated. Many fraud examiners pay too much attention to documents. It is important to remember that witnesses (those who testify at trial) are more important to a fraud case than documents are. While documents are important in giving a witness and the case credibility, witnesses who spend too much time focusing on a document's details will often confuse and bore the fact finders (i.e., the judge or jury members, depending on the jurisdiction's legal system).

Basic procedures in handling evidence are required for documents to be accepted, or given much credence, by the court. Proof must be provided that the evidence is relevant, material, and authentic.

The relevance of documents cannot be easily determined early in a case. For that reason, all possible relevant documents should be obtained. If they are not needed, they can always be returned. Here are a few general rules regarding the collection of documents:

- Obtain original documents where feasible. Make working copies for review, and keep the originals segregated.
- Do not touch originals any more than necessary; they might later have to undergo forensic analysis.
- Maintain a dependable filing system for the documents. This is especially critical when large numbers of documents are obtained. Losing a key document is very problematic and can damage the case. Documents can be stamped sequentially for easy reference.

Obtaining Documentary Evidence

Documentary evidence may be obtained in a number of ways. It is possible to obtain evidence by consent, if both parties agree. This is the preferred method. In some cases, consent can be oral, but when information is obtained from possible adverse witnesses or the target of the examination, it is recommended that the consent be in writing. Sample

consent forms can be found in Appendix C. In many cases, however, the investigator will not wish to alert the suspect to his intentions; thus, other routes must be taken.

If the party that requests the information owns and controls the evidence (e.g., documents in an employee's desk drawer at the office), then the investigator is usually able to obtain the documents as required.

Additionally, certain types of records can be obtained by consent only if the subject of the records consents in writing. Accessing a subject's bank records from financial institutions, for instance, generally requires written consent. If no consent is given and evidence is held by other parties or in uncontrolled locations, specific legal action might be required. Most often, the legal process used takes the form of a subpoena or other court order to produce the documents and records (including electronic records). Other forms of court orders can be used to obtain witness evidence and statements.

Under no circumstances should the investigator attempt to obtain documents by other means, as this can lead to charges of theft, trespass, and other sanctions. Further details are provided in the Law section of the *Fraud Examiners Manual*.

Types of Evidence

There are two basic types of admissible evidence: direct or circumstantial. *Direct evidence* shows prima facie the facts at issue; it proves the fact directly. What constitutes direct evidence depends on the factors involved. For example, in a case involving possible kickbacks, direct evidence might be a check from the vendor to the suspect.

Circumstantial evidence is evidence that tends to prove or disprove facts in issue indirectly, by inference. In the case of a kickback allegation, cash deposits of unknown origin deposited to the suspect's account around the time of the suspect transaction could be considered circumstantial evidence.

Organization of Evidence

Keeping track of the amount of paper generated is one of the biggest problems in fraud cases. It is essential that documents obtained be properly organized early on in an examination, and that they be continually reorganized as the case progresses. Remember, it is

usually difficult to ascertain the relevance of the evidence early in the case. To maintain effective organization in complex cases, fraud examiners should use the following methods.

Segregate the Documents

In general, documents should be segregated by witness or transaction. In the former method, the fraud examiner takes the list of names, whether employee, associate, or witness, and begins assembling collected documents by witness. Alternatively, the fraud examiner might find it easier to organize the information by grouping evidence of the same or similar transactions together. During the evidence-gathering stage of an investigation, organizing the documents chronologically is not recommended because it will make searching for relevant information more difficult. It is generally better to organize them by transaction or by party. The fraud examination report often follows a chronological timeline to give a narrative of a fraud scheme, in which case displaying key documents chronologically often makes sense. But in the organization phase, there usually is too much clutter for chronological organization to be effective.

Make a Key Document File

Fraud examiners should make a *key document file*—a separate file that contains copies of certain important pieces of information for quick access—for easy access to the most relevant documents. Periodically review the key documents. Move the less important documents to backup files and keep only the most relevant documents in the main file.

Establish a Database

Establish a database early on in the investigation and code all documents if there is a large amount of information to process. This database can be manual or computerized and accessed by keywords or Bates Stamp numbering. The coding system should provide meaningful and comparable data; therefore, the database should, at a minimum, include the following fields of information: the date of the document, the individual from whom the document was obtained, the date obtained, a brief description, and the subject to whom the document pertains.

Maintain a Chronology

A chronology of events should be commenced early in the case. The purpose of maintaining a chronology is to establish the chain of events leading to the proof. The chronology might or might not be made a part of the formal report; at a minimum, it can be used for analysis of the case and placed in a working paper binder. Keep the chronology brief and include only information necessary to prove the case. By making the chronology too detailed, you

defeat its purpose. The chronology should be revised as necessary, adding new information and deleting irrelevant details.

Keep a Checklist

Another indispensable aid is the checklist. The checklist, which must be updated frequently, should be kept in a stenographer's pad or other permanent ring binder to allow a cumulative record. In a very complex case, the list can be broken into long- and short-term objectives: that which must be done eventually (e.g., prove elements of a particular count) and that which should be done tomorrow (e.g., conduct an interview or draft a subpoena). However organized, some sort of list must be kept; otherwise, important points will be forgotten in the lengthy case. A sample checklist is included in Appendix B.

Examining Fraudulent Documents

Forged, altered, fabricated, and other suspicious documents are regularly encountered in fraud cases. Most businesses, legal issues, or financial transactions will produce a substantial amount of paper, including contracts, agreements, wills, order forms, invoices, and statements. These documents can be evidence in establishing that a fraud was committed, in determining the nature and scope of the fraud, and in identifying the parties responsible.

The fraud examiner is not expected to be a document expert. He should, however, be aware of ways to spot phony documents and have knowledge of the capabilities and limitations of forensic examinations. In addition, if the fraud examiner suspects that significant documents are phony, he should consider consulting with a forensic document expert. Forensic examinations conducted as a part of a fraud investigation can contribute to its success in several ways:

- Expert examination results can assist in developing and proving the fraud theory: who did what and when they did it.
- Expert examination results can corroborate or refute statements by witnesses or fraud suspects.
- Having the results of expert examinations before interviews can provide significant leverage for the fraud examiner during his interviews with fraud suspects, even resulting in admissions of guilt from suspects who are confronted with the factual evidence.
- Forensic handwriting examinations and comparisons can result in the positive identification of the writer or signer of a document. Because writing is a conscious act,

the identification might serve to prove that a particular act is intentional or willful. Proof of intent is usually necessary to prosecute a wrongdoer successfully.
- Forensic experts may testify at trial to explain evidence discovered through their analysis.

Early Consultation with an Expert Can Prove Valuable

An expert's assistance can be of value early in an investigation, not just in preparation for a trial. Fraud examiners should consider consulting with experts early in their investigation or inquiry if they suspect that significant documents are phony or have been forged, altered, or otherwise manipulated. Many times the scope of an investigation can be narrowed or directed by eliminating multiple suspects through handwriting examinations. The expert's findings might solidify the fraud examiner's theories of how the fraud was committed, or they can prevent wasted effort by proving theories incorrect at an earlier stage. See the end of this chapter for more information about finding help in document examinations.

Types of Forensic Document Examinations

There are many different types of forensic document examinations. However, most examinations concern signatures, handwriting, hand printing, or documents created by a typewriter or word processor. Additionally, issues concerning photocopies and determining when a document was prepared frequently arise. Fraud examiners should be aware that many different types of forensic examinations are possible, but that the following forensic examinations could be of particular value when a fraud involves documents:

- Detecting forged signatures
- Identifying the writers of signatures, handwriting, and hand printing
- Detecting altered documents
- Detecting and restoring erasures and eradications
- Determining when a document was or was not prepared
- Detecting counterfeited documents and examining printed documents
- Detecting and restoring faint indented writings
- Comparing paper and inks
- Determining whether two sheets of paper came from the same tablet or pad of paper
- Examining paper folds and sequence of folds
- Comparing torn or cut paper edges
- Restoring charred and partially burned documents
- Identifying the machine that made a photocopy and whether two copies were made on the same machine
- Examining facsimile (fax) copies

- Identifying the source of, or alterations to, notary seals, wax seals, and cachets
- Detecting the opening and resealing of sealed documents and examining adhesives
- Detecting inserted text in typewritten, printed, or handwritten documents
- Determining the sequence of handwritten text or signatures
- Identifying rubber stamp impressions
- Identifying mechanical check-writer and numbering-device impressions

Handling Documents as Physical Evidence

A document can be a piece of physical evidence and not just a source of information. As a piece of evidence it should be handled carefully and stored properly in a sealed, initialed, and dated paper folder or envelope to avoid damage or contamination. If necessary, make a working copy and preserve the original document for submission to a forensic document examiner. Most forensic examinations will require the original document, not a copy of it, because most photocopies do not reproduce original writings, typescript, or other features with sufficient clarity or detail to allow adequate examination.

All evidence received should be marked so that it can later be identified. The most common way to mark evidence is with the date and initials of the person obtaining it. If it is not practical to mark the document, or if marking it would damage the document, then it should be placed in an acid-free envelope that has been marked and sealed. To avoid creating indentations on the original document, do not write on the envelope after the document has been placed inside of it. When initialing a document for future identification, do it in a noncritical area and use an instrument that is different from the one used on the document. Other than making unobtrusive initials for identification, do not write or mark on original documents. Do not fold, staple, use paper clips, crumple, or do anything else that would change an item's original condition. Store photocopies and laser-printed documents in paper folders or envelopes, not transparent plastic envelopes; such envelopes can result in the copies sticking to the plastic and destroying some document features.

Chain of Custody

From the moment evidence is received, its *chain of custody* must be maintained for it to be accepted by the court. The *chain of custody* is both a process and a document that memorializes who has had possession of an object and what they have done with it. Essentially, the chain of custody is a recordkeeping procedure similar to physical inventory procedures.

Establishing the chain of custody for a document establishes authenticity (i.e., the document is in fact what the party offering the document says it is), but it also ensures that evidence has not been altered or changed from the time it was collected through production in court. In general, to establish the chain of custody, the fraud examiner must make a record when he receives an item or when it leaves his care, custody, or control. This is best handled by a memorandum with the custodian of the records when the evidence is received. The memorandum should state:

- What items were received
- When they were received
- From whom they were received
- Where they are maintained

If the item is later turned over to someone else, a record of this should be made—preferably in memorandum form. All evidence received should be uniquely marked so that it can be identified later. The preferable way is to initial and date the item; however, this can pose problems in the case of original business records furnished voluntarily. For such records, a small tick mark or other nondescript identifier can be used. If it is not practical to mark the original document, it should be placed in a sealed envelope, which should then be initialed and dated.

Preserving for Fingerprint Examinations

If fingerprint examinations are anticipated, use gloves to handle the documents (be careful if tweezers are used because they can leave indentations that might obscure faint indented writings or the identifiable indentations that are sometimes left by copiers and fax machines). If you or other known people have inadvertently handled the documents with bare hands, your names should be provided to the fingerprint specialist. It might be necessary to provide the expert with sets of inked fingerprints of these people for elimination purposes. (See the "Fingerprints" section for additional information.)

Charred or Partially Burned Documents

Charred or partially burned documents might contain valuable evidence if restored by experts, but they are very fragile and should be handled with extreme care. For proper preservation and storage, trained experts might use special polyester film sheets and envelopes, which are not readily available to the fraud examiner. The fraud examiner can best preserve such evidence for submission to the forensic expert by using a sturdy crush-

proof container into which he places layers of cotton (available in rolls at fabric and sewing materials shops). Carefully slide a sheet of paper or thin cardboard under the burned fragments, lift them and place them on the layers of cotton, and then remove the paper used for lifting. Gently place additional layers of cotton over the fragments until the container is filled. Do not compress the cotton. Seal the container, initial and date it, add an identifying contents label or exhibit number, and clearly write or stamp the word "Fragile" on the container.

Recognizing Phony Documents

Forensic document examiners apply scientific methods and use a variety of technical instruments in conducting examinations and comparisons of documents. Individual minute characteristics in handwriting and typewriting are examined and compared with genuine comparison standards. Detailed analyses are made of document features for proof of changes or modifications. Instruments used include sensitive measuring devices, low-power magnifying glasses, several types of microscopes, ultraviolet and infrared lighting, optical filters, micro and macro photography, computerized image-enhancement systems, sensitive instruments to detect faint indented writings, and numerous others. Various chemical analyses are also conducted.

Although not expected to be a documents expert, an observant fraud examiner might be able to recognize some of the following features of documents that could alert him to their fraudulent nature:

- *Signature forgeries* might be recognized by irregularities noticeable in the written letters or by their differences in size from a genuine signature. A side-by-side comparison of a suspect signature with a genuine signature might reveal the differences. However, remember that advanced age, poor health, temporary injury, and the use of drugs and alcohol can result in similar discrepancies and might mislead the fraud examiner. Additionally, the quality of a signature can be dependent on the circumstance in which it was provided (e.g., a person's signature on a mortgage agreement might be more legible than the same person's scribbled signature on a credit card receipt). Genuine comparison samples should be obtained and a forensic document examiner should be consulted to make an expert determination. (See the "How to Obtain Handwriting Samples" section.)
- *Substituted pages* in multiple-page documents, such as contracts and wills, can often be spotted by holding each page in front of a bright light. Differences in the whiteness, density, thickness, opacity, and paper-fiber patterns of the substituted sheets might be apparent.

- Some *ink differences*, *alterations*, *erasures*, and *obliterations* are also revealed by holding the paper in front of a bright light or holding a light over the writings at different angles and observing differences in the color and reflectivity of the inks or disturbances to the paper surface.
- *Counterfeited printed documents*, such as checks, stock and bond certificates, business forms and stationery, birth certificates, drivers' licenses, and other identification documents, are sometimes readily disclosed by side-by-side comparisons with corresponding genuine documents. Be alert for the use of incorrect or different versions or form revisions of the documents. For forensic examinations, it will be necessary to obtain and furnish genuine comparison samples of the printed documents to the document examiner. (See the "Counterfeit Printed Documents" section.)
- *Suspicious indented writings* might be revealed by reducing the light in the room and holding a bright beam of light (a narrow-beam flashlight or small high-intensity lamp will do the job) low and parallel to the page surface. (See the "Indented Writings" section.)

Identifying Writings

Each person's writings contain a unique and identifiable combination of acquired individual personal characteristics and shared "class" characteristics. In fact, individuals' writing skills vary considerably due to their differing physical and mental capabilities, and these differences between individuals increase with age; physical development; and the acquisition of skills, differing aesthetic values, differences in education, and differences in the personal and professional usage of writing.

Forensic document examiners are trained and experienced in examining and comparing writings and assessing this combination of individual and class characteristics in making expert determinations of identity or non-identity.

Class Characteristics

Fraud examiners should not be misled in developing suspects by mistaking similar class characteristics in different writing samples. Samples that *seem* to look alike are not necessarily from the same individual. The writings of some people might share superficial similarities in appearance and style and look the same to the layman when, in fact, they are very different. Forensic document examiners can correct this mistake.

Copy-Book Styles

Some of a writer's letter shapes, handwriting style, and other characteristics might be shared by other writers because they were taught the same original copy-book system. In the United States, different states and different school districts within the states teach several different copy-book systems. Internationally, different systems are also taught. Writers might retain remnants of the system they learned as children. For example, second-language writings of people taught in a Cyrillic (Russian) alphabet style will be influenced by Cyrillic letter styles and might contain some similarities. Similarly, the hand printing and numeral styles taught to drafters, architects, and engineers might result in apparent similarities in the hand printing of people trained in those professions.

"Copycat" Styles

Some writers, especially adolescents, the young, and the easily influenced, might adopt the general handwriting style or some individual letter designs of a respected teacher or parent, or one shared by their peers. An example is the exaggerated rounded letter forms and circular "i" dots and periods that form the so-called bubble writings of some adolescents. This style is usually abandoned as the person matures.

Natural Variations, Disguise, Distortions, and Forgeries

Variations

No one signs his signature or writes *exactly* the same way twice because writing is a human act of coordinated mental and muscular activity, not the precise, repetitive action of a machine. However, each writer has his own specific range of natural variation. Several examples of writing are necessary for a forensic document examiner to establish if a questioned writing is, or is not, within the range of natural variation of a particular writer. If fraud examiners find two signatures that are exactly alike, then at least one is a forgery, probably a tracing.

Disguise

Disguise is the conscious, intentional effort by a person to change or conceal his normal writings. Disguise is attempted in an effort to prepare writings that can later be disclaimed or that the writer hopes will be anonymous and cannot be traced to the source. The success of an attempt to disguise writings depends on the writer's skill and knowledge of writings. Most attempts at disguise involve one or more of the following: change in slant, change in size, change in shapes of capital (upper-case) letters, changes in the shapes and sizes of loops in

letters that contain them, use of bizarre letter designs, or block (squared) hand printing. Only rarely is the opposite, non-writing hand used. Fraud examiners should be aware that it is possible to successfully disguise writings to the point that they cannot be positively identified, even by experts. This is especially true when only limited amounts of writings are involved.

Distortions

Distortions are unintentional changes to a person's writings that are beyond his range of natural variation. Distortion can be caused by temporary impairment due to illness, injury to the writing hand or arm, substance abuse, extreme physical weakness, unusual writing environment, irregular or unusual writing surface, or unfamiliar writing materials. Distortions can also be permanent due to advanced age and cognitive decline. Fraud examiners should be aware that distortions in writings can, on occasion, be so severe that positive identifications of a person's writings might not be possible, even by experts.

Forgeries

A *forgery* is defined as any writing prepared with the intent to deceive or defraud. Most forgeries are signatures. Forgery can be done by *simulation,* by *tracing,* or by *freehand preparation.*

SIMULATED AND TRACED FORGERIES

A simulated or traced forgery is a writing, usually a signature, prepared by carefully copying or tracing a model example of another person's writings. Although identifiable as a forgery, a simulated or traced signature forgery often does not contain enough of the forger's normal handwriting characteristics to permit expert identification.

Remember, no one writes his signature *exactly* the same way twice. If two signatures look exactly alike, try superimposing the signature areas of the two documents by holding them in front of a bright light. If they match, then one or both are traced forgeries. Be aware that, in some instances, it might be possible to locate the original document bearing the genuine signature that was traced. This regularly occurs in employee fraud and embezzlement cases in banks and other financial institutions where the account holder's signature card on file served as the source for the tracing. If the forged signature precisely superimposes over the genuine signature, then it is also likely that faint indentations might be present in the signature area of the original genuine document. Also, ink traces from the genuine signature might be transferred to the reverse side of the traced signature. Latent fingerprint treatment of the original source document might reveal the fingerprints of the suspect.

FREEHAND FORGERIES

A freehand forgery occurs when a writer signs the name of another person without knowing what the real person's signature looks like. The writers of freehand forgeries can usually be identified by experts.

AUTOFORGERIES

An *autoforgery* is a true-name signature by an individual who intends to deny that signature at a later time. Generally, autoforgeries are prepared in a distorted or disguised fashion. This attempt at fraud has occurred in falsely reported traveler's check theft cases, in cases involving disputed home mortgage and other loan documents, credit card frauds, and others.

The Document Expert's Findings

A forensic document examiner *cannot* conduct a handwriting examination to determine with accuracy the writer's age, sex, race, physical or mental condition, personality, character, or which hand the writer used. There are three basic outcomes of forensic handwriting comparisons.

Non-identification

The suspected person did not write the signature or other writings on the questioned document.

Identification

The suspected person did write the signature or other writings on the questioned document.

Inconclusive

No definite determinations were possible as to whether the suspected person did or did not write the signature or other writings on the questioned document. This outcome is often the result of insufficient or inadequate handwriting samples of the suspect or when a photocopy rather than the original document is submitted to the expert for examinations.

Though inconclusive, some writings might contain common characteristics to indicate possible identity, or differences to indicate that the suspected person might not have prepared the writings. The expert might suggest additional leads for the fraud examiner that could resolve the inconclusive results of the comparisons.

How to Obtain Handwriting Samples

Positive results from forensic handwriting examinations and comparisons often depend on how well the fraud examiner has assembled adequate handwriting and signature samples of the suspects. The samples must be comparable to the writings on the evidence documents. Hand printing cannot be compared with handwriting. Capital letters cannot be compared with lowercase letters. Also, the samples must contain the same letters and combinations of letters. For example: "John" cannot be compared with "Susan," "hot" with "cold," "black" with "white," or "July" with "September."

For comparison purposes, experts use two classes of writing standards: undictated writing and dictated writing.

Non-dictated Writing Samples

Non-dictated writing samples include materials that are written by the individual during the everyday course of business. This type of writing tends to reveal the individual's normal writing habits.

Try to obtain samples of a suspect or victim's signature or other writings that were not prepared by him for comparison purposes, but that can be authenticated. Courts will accept any writings that were witnessed by others. Other acceptable documents include those that were created "in the normal course of business," such as canceled checks; signed or written documents in employee personnel records; applications for employment, licenses, or home utilities installations; and many others. The fraud examiner should use personal experiences and knowledge of the suspect's routine activities to locate sources for these types of samples.

When the evidence documents include suspected forged signatures, several genuine samples of the forgery victim's signature should be obtained for submission to the expert. If possible, include any documents bearing the victim's genuine signature that the suspect might have had access to and that might have served as a model for tracing or simulation.

Non-dictated writing samples should:

- Be as contemporaneous as possible to the date of the evidence documents; if the questioned writings were prepared in the 1970s, writings recently prepared by a suspect might not be adequate for comparisons. However, except for infirmity or extreme age, the writings of most adults usually do not change much except over long periods of time.

- Consist of the same signature or words containing many of the same letters and combinations of letters as the questioned writings on the evidence documents.
- Consist of the same type of writings as on the evidence documents, such as hand-printed or handwritten capital letters or small letters, or a combination of both.
- Consist, if possible, of the same kinds of writings. A person's informal writings, such as hastily prepared signatures on credit card receipts, might be very different from more formal writings, such as a signature on a contract or other legal document.

Dictated Writing Samples

Dictated writing samples are those that are written at the request, and usually in the presence, of the fraud examiner. Fraud examiners should try to obtain dictated samples either voluntarily or by obtaining a legal order.

Obtaining Dictated Handwriting Samples by Court Order

When obtaining a legal order for samples, the investigator or attorney should ensure that the order specifies that the samples should be provided in the writer's normal handwriting and in sufficient quantity, text, and form, at the interviewer's discretion, to permit a determination of identity or non-identity. A court order with these specifications will permit an inference of guilt, or might allow pursuit of contempt of court charges if the suspect refuses to comply or attempts to prevent identification by intentionally disguising his writings, limiting the amount of writings, or failing to follow the interviewer's instructions and dictations.

Preparation for Taking Dictated Handwriting Samples

Because expert handwriting identifications can truly prove the case, adequate pre-interview preparation by the fraud examiner is essential. At the time of the interview session, the investigator should have all of the proper writing materials and should have the original or copies of the evidence documents to serve as a guide for dictating the sample text.

Here are a few tips for conducting this type of interview:

- Do not rush through the interview.
- Take as much time as necessary.
- Take short comfort breaks if the suspect tires.
- Do not allow the suspect to see the evidence documents before or during the process of taking the samples.

Directions for Obtaining Dictated Handwriting Samples

Dictated writing samples should be obtained by using the same types of materials as the evidence document: writing instrument (ballpoint pen, fountain pen, pencil, etc.), paper (lined, unlined, size of sheet), and forms (check forms, business forms, etc.). For purposes of the samples, an investigator can use a genuine form of the same or similar kind, make photocopies of it, and have the samples prepared on the blank copies.

To help the suspect relax, begin by having him write miscellaneous innocuous text, such as his name, the date, and a statement as to the voluntary nature of the samples being prepared. This statement will also assist later in getting the samples admitted in court.

Patiently dictate to the suspect the same text or text containing the same letters and combinations of letters of the same type (hand printed, handwritten, capital, or small letters) as the questioned writings on the evidence document. Do not assist the suspect in the spelling of words, punctuation, or grammar.

Obtain one sample at a time on separate sheets or forms. Once a sample is complete, remove it from the suspect's sight before the next sample is prepared. To ensure that the suspect's range of normal variation is displayed, several samples of each text should be obtained.

Be alert for any attempts to disguise normal writings, such as exaggerated slant, very rapid writing, very slow and awkward writing, unusually large or small writing, or bizarre letter formations. (See the "Natural Variation, Disguise, Distortion, and Forgeries" section.)

Typewriters and Computer Printers

Typewriters

Although typewriters are not commonly used, documents prepared on traditional typebar/segment-shift typewriters, both manual and electric, can often be positively identified by experts who look for mechanical defects unique to each machine. Typewritten texts prepared on later-model typewriters equipped with interchangeable daisy wheel, ball, or basket-type elements are difficult, if not impossible, to identify.

Computer Printers

Relative to typewritten documents, the specific sources of documents made by computerized ink jet or laser printers are far more difficult to identify. In some cases, the only expert determinations concerning items made from these printers are that the same typeface design and size (font), letter spacing, and print process were used. Many brands of laser printers do print small yellow dots on all documents that reveal the printer's serial number and the time and date that the document was printed. These marks can be seen under a microscope or by holding the document under a blue light, which causes the yellow dots to appear black. However, only some law enforcement agencies, such as the U.S. Secret Service, have the ability to fully decode these marks, which are largely used to detect counterfeit currency.

In some instances, experts might be able to identify the product used to print a document. Product identification might be possible because some color printers embed their identification number in some printouts. Similarly, some printers can be identified by minor variants in the way they feed paper through the printing mechanisms.

Photocopies

A *photocopy* is a paper copy of a document or other visual image. Increasingly, photocopies are retained as "original" records of documents (particularly in outgoing correspondence files), and photocopies might be the only evidence of a document if the original cannot be located or, in some cases, cannot be released.

Fraud examiners and other investigators sometimes submit a copy of a document to a document examiner for examination because they do not wish to part with the original. Document examiners, however, cannot uncover certain types of clues, such as indentations and erasures, from photocopies. As a result, document examiners might not be able to determine features and reach conclusions that could have been made from the original documents. Therefore, when possible, the fraud examiner should submit the original document to the document examiner. Original documents should be handled according to their importance, and transferring them will often require the observance of chain of custody procedures.

Identifying the Source of a Photocopy

Photocopies are admissible as original evidence for:

- Anonymous letters
- Unauthorized "leaks" of information in the form of copies of letters, memoranda, files, and other records
- Copies made to conceal forgeries or to insert or manipulate text
- Spurious "disinformation" dissemination of phony official documents

Locating the source of a copy can be crucial in some investigations. And in some cases, it is possible to determine what kind of copier was used to produce the copy in question. Some types of machines leave minute markings, indentations, and other features on the copy that will assist the expert in determining the brand and model of the machine used.

It is also possible to identify the particular machine used by examining the pattern of unique and identifiable "trash marks." *Trash marks* are uniquely identifiable markings on copies (e.g., specks, spots, streaks, or edge markings). Fraud examiners can identify a particular machine by examining the trash marks left on copies and comparing the marks with copies from a known machine. The fraud examiner should be aware, however, that some of these markings are permanent, while others are transient and temporary.

Permanent "Trash Marks"

Permanent trash marks are uniquely identifiable markings on copies, and they are usually caused by accidental deep scratches and imperfections in the copier's glass surface or document cover, in the printing element surface, or in other machine parts that are not readily replaced or changed during servicing of the machine. These marks can be reproduced on copies until the machine is repaired or the part replaced.

Transient "Trash Marks"

Again, trash marks are uniquely identifiable markings on copies. Transient trash marks are usually caused by dirt, smudges, or small bits of foreign matter on or in machine surfaces that will appear until the machine is cleaned or serviced. These markings can prove not only that a particular machine was used to produce the copy, but that documents that share the same transient trash marks might have been produced at approximately the same time. This is one of several ways to determine when a document was prepared.

Taking Photocopier Samples

There are four steps that fraud examiners should follow when taking photocopier samples. First, make six "blank" copies. As the machine produces each "copy," remove it, turn it over, and initial and number the reverse side of each copy *in the same sequence* it was produced by the machine. These copies will reproduce all trash marks made by the machine, including the entire document cover, glass surface, and internal printing element surface. The fraud examiner should obtain six sample copies because different photocopier models have varying printing element surface sizes, usually ranging in size from one to three sheet impressions before repeating on the same area of the surface).

Second, place a ruler or other calibrated measuring device on the glass document surface, close the cover, and make six copies. (These copies will allow an expert to determine the standard amount of reduction or enlargement the machine makes when in the "actual size" or one-to-one mode.) If the machine requires documents to be fed into it (because it does not have a glass document surface), use any sample document available as an "original" and include that sample document along with the copies of it. On the reverse side of each copy, initial and number it in the same sequence that the copies were produced by the machine, as outlined in the first step.

Third, place a sample document containing both typewritten and handwritten text on the glass document surface in the standard position, close the document cover, and again print six copies, initialing and numbering as previously directed. Also, include the sample document with the copy samples.

Finally, place all of the sample copies and sample documents into a large sturdy paper or cardboard envelope or folder (do not use a plastic envelope). But before placing the documents in the envelope, note the make, model, and location of the machine. Initial, date, and seal the envelope, and submit it to the document examiner along with the questioned evidence documents.

Dating a Document

Occasionally, documents are backdated to make them appear as though they were created at an earlier date. More specifically, *backdating* is the process whereby an individual posts a date on a document at a time earlier than the document's actual creation date for purposes of deception.

Sometimes, the question as to whether a document is genuine or a backdated fabrication arises during fraud inquiries. Forensic experts can use a variety of techniques to answer this type of question by examining the suspect documents. The fraud examiner should be alert for these types of analyses, have some knowledge of what can be done with these methods, and understand their limitations.

The "Alibi" Document

Alibi documents suddenly appear "from out of nowhere," and they often appear late in the course of an investigation, inquiry, or trial. They are always favorable to the suspect and refute previously developed information or evidence that is damaging to the suspect. Often, alibi documents are fabricated.

The "Long Lost" Will

The sudden appearance of a new will that post-dates and supersedes all other wills is all too common. Amazingly, these wills often leave large portions of the testator's estate to the person who found them, and typically, only a photocopy of the will can be located. Many of these wills are proven to be fabricated with the cut-and-paste method. The fabricated and forged "Mormon Will" of billionaire Howard Hughes is a prime example of a long lost will, although the Mormon Will did not involve the use of photocopiers.

Valuable Historical and Collectible Documents

The production of phony historical and collectible documents, artworks, and antiques has been a lucrative field for fraud artists for years. Major frauds involving losses of millions of dollars have involved such diverse phony documents. Some examples of frauds involving valuable historical and collectible documents include the fake "Hitler Diaries," counterfeited baseball cards, forged autographs of historical figures and celebrities, fake old treaties with Native American tribes, newly discovered handwritten "rough drafts" of the U.S. Declaration of Independence, counterfeited "first edition" books, and many others.

Anachronisms in Historical Documents

Anachronisms are items located at a time when they could not have existed or occurred. Generally, exposing anachronisms in fraudulent historical documents requires the expertise of investigators, historical experts, scientific laboratories, and forensic document examiners. For example, accurate handwriting comparisons are rarely possible in the absence of

adequate contemporaneous genuine writings of the purported author. In such cases, the experts will examine the materials used to produce the documents, such as paper, ink, printing, adhesives and seals, bindings, and covers.

Often, to add credibility to forged documents, fraudsters will backdate them. To determine whether contemporary documents were backdated, experts usually rely on diligent investigation and forensic document examiners.

When adequate handwriting or signature samples are available, expert comparisons can expose forgeries. Otherwise, to disprove the purported date of the document, an analysis of the materials might prove that the document did not exist at the time the document was supposedly prepared. Expert examinations of contemporary documentary materials include the following methods:

- To determine the kind of ink and when the ink was first manufactured, experts conduct ink analyses and comparisons with a library of ink standards maintained by the U.S. Secret Service Laboratory in Washington, DC.
- To determine the kind of typewriter that was used and when the typewriter was first manufactured, experts examine the typewriting and compare the typewriting with collections of typewriter reference standards maintained by forensic laboratories.
- To determine who manufactured the paper and when it was first produced, experts examine the paper, especially watermarked paper, and conduct searches of reference materials.
- To determine what kind of machine was used and when those machines were first produced, experts examine photocopies and fax copies and compare them to the reference standards.
- To prove or disprove the date of the questioned copy, experts compare the questioned photocopies with photocopies known to have been produced on a particular machine on a particular date.

Fraud examiners should note that there are currently no methods for accurately determining how long ink, typewriting, and photocopier/printer toner have been on paper.

In some instances, historical and linguistic anachronisms might raise suspicion about a document's validity. A backdated document might contain a historical reference that has not occurred yet (e.g., a receipt listing a tax that had yet to go into effect at the time of the writing). In the case of purportedly older documents, a forger might use anachronistic

words, idioms, or syntax. If a word or phrase seems out of place in a suspected forgery, it might be helpful to use an etymology resource (such as www.etymonline.com).

Indented Writings

Indented writing is the impression a writing instrument leaves on sheets of paper below the piece of paper that contains the original writing. Fraud examiners should be alert for the presence of incriminating indented writings or the absence of logical indentations, both of which can be valuable in proving fraud. In some situations, documents are routinely kept in multiple-page sets, such as in legal forms, multiple-copy invoices, notebooks, tablets, pads, clipboards, and so on. In these situations, the writings on one sheet should correspond to indentations on the following sheet. The absence of corresponding indented writings on the following sheet, or the presence of indented writings on one sheet that do not correspond with the text of the writings on the preceding sheet, could provide proof that pages have been removed or substituted.

Developing Indented Writings

Fraud examiners should never attempt to develop indented writings by shading or scratching on the surface of a sheet of paper with a pencil. Although this method will reveal deep indentations, it will not reveal faint indentations and will prevent expert examinations from analyzing them. Moreover, shading or scratching with a pencil might prevent other types of technical examinations. Likewise, fraud examiners should not apply any sort of liquid to an original document with indented writings, as doing so can damage the document's ability to be analyzed.

Some indented writings can be seen by employing an oblique-lighting method. In this method, the fraud examiner will take the document into an area with subdued overhead lighting, place the document on a flat surface, and shine a bright beam of light—from a small-beam flashlight or small high-intensity lamp—across the document at a low oblique angle or parallel to the surface. Because shadows in the indentations will only show at right angles to the beam of light, it will be necessary to move the light around and note the changing shadows as they form the text of the indentations.

Forensic document experts can perform advanced analysis to reveal messages in indented writings. They can use special lighting, photographic techniques, and sensitive instruments

such as the electrostatic detection apparatus (ESDA) to detect and permanently record extremely faint indented writings that cannot be seen by the oblique-lighting method.

Counterfeit Printed Documents

Many types of documents are counterfeited. Most documents that have monetary value, such as currency, bank checks, traveler's checks, money orders, bearer bonds, postage stamps, gift certificates, or lottery tickets, have all been counterfeited at one time or another. Identity documents (e.g., passports, birth certificates, driver's licenses, and government and commercial employee identity cards) are also often counterfeited. Other counterfeited documents include commercial product labels, business stationery and forms, business logos, motor vehicle titles and registration forms, and safety inspection stickers. Despite most efforts to prevent counterfeiting, almost every type of document with value can be, and probably has been, counterfeited.

Counterfeiting has become big business, especially in some developing countries, where they use the latest high-tech printers to produce large quantities of high-quality counterfeit documents and "knock-off" products in violation of international copyright and trademark laws.

Counterfeiting Methods

The days of old-style counterfeiters—skilled artisans who carefully etched counterfeit printing plates—are over. Today, most counterfeit documents are prepared by various photo-reproduction processes such as the photo-offset printing process (lithography) and flexography, which uses rubberized printing "plates." These processes begin with the photographic reproduction of a genuine document. The photographic negatives are then carefully retouched to remove the filled-in text, serial numbers, and other distinguishing features that appeared on the genuine document. Printing plates are then made from the retouched negatives, and counterfeit copies are printed from the plates.

Rapidly advancing technology now allows individuals with no commercial printing experience to use sophisticated computerized scanners, computer graphics software, multicolor computer printers, and full-color photocopy machines to produce relatively high-quality counterfeit documents.

Detecting Counterfeits

Many counterfeits can be detected by making a side-by-side comparison with a corresponding genuine document. But when conducting a side-by-side comparison, fraud examiners must be alert for different versions or form revisions. Look for subtle differences in ink colors and brilliance, different types of paper substrate, different typestyles and type sizes (fonts), and evidence that the text on the genuine document was retouched for the reproduction. Retouching will be most evident in areas where text, serial numbers, and the like are superimposed on a background design, especially if the documents are printed in black ink.

When furnished with genuine documents for comparisons with suspected counterfeits, forensic document examiners can also identify differences between the printing processes, ink formulations, and paper substrates used. In some instances, experts have been able to reconstruct portions of the filled-in text or serial numbers that appeared on the genuine document, but were removed in the retouching process. If the expert can reconstruct portions of the genuine document's text, he might be able to identify the original document. And if the original document is identified, fraud examiners can trace the history of the document's ownership to identify and locate the counterfeiter. Moreover, if the original document is identified, it might be possible to identify the counterfeiter by obtaining fingerprints from the document.

Fingerprints

There are two basic types of fingerprints: latent and patent. *Latent* (invisible) prints are unique personal identifiers, and these prints are left on surfaces by the body oils, salts, and amino acids clinging to or exuded by friction ridges in the skin on fingers, palms of the hands, and soles of the feet. Latent prints might also be deposited on surfaces by hands, fingers, and bare feet through the transfer of oils and greases. *Patent* (visible) prints are visible to the human eye. They are sometimes deposited on surfaces by hands, fingers, and bare feet through the transfer of materials such as blood, paint, soot, and soil.

Latent prints absorbed into protected porous surfaces, such as paper in files or pages in books, can survive for decades. However, latent fingerprints on hard, nonporous surfaces can be destroyed or start to deteriorate rapidly if handled; not protected from the environment; or exposed to high temperatures, humidity, or water.

To avoid smudging and contamination, fraud examiners should wear protective gloves or carefully use tweezers when handling latent fingerprint evidence. However, tweezers should not be used on documents if indented writing or photocopier examinations are planned.

Fingerprints on Paper or Other Absorbent Porous Surfaces

Fraud examiners should never try to develop latent fingerprints that have been absorbed into paper or other porous materials by dusting with fingerprint powder or any other means. Such efforts will not only be unsuccessful, but they will prevent additional examinations. Instead, fraud examiners should preserve evidentiary documents that contain latent fingerprints by placing them into labeled protective containers, such as sealable, acid-free paper envelopes. Many types of paper and plastic containers can leach acids that damage originals over long periods of storage. While some plastic containers, such as those made of polyethylene or polypropylene, will not leach acid, they might cause harmful condensation to develop on the document. If storing the documents, it is important to consider other environmental hazards, such as potential flooding or insects (silverfish, cockroaches, carpet beetles, etc.) that can cause damage.

Also, fraud examiners should label the item's container with their initials, the current date, where the document was taken from, and an identifying exhibit number (if any).

Experts will use various methods to examine fingerprints on porous surfaces, including iodine fuming and brushing or spraying silver nitrate solution or ninhydrin spray, which reacts with the body chemicals and other substances in the latent prints that have soaked into the absorbent surface. Some of these methods will permanently discolor a document.

Fingerprints on Hard, Nonporous Surfaces

Fingerprints on items with hard, nonporous surfaces, such as plastic, metal, and glass, can be dusted for the presence of latent fingerprints. Special fingerprint dusting powders and lifting materials are available from law enforcement suppliers. The dry, powdered toner used in some photocopy machines has also been used to dust for fingerprints.

After dusting the surface and locating a suspected print or partial print, blow or gently brush off the excess powder. Remove the developed print with adhesive lifting tape and place the tape on an index card that contrasts in color with the dusting powder used. Mark the card

with the fraud examiner's initials, the date, an identifying exhibit number, and where the print was found.

Some latent prints on nonporous surfaces, however, might not be developed by the dusting method. Therefore, if possible, the fraud examiner should retain the item instead of dusting it; place it in a protective container; initial, date, and label the container with an identifying exhibit number; and submit it to a fingerprint expert for processing. Fingerprint experts can obtain fingerprints using various methods. They might use cyanoacrylate (i.e., super-glue) fuming or a laser to successfully develop and photograph the latent prints on some materials, such as black plastic bags.

Fingerprint Comparison Standards

The fingerprints of millions of people are on record in repositories of fingerprint cards maintained by law enforcement agencies throughout the world. These cards contain the inked fingerprints of people for various reasons. For example, they contain the fingerprints of people who have been arrested, served in the military, applied for employment at various levels of government, volunteered their fingerprints to assist in personal identification in the event of their deaths, and so on. Many of these fingerprint databases have been computerized and are linked by networks. However, millions of people have never been fingerprinted.

If a suspect has never been fingerprinted or refuses to furnish inked print samples voluntarily, the fraud examiner might need to obtain a legal court order directing the suspect to furnish inked prints for identification purposes.

If an item of evidence has been handled by several people, it could still bear the guilty party's latent prints. In such cases, the fraud examiner should obtain the inked prints of everyone who might have handled the item.

Sources for Expert Document Examinations

The following are potential sources for expert document examinations:

- Law enforcement laboratories
- Forensic document experts in private practice
- Graphologists

Law Enforcement Laboratories

In cases where criminal prosecutions are likely, there are often forensic laboratories available through law enforcement agencies. However, access to these resources is typically limited and depends on the jurisdiction and the fraud examiner's relationship with the agency.

Forensic Document Experts in Private Practice

When an expert's services are needed, some jurisdictions offer lists of qualified forensic document examiners. For example, in the United States, fraud examiners may contact the American Board of Forensic Document Examiners (www.abfde.org), and in the United Kingdom, fraud examiners may seek assistance from the British Academy of Forensic Sciences (www.bafs.org.uk).

Graphologists (Graphoanalysts)

Graphology (graphoanalysis) has been described as a pseudoscience whose practitioners have the purported ability to determine a person's character, moral traits, personality, and mental state based upon an analysis of that person's handwriting. Graphology is often erroneously confused with forensic document examinations, especially by the media. Fraud examiners should be aware that some people who practice graphological analyses might have little academic and scientific training. They might be self-taught or graduates of a correspondence course. Therefore, fraud examiners should be cautious in relying on handwriting identifications made by some of these "handwriting experts." Also, because a conclusive accuracy level has not been established for graphology examinations, courts and similar administrative bodies often reject expert testimony by graphologists.

INTERVIEW THEORY AND APPLICATION

An *interview* is a question-and-answer session designed to elicit information. It differs from an ordinary conversation in that an interview is structured, not free-form, and is designed for a purpose. An interview might consist of only one question or a series of questions.

Preparation

To effectively prepare for the interview phase of an investigation, the fraud examiner must first develop a plan. The fraud examiner should contemplate what the interview is intended to accomplish and state an objective. He should also review the case file to ensure that it does not contain important information that has been overlooked.

Prior to the commencement of an interview, there should be a clear concept of what information might be gleaned from each of the potential witnesses, as well as the best strategy to go about obtaining it. Generally, the most vulnerable witnesses should be interviewed before the more reluctant witnesses. This will provide the fraud examiner with a broader base of information that can be used to formulate later questions.

When possible, the interview should be held in a venue where the subject will feel comfortable and secure, although it is not recommended that the interview take place in a particularly familiar environment such as the interviewee's home or office. The most appropriate member of the investigative team should be selected to conduct the interview based on the specifics of the interview.

Rather than devise an exhaustive list of questions to ask the subject, the fraud examiner should instead formulate a brief outline of key points to discuss during the interview. Additionally, an investigator should consider which evidentiary documents to bring into the interview, if any, as well as which documents he might seek from the subject.

Characteristics of a Successful Interview

Successful interviews share common characteristics. The interview should be of sufficient length and depth to uncover relevant facts. Most interviewers tend to get too little, rather than too much, information.

A successful interview includes all pertinent information and excludes irrelevant information. From the outset, it should be determined what information is relevant, and that information should be sought. Extraneous or useless facts tend to complicate the gathering and analysis of the information.

The interview should be conducted as closely as possible to the event in question. With the passage of time, the memories of potential witnesses and respondents can become faulty, and critical details can be distorted or forgotten.

Additionally, a good interview is *objective* in scope. Therefore, interviews should be aimed at gathering information in a fair and impartial manner.

Characteristics of an Effective Interviewer

All effective interviewers share certain characteristics. Above all, they are amiable and possess strong interpersonal skills. Successful interviewers are the type of people with whom others are willing to share information. The effective interviewer does not interrupt the respondent with unnecessary questions. In most interviews, pertinent information results from volunteered information, as opposed to responses to a specific question. The effective interviewer displays interest in his subject and in what is being said.

Additionally, effective interviewers demonstrate fairness. The respondent must understand that the interviewer is attempting to obtain only the relevant facts and is not targeting him unfairly. This can best be done by phrasing questions in a nonaccusatory manner.

Also, effective interviewers work informally. Little is accomplished when the interviewer is formal, ostentatious, or attempts to impress the respondent with his authority. Information gathering is best accomplished by approaching the interview in an informal and low-key fashion.

Moreover, an interviewer should lack bias. If the respondent perceives that the interviewer is biased or is attempting to confirm foregone conclusions, the respondent will be less likely to cooperate. Accordingly, the interviewer should make every effort to demonstrate impartiality.

Furthermore, effective interviewers project professionalism. Professionalism in the interview often involves a state of mind and a commitment to excellence. The interviewer should be on time, be professionally attired, and be fair in all dealings with the respondent.

Finally, effective interviewers present no threat. It is vital that the interviewer not appear to be a threat to the interviewee. If people perceive that they are the target of an inquiry, they will be less likely to cooperate.

Legal Considerations When Conducting an Interview

Interviews, and especially admission-seeking interviews, might expose the company and the fraud examiner to certain legal risks. Thus, before engaging in an interview, fraud examiners must understand the ramifications of their actions. This requires an understanding of certain legal issues and how they limit or affect the ways in which an interview might be conducted. However, because employee rights vary from case to case and jurisdiction to jurisdiction, fraud examiners should always consult with counsel regarding the specific laws and regulations for their locality.

Legal Authority to Conduct Interviews

In most instances, legal authority is not required to interview people or to inquire into matters. Most jurisdictions provide citizens the authority to inquire into virtually any subject area, as long as the rights of individuals are not transgressed in the process. Generally, no license is required to conduct interviews; however, if the interviewer represents himself as an investigator, some jurisdictions require a license.

False Imprisonment

False imprisonment is the restraint by one person of the physical liberty of another without consent or legal justification. In the context of employee interviews, a claim of false imprisonment may be made if the interviewer locks the interview room, stands in front of the exit, or refuses to let the suspect leave.

Use of Deception in Interviews

The use of deception to gain information can sometimes be employed legally, but fraud examiners should check with counsel regarding the applicable laws and regulations before engaging in such activity. In cases where deception is legal, the theory is that information can

be obtained by nearly any means, with the exception of force or threats. The interviewer, however, may not employ any deception likely to cause an innocent person to confess. The use of deception is generally not justified regarding promises of leniency or confidentiality, nor is it usually justified to obtain a monetary or business advantage.

Recording Interviews

In some circumstances, recording an interview might be illegal. Some jurisdictions limit an employer's right to record employee interviews during an investigation. In fact, in some jurisdictions, audio recording an interview is permitted only with the consent of all parties to the communication. Thus, fraud examiners should always consult with an attorney when deciding whether to record an interview.

If recording an interview without the respondent's consent is legal, consider recording the interview covertly. Covert recording offers an advantage in that it provides an accurate record without disturbing the flow of the interview. If there is to be a covert recording and the subject asks if the interview is being recorded, do not lie. Explain that it is in the subject's best interest that an accurate recording be made and that he can have a copy when completed.

Elements of Conversations

Since an interview is essentially a structured conversation, it is helpful to understand the basic elements of communications. Whenever two or more human beings are conversing, several types of communication occur—either individually or in combination. Some common types of communication include: expression, persuasion, therapy, ritual, and information exchange.

Expression

A common function of conversation is self-expression. One or more of the conversationalists might need to express ideas, feelings, attitudes, or moods. The urge for spontaneous expression can be a vital asset in interviewing, and it should be encouraged in the respondent. The interviewer can direct the subject's urge for expression toward the information-gathering objectives; however, the interviewer should also take precautions to avoid giving in to his own urges for personal self-expression.

One of the most common errors made by novice interviewers is to yield to the temptation to impress the respondent with their knowledge of the interview subject. In doing so, interviewers run the risk of making the respondent feel threatened, with the resultant tendency for respondents to guard responses rather than express their feelings frankly. Experienced interviewers will have the discipline to control their own responses.

Persuasion

The concepts of persuasion and expression differ in that persuasion is essentially aimed at inducing a belief or action. There are times when persuasion can be used effectively in the interview. Often, the interviewer can use persuasion to convince the subject of the interview's legitimacy.

Therapy

Making people feel good about themselves is often a function of conversation. In an ordinary conversation with a friend, a person often expresses ideas and feelings to remove emotional tension. This release is called *catharsis* and is encouraged, for example, in psychiatric interviews. There are many times when the information sought in an interview is closely related to the respondent's inner conflicts and tensions. For example, in the area of fraud, a person embezzling money from the company will typically feel guilty. A skillful interviewer will know the therapeutic implication of such a feeling when attempting to develop information.

Ritual

Some aspects of conversation are ritualistic; that is, they are merely a form of verbal behavior that has no real significance other than to provide security in interpersonal relations. Examples of rituals include "Good morning!" and "How are you today?" In interviewing, fraud examiners must learn to detect ritualistic answers by the respondent and avoid giving them. The interviewer must be aware of the danger of engaging in ritualistic conversation and then confusing the results with valid information.

Information Exchange

Information exchange is the central purpose of the interview. The word *exchange* reminds us that the flow of information in an interview goes both ways. Too frequently, interviewers become so concerned with the information they wish to obtain that they do not properly

exchange information with the respondent. Although details of what the interviewer says should be carefully measured, fraud examiners should not be cagey because it is a tactic that rarely works.

Two basic problems occur in the exchange of information. First, the information sought by the interviewer is not of equal importance to the respondent. Second, there is often a communication barrier between people of dissimilar backgrounds. These barriers are common between people who do not know one another.

Inhibitors of Communication

To be an effective interviewer, one must understand that certain matters inhibit communication, while others facilitate it. It is the interviewer's task to minimize inhibitors and maximize facilitators. An *inhibitor* is any social-psychological barrier that impedes the flow of relevant information by making the respondent unable or unwilling to provide the information to the interviewer. Eight inhibitors to communication are listed in this section. The first four tend to make the respondent unwilling; the last four make the respondent unable to give the information, even if he is willing.

Competing Demands for Time

The respondent might hesitate to begin an interview because of other time demands. When demands for time are present, the subject does not necessarily place a negative value on being interviewed, but he weighs the value of being interviewed against doing something else. In such circumstances, the interviewer must convince the respondent that the interview is a good use of time.

Ego Threat

In some cases, the respondent might withhold information because of a perceived threat to his self-esteem. There are three broad categories of ego threats: repression, disapproval, and loss of status.

Repression

The strongest ego threat is repression. *Repression* is a defense mechanism that protects an individual from items that would cause anxiety by preventing the items from becoming conscious. Respondents might not only refuse to admit information to the interviewer, they

might also refuse to admit the information inwardly. When this happens, the respondents are being honest when answering that they do not know or that they have forgotten. Embezzlers, for example, might repress memory of their act of embezzlement because it does not conform to their moral code.

Disapproval

A less intense but more common effect of ego threat is found when respondents possess information but are hesitant to admit it because they anticipate disapproval from the interviewer. If respondents are made to feel that the interviewer will not condemn them, they might welcome the opportunity to divulge information. A generally accepting and sympathetic attitude toward the respondent goes far toward eliciting candid responses.

Loss of Status

Sometimes respondents fear losing status if the information provided becomes public. This can sometimes be overcome by the interviewer's assurance that the information will be handled confidentially to the extent possible.

Etiquette

The etiquette barrier operates when an answer to the interviewer's question contains information perceived by the respondent as inappropriate. Answering candidly would be considered in poor taste or evidence of a lack of proper etiquette. For example, there are certain things that men do not discuss in front of women and vice versa, things that students do not tell teachers, and things that doctors do not tell patients. The desire to avoid embarrassing, shocking, or threatening answers is distinct from the fear of exposing oneself. Often, the negative effects of the etiquette barrier might be forestalled by selecting the appropriate interviewer and setting for the interview.

Trauma

Trauma denotes an acutely unpleasant feeling associated with crisis experiences. The unpleasant feeling is often brought to the surface when the respondent is reporting the traumatic experience. Trauma is common when talking to victims, but it can usually be overcome by sensitive handling of the issue.

Forgetfulness

A frequent inhibitor to communication is the respondent's inability to recall certain types of information. This is not a problem if the objectives of the interview deal only with current attitudes, beliefs, or expectations. The natural fading of the memory over time makes it easier for the ego-defense system to reconstruct one's own image of the past by omission, addition, or distortion.

The memory problem is a much more frequent obstacle than most interviewers expect. Even some of the most simple and obvious facts cannot be elicited because of the respondent's memory problems.

There are three factors that contribute to recollection of an event. First, the vividness of the person's recall is related to the event's original emotional impact, its meaningfulness at the time, and the degree to which the person's ego is involved. Second, the amount of time that has elapsed since the event contributes to the recollection of an event. Third, the nature of the interview situation, including the interviewer's techniques and tactics, also contributes to the recollection of an event.

Knowledge of these factors will help the interviewer anticipate problems that might occur. And there are certain techniques, discussed later, that will help the interviewer overcome many of these memory problems.

Chronological Confusion

Chronological confusion refers to the respondent's tendency to confuse the order of experiences, and it commonly occurs in interviews seeking case history information. Chronological confusion can occur in two ways:

- Two or more events are correctly recalled, but the respondent is unsure of the sequence.
- Only one event is recalled, and it is incorrectly assumed to have been true at an earlier point.

Inferential Confusion

Inferential confusion denotes confusion and inaccuracies resulting from errors of inference. These errors generally fall into two categories: induction or deduction. *Induction* occurs when the respondent is asked to convert concrete experiences into a higher level of generalization.

Deduction occurs when the respondent is asked to give concrete examples of certain categories of experience.

Unconscious Behavior

Often, the interview process reveals information about a person's unconscious behavior. There are three types of unconscious behavior: customs or habits, circular reactions, and reactions to acute emotional crises. A *custom* or *habit* is a settled tendency or usual pattern of behavior; it is the behavior that an individual engages in regularly. A *circular reaction* is the immediate, unwitting response of one person to the subliminal, nonverbal clues of another. A response to an *acute emotional crisis* does not follow a habitual pattern or result from a reaction to others; it arises only in special circumstances when the interviewee is experiencing an emotional dilemma.

Facilitators of Communication

Facilitators of communication are those social-psychological forces that make conversations, including interviews, easier to accomplish. These facilitators require a basic understanding of what motivates people.

Fulfilling Expectations

One of the important forces in social interaction is the tendency of one person to communicate, verbally or nonverbally, his expectations to the other person. The second person then tends to respond, consciously or unconsciously, to those expectations. This might be viewed as one manifestation of the more general human tendency to conform to the group and to the anticipations of higher-status people. It is in this conformity to group norms that security is sought.

In the interview setting, the interviewer communicates expectations to the respondent. The interviewer should be able to transmit both a general expectation of cooperation and a more specific expectation that the respondent will answer the questions truthfully. The interviewer must clearly distinguish between asking for information and expecting it. The former is mainly achieved with verbal communication, while the latter is accomplished through nonverbal behavior. The interviewer who expects the respondent to cooperate will likely be more successful than one who only asks questions.

Recognition

All human beings need the recognition and the esteem of others. Social interaction often depends on an exchange of social goods. People will "perform" in exchange for recognition and other social rewards. The need for recognition can be fulfilled by attention from people outside the individual's social circle. The skillful and insightful interviewer takes advantage of every opportunity to give the respondent *sincere* recognition.

Altruistic Appeals

There seems to be a need for humans to identify with some higher value or cause beyond immediate self-interest. This might sometimes take the form of identification with the objectives of a larger group. Altruistic deeds usually increase self-esteem, whether or not the deeds have been made public. This distinguishes altruism from publicity. Altruism is of major importance in motivating many respondents. Interviewers who understand the respondent's value system can use strategy and techniques that appeal to altruism.

Sympathetic Understanding

Human beings need the sympathetic response of others. They like to share their joys, fears, successes, and failures. This need for understanding differs from the need for recognition that requires success and increased status. Interviewers who reflect a sympathetic attitude and who know how to direct that attitude toward the interview's objectives will find that their interviews will be more successful than those who do not.

New Experience

People welcome new experiences. Sometimes the respondent is motivated by curiosity regarding the interviewer. Interviewers should consider this when deciding what to say about themselves. One must not assume that just because an interview is a new experience, it will satisfy the respondent's needs. Aspects of the respondent's perception of the new experience can be ego threatening. The respondent might be anxious about the impression left with the interviewer. This apprehensiveness can often be detected by the interviewer at the beginning of the contact. Once these fears are dispelled, the respondent frequently finds the interview to be a new and interesting experience.

Catharsis

Catharsis is the process by which a person obtains a release from unpleasant emotional tensions by talking about the source of these tensions. We often feel better by talking about

something that upsets us. Although we are all familiar with the frequent necessity for catharsis in ourselves, we do not always perceive the same need in others. The need for sympathetic understanding and the need for catharsis are related, but they are not the same thing. The interviewer who does not have time to listen to what he considers inconsequential or egocentric talk will often find the respondent unwilling to share important consequences.

Need for Meaning

Another general trait common to people is the need for meaning. Every society has a set of assumptions, values, explanations, and myths lending order to it. The concept of need for meaning is related to *cognitive dissonance* (i.e., an uncomfortable emotional state caused by holding conflicting ideas simultaneously). Psychological tension is created when an individual becomes aware of incongruence of facts, assumptions, and interpretations. This tension is painful, and its reduction is rewarding to the individual. In cases where the interview topic deals directly with the sources disturbing a person's system of meaning, there is a strong motivation for the respondent to talk it through if he is convinced of the interviewer's interest.

Extrinsic Rewards

Extrinsic rewards are rewards the interviewee receives that are not directly related to the interview experience, and they cause the respondent to see the interview as a means to an end. Extrinsic rewards for interviewees can include money, job advancement, and retention of privileges. What is irrelevant to the interviewer might be relevant to the respondent. A sensitive interviewer will be able to recognize what extrinsic rewards the respondent receives, if any, from being interviewed.

Kinesic Interview and Interrogation

In recent years, the kinesic interview or interrogation has become more popular among those in the law enforcement community. The methods used in kinesic interviews are different than those used in traditional interviews. In kinesic interviews, the interviewer is not necessarily looking for a confession from the subject. Instead, the interviewer is attempting to assess whether the subject is telling the truth by reading his body language and other physical manifestations of deception.

In the book *The Kinesic Interview Technique*, authors Frederick C. Link and D. Glenn Foster define the kinesic interview technique as:

> *[An interview technique] used for gaining information from an individual who is not willingly or intentionally disclosing it.*

Link and Foster believe that the kinesic interview is based entirely on the concept of stress—an event or circumstance that forces an individual's mind or body out of psychological equilibrium. When stress occurs, humans, like any other living creature, have an emotional reaction. Link and Foster refer to this as the "fight or flight syndrome," in which we either run from a stressful situation or brace to face it. Either way, they hypothesize, our animalistic tendencies dictate that we must react to stress. When this concept is applied to the interview situation, the kinesic interview technique is applied to attempt to read the interview subject's reaction to stress.

The kinesic method relies, in a broad sense, on the interviewer's ability to observe the subject for signs or symptoms of deceit. The kinesic interview is conducted not just to observe what the subject says, but also how the subject says it; the subject's gestures, posturing, facial expressions, and voice inflection are just a few of the traits that an investigator looks at. This style of interviewing assumes that when most human beings lie or are deceitful to others, they will reveal this deceit through their body language.

An individual's reactions to stress are generally subconscious; in most cases, the interviewee does not even realize that he is acting noticeably different. The actions or signs that an interviewer is looking for are called *meaningful behavior*—activities that might suggest that an interviewee is under stress.

Link and Foster identify three distinct categories into which meaningful behavior can be divided:

- Self-initiated verbal statements that the interviewee initiates without prompting
- Prompted verbal responses or statements made by the interviewee in response to structured questions asked by the interviewer
- Nonverbal behavior or body language, which includes body positioning movements, lack of movement, and observable physiological changes

Self-Initiated Verbal Statements

Interviewees make self-initiated verbal statements without any prompting by the interviewer. Examples of these statements include changes in speech pattern, overly respectful or friendly words directed at the interviewer, or indirect answers and statements. The subject's speech tempo will tend to increase, or the subject will hesitate or stammer frequently before giving any responses. These verbal clues are a subconscious attempt by the interviewee to dodge the line of questioning or suppress his guilty feelings.

Generally, a dishonest person is much more likely to give more self-initiated verbal signs than a person who is telling the truth.

Prompted Verbal Responses

Prompted verbal responses can help an interrogator to differentiate an honest person from a deceitful one. By using a series of structured questions, interviewers can generally get a good indication of how truthful the subject is. These responses should be woven into a casual conversation so that the subject is not aware of the significance of the structured questions. Also, structured questions must not appear to be interrogational in manner.

Structured Questions

The fraud examiner has several types of loaded questions he can use to help determine the interviewee's guilt or innocence.

- *Punishment question*: The interviewer will casually discuss the punishment of the crime with the subject, asking, for example, "What do you think should happen to the criminal?" When posed with this sort of question, the innocent person, having nothing invested in the crime, will generally answer that the criminal should be severely punished, saying something like, "Lock him up and throw away the key." However, if guilty of the crime, the interview subject will generally answer that the criminal should be treated fairly, saying for example, "The person who stole that money is very sick and probably needs mental help." In essence, the guilty person is more likely to answer "Don't hurt me."
- *Physical evidence question*: This type of question is meant to jar the suspect into making a mistake. The interviewer will suggest that there is a piece of evidence that might link the interviewee to a crime, asking, "Is there any reason that your fingerprints might have been found near the crime scene?" This question does not assert that there is any evidence. The innocent person, knowing that he had nothing to do with the crime, will simply answer "no," unconcerned about the possible evidence. The guilty party will often become concerned with this possible evidence and attempt to cover for it with

another lie. However, interviewers should be circumspect when employing this tactic. For example, if the subject is guilty, but wore gloves while committing the crime, a question implying that his fingerprints were found at the crime scene might inadvertently undermine the remainder of the interview by informing the subject as to how little the interviewer actually knows about the methods used to perpetrate the fraud.

- *Crime existence question*: A variation on this question would be "Do you think that this crime was even committed?" The guilty party will see this as a possible way out and answer "no," while the innocent person will likely answer "yes."

Nonverbal Behavior/Body Language

The evaluation of an interview subject's body language can provide the fraud examiner with numerous insights into the subject's true intentions. Quite often, while an interviewee says one thing, his body language tells a different story. The first step in this process is to evaluate the subject's "normal" body language. While there are some general tendencies that suggest that a subject is being less than truthful, the interviewer must first evaluate the subject's natural tendencies. For example, some people use their hands a lot when speaking, while others do not.

For most people, the head is the most expressive portion of the body. The interviewer can read several facial traits or expressions, including:

- *Eyes*: Breaks in eye contact can indicate deception. To break eye contact, the subject might close his eyes, cover his eyes, or turn or lower his head. While any of these breaks in eye contact can suggest a subject's deceit, the interviewer must remain keenly aware that what is considered an appropriate amount of eye contact differs greatly among various cultures. In some cultures, direct or prolonged eye contact is purposefully avoided because it can be interpreted as disrespectful or threatening.
- *Eyebrow movement*: When a subject uses his eyebrows to display disbelief or concern, the display is often a deceptive reaction to the interviewer's questioning.
- *Touching the face*: Many subjects, when under stress, repeatedly touch the tip of their nose or rub their chin. These movements are often nervous reactions to threatening situation.
- *Blushing*: A person whose face or cheeks become red is generally experiencing increased blood pressure, indicating pressure or stress.
- *Adam's apple*: Often, the subject's larynx will move up and down when he is concerned or nervous.
- *Carotid arteries*: Often, the veins in a person's neck will become exposed when he becomes nervous.

In addition, many interviewees will attempt to cover or defend themselves by crossing their arms or their legs. Generally, such movements are defensive postures.

The following factors should be considered when applying kinesic techniques:

- No single behavior, by itself, proves anything.
- Behaviors must be relatively consistent when the stimuli are repeated.
- The interviewer must establish what is normal or baseline behavior for each subject and then look for changes from the baseline. These observed changes in the subject's baseline behavior are diagnosed in clusters, not individually.
- Behaviors must be timely.
- Observing and interpreting behavior is hard work.
- The subjects will watch the interviewers while the interviewers watch them.
- Kinesic interviewing is not as reliable with some groups.

The Cognitive Interview Technique

Police and fraud investigators must often rely on the testimony of witnesses to bring the facts of a case together. The testimony of an important witness can determine the entire outcome of a fraud case, so it is essential that witnesses' words be as reliable and detailed as possible.

Unfortunately, witnesses are human, and humans are prone to make errors. Fraud investigators must understand that in a time of crisis, or even in a situation in which the witness was simply not paying close attention, the eyewitness can easily miss acute details. Often, witnesses have trouble recalling large portions of events because they did not know at the time that they should have been looking for specific details. Dr. R. Edward Geiselman and Dr. Ronald P. Fisher write in the National Institute of Justice article "Interviewing Victims and Witnesses of Crime" that "most victims and eyewitnesses . . . are so occupied with the event that they do not have the time to try to learn or memorize details about a suspect at the time of the crime."

Because of these problems, different techniques for filling out the witnesses' testimony have been developed to assist the investigator. One of the first techniques developed was the use of hypnosis on witnesses. The notion behind this approach was that an investigator could open the mind of a witness and pick into his subconscious for specific details. The merits of this technique are highly debatable and have been contested in courts of law.

But more recently, the cognitive interview technique was developed to serve much the same purpose. This approach has proven far more effective than questionable hypnosis techniques and has been deemed a reliable method in the court of law.

The cognitive interview technique was established, researched, and fine-tuned by Dr. Geiselman, a professor at the University of California, Los Angeles, and other professionals in the psychiatric profession. Geiselman and others have written numerous articles and governmental documents detailing the extensive research dealing with interviewing witnesses.

Geiselman believes that the cognitive interview should be split into two distinct phases: the narrative phase and the specific-detail phase. The narrative phase deals more with "what happened" during the event; the specific-detail phase seeks to track down who was involved and obtain specific details about the suspect. When the fraud examiner uses these phases in succession during an interview, it is likely that he will come away from the interview with an excellent witness account of an event.

The Narrative Phase

The first portion of the cognitive interview is the narrative phase, in which the witness tells the "whole story." The investigator should first allow the witness to recount the situation, using several steps to guide the narrative portion. There are four primary steps in the narrative phase:

1. Reconstruct the circumstances of the event.
2. Instruct the witness to report everything and be complete.
3. Recall the events in different orders.
4. Change perspectives.

Reconstruct the Circumstances of the Event

In this first, important step, the interviewer should ask the witness to describe the context in which the incident occurred. The interviewer should ask the witness to describe everything, including the weather, time of day, and the look and feel of the environment in which the incident took place. What did the people and/or objects in the surroundings look like?

The objective of this step is to mentally return the witness to the scene so that he will vividly recall the unfolding events. Asking the witness to describe the emotional state he was in at the time of the occurrence often helps accomplish this first step.

Instruct the Eyewitness to Report Everything and Be Complete

In this stage, the interviewer should ask the eyewitness to recount every last detail as completely as possible. Geiselman says that a witness will often withhold information that he thinks might be relevant to the investigation. Therefore, the investigator should instruct the witness not to omit anything when giving his statement, no matter how trivial the information might seem. The small details that the witness remembers during the interview might not be directly beneficial to the investigation, but they will be important in helping the witness remember the events descriptively and thoroughly.

Recall the Events in Different Orders

Constructing the event in a different order will give the witness the freedom to recreate the event completely. When recounting the event in sequential order, the witness could very well forget minute details in an effort to describe what happened next. If the witness constructs the event from the single moment or thing that left the greatest impression on him, the interviewer might gain a foothold on the witness's perspective.

Change Perspective

The final step of the cognitive interview process is to get the witness to alter his perspective of the event. The investigator should ask him to reconstruct the scenario and assume a different position within the situation. For instance, ask the witness to pretend to be a different person within the event, and recount the event from that perspective. What was the other person thinking or feeling? This technique might seem a bit odd, but it might allow the witness to consider various elements of the event that he previously had not.

Specific Details

Once the narrative portion of the interview is completed, it is likely that the investigator will have questions about specific details. Geiselman and his contemporaries have developed five techniques to cultivate specific details and items of information from the witness. The five categories are:

- Physical appearance
- Names

- Numbers
- Speech characteristics
- Conversation

Physical Appearance

The investigator can often elicit additional information about the event by asking the witness to describe the suspect. A particularly effective technique is to ask the witness whether the suspect reminded the witness of anyone he knows. Often, physical descriptions, such as the type of clothing a suspect was wearing or the particular way a suspect walked or looked, will not be presented during the narrative phase of the interview. This additional information, however, can be key to linking a suspect with a specific crime.

Names

Often, the name of the suspect or another person will be spoken during an event, but many times the event proves too traumatic or happens too quickly for a witness to recall. If a witness cannot remember any names spoken during the event, ask him to attempt to recall the first letter of the suspect's name (or any other names spoken) by going through the alphabet one letter at a time.

Numbers

Once the witness has possibly established the first letter of the suspect's name, the investigator should ask the witness how many syllables or letters were in the name. Establishing whether the name was long or short might effectively jar the witness's memory.

Speech Characteristics

The investigator can also ask the witness what types of speech characteristics the suspect has. Geiselman suggests asking the witness whether the suspect's speech reminds the witness of anyone else. The interviewer should also determine whether the suspect had any specific accent, an awkward or unusual voice, or used any words repeatedly during the event.

Conversation

The witness should be asked whether anything that the suspect or anyone else said during the event elicited an unusual response. Did the suspect or any other witnesses react in a strange manner to anything that was said?

The extensive research that Geiselman and his colleagues have done on the cognitive interview technique has shown that the technique improves the recall performance of witnesses when compared to standard interview techniques. The cognitive technique places emphasis on the witness's recollection of details to give investigators a more complete picture of what actually happened during a specific event.

Interview Mechanics

As with all other phases of a fraud examination, an interview will be most successful if the investigator is thoroughly prepared, which requires that the interviewer understands the mechanics of interviewing.

Note-Taking

The interviewer will frequently need to take notes during the interview. Interviews without notes are limited in value because they leave the results of the interview open to interpretation or dispute.

When taking notes, fraud examiners should follow a few basic rules. First, start each interview on a separate sheet of paper. This can be especially helpful if documents from a particular interview are subpoenaed.

Take accurate, but not necessarily verbatim, notes during the interview. Do not try to write down all the information you are given during an interview, only the pertinent facts. Taking too many notes will make the interview process cumbersome, and it might inhibit the respondent. If, however, a quote is particularly relevant, try to write it down verbatim. Enclose all direct quotes in quotation marks.

Do not slow down the interview process for note-taking. Instead, write down key words or phrases, and then go back over the details at the end of the interview. In general, it is better to err on the side of taking too few notes rather than too many.

An investigator might choose to use electronic note-taking, which typically entails recording the interview and then summarizing the recording. This allows the investigator to conduct the interview without disrupting the flow of the conversation to take notes. Additionally, recording the interview prevents the subject from observing which points the investigator

finds most significant. It is important to keep in mind that an electronic recording device can distract the subject and inhibit his responses. Additionally, as laws regarding the use of recording devices vary by jurisdiction, an investigator should ensure that his use of electronic note-taking is acceptable.

Maintain Eye Contact

The interviewer should maintain eye contact with the respondent as much as possible while taking notes. Eye contact personalizes all human communication, and it creates a more comfortable environment and facilitates the flow of information during the interview process. However, it is important to recognize that direct or prolonged eye contact is not customary in many cultures, including parts of Latin America, the Middle East, Africa, and East Asia. For example, if interviewing a Japanese man, sustained eye contact might be construed as disrespectful or as a challenge.

Opinions

Avoid making notes regarding your overall opinions or impressions of a witness. Such notes can cause problems with credibility if they are later produced in court.

Do Not Telegraph Emotions

Avoid showing excitement or other emotions when taking notes. During interviews of targets and adverse witnesses, take notes in a manner that does not indicate the significance of the information; that is, never allow note-taking to "telegraph" your emotions.

Writing Down Questions

Whenever possible, do not prepare a list of predetermined questions to ask the subject. The interview should flow freely. The interviewer might, however, want to develop a list of key points to cover during the interview.

Also, do not provide the subject with a list of predetermined questions. Allowing the respondent to read a written list of questions can give him an opportunity to fabricate his answer.

Documenting Results

Expound on the interview notes as soon as possible after concluding the interview—preferably immediately afterward. If this procedure is followed, the fraud examiner will not have to take copious notes during the interview.

Do Not Interview More Than One Person

One of the basic rules is to question only one person at a time. The testimony of one respondent will invariably influence the testimony of another. There are few absolute rules of interviewing, but this is one of them.

Privacy

Another basic rule is to conduct interviews under conditions of privacy. The interview is best conducted out of the sight and sound of friends, relatives, or fellow employees. People are very reluctant to furnish information within the hearing of others.

Question Typology

When conducting an interview, there are five general types of questions an interviewer can ask: introductory, informational, assessment, closing, and admission-seeking.

Because fraud examinations move in a linear order, starting with the general and working to the specific, the first interviews should be with those individuals who are least likely to be involved, working toward those individuals who are more likely to be involved. The first interviews are conducted for the purpose of gathering information; therefore, they should be nonconfrontational, nonthreatening, and should encourage open communication. In these routine interview situations, only three of the five types of questions will normally be asked: introductory, informational, and closing questions. If the interviewer has reasonable cause to believe the respondent is not being truthful, he can ask assessment questions. And finally, if the interviewer decides with reasonable cause that the respondent is responsible for misdeeds, he can pose admission-seeking questions.

Introductory Questions

Introductory questions are designed to meet four objectives: to provide an introduction, to establish rapport, to get the respondent to agree verbally to cooperate in the interview (i.e., establish the interview theme), and to observe the respondent's reactions to questions.

Informational Questions

Once the proper format for the interview is set, the interviewer then turns to the fact-gathering portion. Informational questions should be nonconfrontational and nonthreatening, and they should be asked for the purpose of gathering unbiased factual information.

Typically, the interviewer will ask three types of questions during the fact-gathering portion of an interview: open, closed, and leading. These question types are discussed in more detail below. Each type is used in a logical sequence to maximize the development of information. If the interviewer has reason to believe that the respondent is being untruthful, he can pose assessment questions. Otherwise, he should bring the interview to a logical close.

Closing Questions

Closing questions seek to close the interview positively. In routine interviews, closing questions serve the following purposes: reconfirm facts, gather additional facts, and conclude the interview in a manner that maintains goodwill.

Assessment Questions

If the interviewer has reason to believe the respondent is being deceptive, he should begin asking assessment questions. These are questions specifically designed to establish the respondent's credibility. When assessing credibility, the interviewer must observe the subject's verbal and nonverbal responses. By observing the respondent's verbal and nonverbal responses to these questions, the interviewer can assess the respondent's credibility with some degree of accuracy. That assessment will form the basis of the interviewer's decision about whether to pose admission-seeking questions and seek a legal admission of wrongdoing.

Admission-Seeking Questions

Again, admission-seeking questions are designed to obtain a legal admission of wrongdoing. The choice of when to conduct an admission-seeking interview of a suspect is critical. Admission-seeking interviews are reserved specifically for individuals whose culpability is reasonably certain. They should take place only when all other reasonable investigative steps have been completed and as much information as possible has been developed from other sources. In addition, the interviewer should be able to reasonably control the interview's place, time, and subject matter.

Admission-seeking questions serve at least three purposes: (1) to clear an innocent person, (2) to encourage the culpable person to confess, and (3) to convince the confessor to sign a written statement acknowledging the facts. But the interviewer must be careful to pose these questions in a way that does not violate the rights and privileges of the subject.

Introductory Questions

One of the most difficult aspects of an interview is getting started. Indeed, the introduction might be the hardest part. In many instances, the interviewer and the respondent have not met before. The interviewer has a tall order: meet the person, state a reason for the interview, establish necessary rapport, and get the information.

The introduction is accomplished through questions as opposed to statements. The questions allow the interviewer to assess feedback from the respondent. This is an important aspect of the introduction. If the respondent is reluctant to be interviewed, that fact will come out through the introductory questions.

Four Objectives

Introductory questions are designed to meet the following four objectives.

Provide the Introduction

The interviewer must introduce himself before the interview commences. The interviewer generally should indicate his name and company, but he should avoid stating his title. In general, the more informal the interview, the more relaxed the respondent.

In some instances, the interviewer cannot avoid giving his title, and in such cases, the interviewer should use a title that will not conjure up emotions or possible fear in the respondent's mind.

Establish Rapport

Introductory questions should be designed to establish rapport. Merriam-Webster's Dictionary defines *rapport* as a "relation marked by harmony, conformity, accord, or affinity." In other words, the interviewer must establish some common ground with the respondent before he begins the fact-gathering portion of the interview. Interviewers usually establish rapport by spending a few minutes engaging the respondent in casual conversation. This

aspect, however, should not be overdone, as most people are aware that the interviewer is there for a meaningful purpose.

Establish the Interview Theme

The interviewer must state the interview's purpose in some way prior to the commencement of serious questioning. Otherwise, the respondent might be confused, threatened, or overly cautious. Stating the purpose of the interview is known as establishing the interview theme.

Additionally, the purpose of the interview should be general and not specific. The specific interview purpose will be conveyed to the respondent later. The stated purpose of the interview should be one that is logical for the respondent to accept and easy for the interviewer to explain, but it might be related only indirectly to the actual purpose of the interview. Normally, the more general the theme, the better.

EXAMPLE

Interviewer:

"I am working on a matter and I need your help."

OR

"I am doing a review of procedures here at the company."

OR

"I am developing some information on our purchasing procedures."

The goal of the theme is to get the respondent to make a commitment to assist. Failure to get a commitment to assist from the respondent is one of the common mistakes interviewers make. Obtaining a commitment to assist is a critical step in setting the tone for the interview. A commitment of assistance requires positive action on the part of the person being interviewed. Remaining silent or simply nodding the head in response to a request for assistance is generally not sufficient.

The interviewer should ask for the commitment before the interview commences, and he should encourage the respondent to voice that commitment aloud. If the interviewer makes a request for assistance and the respondent remains silent, the interviewer should repeat the question in a slightly different way until the respondent verbalizes commitment. In the following example, Hayden Barlow, the Certified Fraud Examiner, introduces himself to Emma Martin, who works in the purchasing department of Westbrook Furnishings Incorporated, and obtains a commitment to assist from Martin.

EXAMPLE

Interviewer:

"Ms. Martin, I'm Hayden Barlow. I'm doing a review of our purchasing function. Do you have a few minutes?"

Respondent:

"Yes."

Interviewer:

"I am gathering some information on certain company procedures. Maybe you can help me?"

Respondent:

No response.

Interviewer:

"Could I get you to help me, if you can?"

Respondent:

"Yes. What's this about?"

Generally, the most effective interview theme is that help is being sought. Nearly all human beings get satisfaction from helping others. Thus, in most interviews, the interviewer should approach the respondent so that he does not feel threatened in any way and is made to feel important in helping out.

In the following examples, the interviewer is introducing himself to a fellow employee.

EXAMPLE

WRONG:

Interviewer:

"Ms. Martin, I am Hayden Barlow, a Certified Fraud Examiner with Westbrook Furnishing's fraud examination unit. I am investigating a case of suspected fraud, and you might know something about it. How long have you worked here at the company?"

RIGHT:

Interviewer:

"Ms. Martin, I am Hayden Barlow. I work here at the company. Have we met before?"

Respondent:

"I don't think so."

Interviewer:

"I am working on an assignment and I need your help. Do you have a few minutes I can spend with you?"

Observe Reactions

The interviewer must be skilled in interpreting the respondent's reactions to questions. Social scientists say that more than half of the communication between individuals is unspoken. The interviewer must, therefore, observe systematically, though in a nondescript manner, the various responses the respondent gives during the course of the conversation.

To observe the respondent's reactions, the fraud examiner should move from comfortable to sensitive questions. That is, the interview process should begin by posing comfortable questions while establishing rapport. Asking comfortable questions will help the interviewer find some common ground on which to connect with the respondent.

Sensitive questions should be avoided until well into the interview. Even then, such questions should be asked only after careful deliberation and planning. Moreover, all questions should be non-accusatory. Nothing closes up the lines of communication in an interview like an accusatory question. If the respondent starts to become uncomfortable with the questioning, the interviewer should move into a different area and approach the sensitive question later from a different vantage point.

Likewise, interviewers are encouraged to formulate their questions in a way that will not bring about a strong emotional reaction from the respondent, and emotive words of all types should be avoided during the introductory phase. Such words put people on the defensive, making them more reluctant to answer and cooperate.

EXAMPLE

Instead of:	**Use:**
Investigation	*Inquiry*
Audit	*Review*
Interview	*Ask a few questions*
Embezzle/steal/theft	*Shortage or paperwork problems*

Furthermore, some people will not volunteer information; they must be asked. The interviewer must not be reluctant to ask sensitive questions after the proper basis has been established. If the interviewer poses the question with confidence and with the attitude that an answer is expected, the respondent will be much more likely to furnish the requested information. If the interviewer is apologetic or lacks confidence in the question, the respondent is much less likely to answer.

Again, after the interviewer establishes rapport through normal conversation, he must observe the respondent's reactions. This will serve as a baseline for observing behavior when questions that are more sensitive are asked. If the respondent's verbal and nonverbal behaviors are inconsistent from one type of question to another, the interviewer should attempt to determine why.

To determine why the respondent's behaviors are inconsistent, the interviewer must be knowledgeable about nonverbal clues of behavior, which generally fall within one of the following categories: proxemics, chronemics, kinetics, or paralinguistics.

PROXEMICS

Proxemic communication is the use of interpersonal space to convey meaning. The relationship between the interviewer and respondent is both a cause and effect of proxemic behavior. If the distance between the interviewer and the respondent is great, there is more of a tendency for them to watch each other's eyes for clues to meaning.

It is important to position the respondent's chair and the interviewer's chair at an acceptable distance. The correct conversational distance varies from one culture to another. In the Middle East, the distance is quite short; in Latin America, equals of the same sex carry on a conversation at a much closer distance than in North America. Often, as the subject matter

of the interview changes, the interviewer can note the changes in the respondent's proxemic behavior. If the person is free to back away, he might do so when the topic becomes unpleasant or sensitive.

CHRONEMICS

Chronemic communication refers to the use of time in interpersonal relationships to convey meaning, attitudes, and desires. If the respondent is late in keeping an appointment, for example, this might convey a lack of interest in the interview or an attempt to avoid the interview.

The most important chronemic technique used by interviewers is in the timing of questions. The interviewer can control the length of pauses and the rate of his speech. This is called *pacing*. The interviewer can also control the length of time after the respondent has finished a sentence before another question is posed. This is called the *silent probe*.

Pacing is one of the principal nonverbal methods of setting an appropriate mood. The tense interviewer often communicates anxiety by a rapid-fire rate of speech, which, in turn, might increase anxiety in the respondent. To establish a more thoughtful, deliberative mood usually needed to stimulate free association, the interviewer must take the initiative in setting a more relaxed, deliberate pace.

KINETICS

As previously mentioned, *kinetic communication* involves the use of body movement to convey meaning. Even though posture, hands, and feet all communicate, interviewers tend to focus attention on the face, and interviewers are more accurate in their judgments of others if they can see facial movements and expressions. When the interviewer concentrates on facial expressions, the primary interest is eye contact. Eye contact primarily communicates the desire to make or avoid communication. A person who feels shame normally will drop the eyes to avoid the glance of another. This is not only to avoid seeing disapproval, but to conceal personal shame and confusion.

PARALINGUISTICS

Paralinguistic communication involves the use of volume, pitch, and voice quality to convey meaning. One of the basic differences between written and verbal communication is that oral speech gives the full range of nonverbal accompaniment. For example, a "yes" response might not mean complete agreement; it depends on the way in which the "yes" is said.

The interviewer must learn to listen and observe changes in the nonverbal accompaniment and whether the verbal and nonverbal are harmoniously reinforcing or tend to give conflicting signals, as in cases where the respondent is trying to deceive the interviewer. Ten emotions have been studied by social scientists: anger, fear, happiness, jealousy, love, nervousness, pride, sadness, satisfaction, and sympathy. Some emotions, like anger and nervousness, can be more reliably identified than the others.

Methodology

Respondents must perceive that they have something in common with the interviewer and should feel good about the situation. This is best accomplished when respondents perceive the interviewer as being open and friendly. The following techniques promote this perception: make physical contact, establish a transitional statement, seek continual agreement, and avoid invading personal space.

Physical Contact

Make physical contact with the person being interviewed by shaking hands. Making physical contact helps break down psychological barriers to communication. The interviewer should not invade the respondent's personal space, however, as this might make the person uncomfortable.

The interviewer uses body language to create the impression of trust during the interview by gesturing openly with the arms, clasping hands together, and leaning forward in a manner to indicate interest. Rapport can be established through verbal techniques, such as using soft words, agreeing with the respondent, and avoiding negative terms.

Establish a Transitional Statement

Once the interviewer has a commitment for assistance, he must describe the purpose of the interview in more detail. This is done with a transitional statement, which is used to provide a legitimate basis for the inquiry and to explain to respondents how they fit into the inquiry. The interviewer usually can provide such information with a broad description. When interviewing employees in the same company, most of them already presume the legitimacy of the interviewer's request for assistance.

After describing the basic nature of the inquiry with the transitional statement, the interviewer should seek a second commitment for assistance.

EXAMPLE

Interviewer:

"It's pretty routine, really. I'm gathering some information about the purchasing function and how it is supposed to work. It would be helpful to me if I could start by asking you to tell me about your job. Okay?"

When interviewing strangers, the interviewer might have to provide more particularity when describing how the respondent's assistance is needed. This can be accomplished by one or more of the following methods. In the example below, the interviewer is talking to an outside vendor.

EXAMPLE

Interviewer:

"It's pretty routine, really. As I say, I work for Westbrook Furnishings and I've been assigned a project to gather some information about some of our procedures. And because you work for one of our vendors, I thought it might be helpful to talk to you. Okay?"

OR

"It's pretty routine, really. I have been asked by the company to gather information on some of our procedures. I thought you might be able to help by answering a few questions. Okay?"

OR

"It's pretty routine, really. I have been asked by the company to gather some information, and they suggested I might contact you. Okay?"

Seek Continual Agreement

Throughout the interview process—from the introduction to the close—the interviewer should seek continual agreement by attempting to phrase the questions so that they can be answered "yes." It is easier for people to reply in the affirmative than in the negative.

EXAMPLE

Interviewer:

"Okay?"

"Can you help me?"

"That's okay, isn't it?"

Do Not Invade Personal Space

During the introductory part of the interview, the interviewer generally should remain at a distance of four to six feet. Do not invade the respondent's personal zone (closer than about three feet), as it might make the respondent uncomfortable.

Informational Questions

Informational questions are nonconfrontational, nonthreatening, and are asked for information-gathering purposes. The great majority of the interviewer's questions fall into this category. These types of questions may be asked during any of the following types of interviews:

- Interviews to gain an understanding of accounting control systems
- Interviews concerning documents
- Interviews to gather information regarding business operations or systems
- Pre-employment interviews

Informational questions seek to elicit unbiased factual information. The interviewer will be alert to inconsistency in facts or behavior.

Question Sequences

As a general rule, questioning should proceed from the general to the specific; that is, it is best to seek general information before seeking detailed information. A variation to this approach is to "reach backward" with the questions, by beginning with known information and working toward unknown areas. An efficient method of doing this is to recount the known information and then frame the next question as a logical continuation of the facts previously related.

It is common, especially in accounting and fraud-related matters, for figures or numbers to be critical to an examination. Unfortunately, some witnesses are unable to recall specific amounts. The interviewer can jog the respondent's memory by comparing unknown items with known items.

EXAMPLE

Interviewer:

"Was the amount of money involved more than last year's figure?"

Questioning Techniques

Asking the right question is necessary to conduct an effective interview. By asking the right questions, the interviewer can improve a whole range of communication skills. Informational questions—as well as others—fall into several general categories.

Open Questions

Open questions are those worded in a way that makes it difficult for the respondent to answer "yes" or "no." Also, the answer to an open question is not dependent on the question. The typical open question calls for a monologue response, and it can be answered in several different ways.

During the information phase of the interview, the interviewer should endeavor to ask primarily open questions. This is to stimulate conversation.

Some of the best open questions are subtle commands.

EXAMPLE

Interviewer:

"Please tell me about your job."

"Please tell me about the operation of your department."

"What do you think about this problem?"

"Please describe the procedures to me."

Closed Questions

Closed questions are those that require a precise answer: usually "yes" or "no." Closed questions also deal with specifics, such as amounts, dates, and times. As far as possible, closed questions should be avoided in the informational part of the interview. They are used extensively in closing questions.

EXAMPLE

Interviewer:

"Do you work here?"

"What day of the week did it happen?"

Leading Questions

Leading questions are questions that are framed in a way that evokes a specific reply from the respondent; they are questions that contain a suggested answer. Most commonly, leading questions are used to confirm facts already known. This type of question gives the subject much less room to maneuver than an open or closed question because these questions direct the subject to answer in a particular way. Leading questions imply that the interviewer already knows the answer, asking the subject to confirm what is already known, and they can be particularly effective in interview situations.

EXAMPLE

Interviewer:

"So there have been no changes in the operation since last year?"

"Are you still employed by the Westbrook Furnishings Corporation?"

"You got promoted, right?"

"Don't you get your income from various sources?"

Double-Negative Questions

Double-negative questions are questions that have two forms of negation within a single clause. Double-negative questions, or statements containing double negatives, are confusing and often suggest an answer opposite to the correct one. Therefore, they should not be used.

EXAMPLE

Interviewer:

"Didn't you suspect that something wasn't right?" (What does a negative answer mean here?)

Complex Questions

Complex questions are those that consist of a series of interrelated questions. Complex questions and statements are too complicated to be easily understood, cover more than one subject or topic, require more than one answer, or require a complicated answer. Therefore, fraud examiners should avoid asking complex questions.

EXAMPLE

Interviewer:

"What are your duties here, and how long have you been employed?"

Attitude Questions

The attitude of the interviewer can be conveyed by the structure of the question or statement, as well as by the manner in which the question is asked. When the interviewer wishes to establish a friendly mood, he can employ *attitude questions.*

EXAMPLE

Interviewer:

"How are you doing this morning, Ms. Martin?"

"Do you like sports?"

It is always a good idea, however, to ask a question to which you know that the respondent will answer "yes."

Controlled Answer Techniques

Controlled answer techniques or statements may be used to stimulate a desired answer or impression. These techniques direct the interview toward a specific point. For example, it might be possible to get a person to admit knowledge of a matter by phrasing the question like this: "*I understand you were present when the internal controls were developed; would you please describe how they were constructed?*" This phrasing provides a stronger incentive for the respondent to admit knowledge than does, "*Were you present when the internal controls were developed?*"

To stimulate the person to agree to talk or provide information, you might use a prompt, such as, "*Because you are not involved in this matter, I am sure you would not mind discussing it with me.*" This provides a stronger incentive to cooperate than, "*Do you have any objections to telling me what you know?*" Avoid negative construction, such as, "*I don't guess you would mind answering a few questions?*"

Free Narratives

The *free narrative* is an orderly, continuous account of an event or incident, given with minimal or no prompting. It is used to get a quick synopsis of what is known about a matter.

But when seeking to obtain a free narrative, be sure to designate specifically the occurrence that you wish to discuss.

Sometimes the respondent must be controlled to prevent unnecessary digression. Otherwise, avoid interrupting the respondent, and do not stop the narrative without good reason. The respondent will sometimes provide valuable clues when talking about things that are only partially related to the matter under inquiry.

Methodology

Once the introduction has been completed, the interviewer needs a transition into the body of the interview. This is usually accomplished by asking people an easy question about themselves or their duties.

EXAMPLE

Interviewer:

"As I said, I am informally gathering information about Westbrook's operations. I don't know if you can really help me. Can you give me an idea of what you do here?"

Begin with Background Questions

Assuming the respondent does not have a problem answering the transitional question, the interviewer should then ask a series of easy, open questions designed to get the respondent to talk about himself.

EXAMPLE

Interviewer:

"What is your exact title?"

"What do your responsibilities involve?"

"How long have you been assigned here?"

"What do you like best about your job?"

"What do you like least about your job?"

"What would you eventually like to do for the company?"

"Overall, how do you like your current job?"

Observe Verbal and Nonverbal Behavior

During the period when the respondent is talking about himself, the interviewer should discreetly observe verbal and nonverbal behavior.

Ask Nonleading (Open) Questions

Open questioning techniques are used almost exclusively in the informational phase of the interview. The questions must be inquisitory and not accusatory. Remember, the most effective question is constructed as a subtle command.

EXAMPLE

Interviewer:

"Please tell me about _____."

"Please tell me about your current job procedures."

"Please tell me what paperwork you are responsible for."

"Please explain the chain of command in your department."

"Please tell me what procedures are in effect to prevent errors in the paperwork."

"Please explain what you understand to be the system of checks and balances (or internal controls) in your department."

"Please explain where you see areas that need to be improved in the system of checks and balances in your department."

Once the respondent has answered open questions, the interviewer can go back and review the facts in greater detail. If the answers are inconsistent, try to clarify them. But the interviewer should not challenge the honesty or integrity of the respondent at this point.

Approach Sensitive Questions Carefully

Words such as *routine questions* can be used to play down the significance of the inquiry. It is important for information-gathering purposes that the interviewer does not react excessively to the respondent's statements. The interviewer should not express shock, disgust, or similar emotions during the interview. The following are examples of ways to discuss fraud within a company. The questions are posed in a hypothetical way to avoid being accusatory.

EXAMPLE

Interviewer:

"Part of my job is to prevent and uncover waste, fraud, and abuse. You understand that, don't you?"

"Please tell me where you think the company is wasting assets or money."

"Where do you think the company is vulnerable to someone here abusing their position?"

Suggestions

The following are suggestions to improve the quality of the interview during the information-gathering phase.

- Begin by asking questions that are not likely to cause the respondent to become defensive or hostile.
- Ask the questions in a manner that will develop the facts in the order of their occurrence, or in some other systematic order.
- Ask only one question at a time, and frame the question so that only one answer is required.
- Ask straightforward and frank questions; generally avoid shrewd approaches.
- Give the respondent ample time to answer; do not rush him.
- Try to help the respondent remember, but do not suggest answers; also, be careful not to imply any particular answer by facial expressions, gestures, methods of asking questions, or types of questions asked.
- Repeat or rephrase questions, if necessary, to get the desired facts.
- Be sure you understand the answers, and if they are not perfectly clear, have the respondent explain them at the time instead of asking for more explanation later.
- Give the respondent an opportunity to qualify his answers.
- Separate facts from inferences.
- Have the respondent give comparisons by percentages, fractions, estimates of time and distance, and other such comparisons to ascertain accuracy.

- Get all of the facts; almost every respondent can give you information beyond what was initially provided.
- After the respondent has given a narrative account, ask questions about every item that has been discussed.
- Upon conclusion of the direct questioning, ask the respondent to summarize the information given. Then summarize the facts as you understand them, and have the respondent verify that these facts are correct.

Dealing with Resistance

There is always the possibility that the respondent will refuse a request for interview. When the respondent and the interviewer have no connection, respondents are more likely to refuse an interview if contacted first by telephone. Fewer respondents will refuse interviews if contacted in-person. Of course, the more unpleasant the topic, the more likely the respondent is to refuse.

With inexperienced interviewers, there is a danger that the interviewer will perceive resistance when there is none. As a result, the interviewer might become defensive. It is incumbent upon the interviewer to overcome such feelings to complete the interview. The following are specific examples of the types of resistance that will be encountered and how to try to overcome them.

"I'm Too Busy"

When the interviewer contacts the respondent without a previous appointment, there is a possibility that the respondent will be too busy at the moment to cooperate. "I'm too busy" is also used as an excuse for the real source of the person's resistance, which might be lethargy, ego threat, or a dislike of talking to strangers. These situations can be diffused by the interviewer stressing that:

- The interview will be short.
- The interviewer is already there.
- The project is important.
- The interview will not be difficult.
- The interviewer needs help.

"I Don't Know Anything About It"

The interviewer will sometimes get this response immediately after stating the purpose of the interview. This resistance is typically diffused by accepting the statement and then

responding with a question. For example, if a person says, "I don't know anything," the interviewer could respond by saying:

> *"I see. What do your duties involve, then?"*
>
> OR
>
> *"Well, that was one of the things I wanted to find out. Do you know about internal controls, then?"*

"I Don't Remember"

If, during an interview, the respondent replies, "I don't remember," or gives some similar reply, this type of response usually is not an expression of resistance. Instead, it is an expression of modesty, tentativeness, or caution. One of the best ways to respond to this type of response is to remain silent while the person is deliberating. He is saying, in effect, "Give me a moment to think." If this is not successful, the best way to counter is to pose an alternate, narrower question. As with symptoms of resistance, the modesty is accepted and diffused, and an alternate question is posed.

EXAMPLE

Interviewer:

"Mr. McGuire, I understand you might not remember the entire transaction. Do you remember if it was more than $10,000?"

OR

"It's okay if you don't remember the details. Do you remember how it made you react at the time?"

"What Do You Mean by That?"

When the respondent asks for clarification about a posed question, it might represent a symptom of mild resistance with which the respondent is attempting to shift the attention from himself to the interviewer. It also might be a way for the respondent to stall for time while deliberating. Or it could be that the respondent is not sure what the interviewer's question means. The interviewer should typically react to such a question by treating it as a request for clarification. The interviewer should not become defensive; to do so generally will escalate the respondent's resistance.

Difficult People

The interviewer will invariably encounter a few difficult people. There are five common-sense steps to take with such people.

Don't React

Sometimes a respondent will insist on giving the interviewer a "hard time" for no apparent reason, though, in reality, there can be a multitude of reasons why the person refuses to cooperate. There are three natural reactions for an interviewer who is verbally assailed by the respondent: to strike back, to give in, or to terminate the interview. None of these tactics is satisfactory, because none of these responses lead to a productive interview. Instead, the interviewer should consciously ensure that he does not react to anger with hostility.

Disarm the Person

A common mistake interviewers make is to try to reason with an unreceptive person. When a respondent is not receptive, the interviewer must disarm the respondent. Surprise is the best tactic for disarming a hostile person. If the person is stalling, he expects the interviewer to apply pressure; if the person is on the attack, he expects the interviewer to resist. To disarm the person, listen, acknowledge the point, and agree wherever possible.

Change Tactics

In some situations, changing tactics to reduce hostility might be the only viable option. This means casting what the respondent says in a form that directs attention back to the problem and to the interests of both sides. This normally means asking the respondent what he would do to solve the problem.

Make It Easy to Say "Yes"

In trying to negotiate with difficult people, the usual tactic is for the interviewer to make a statement and attempt to get the respondent to agree with it, but there is a better option. A better choice is to agree with one of the respondent's statements and go from there. It is better to break statements into smaller ones that would be difficult to disagree with. This technique will help the difficult person save face.

Make It Hard to Say "No"

Another method interviewers can use to deal with difficult people is to make it hard for the respondent to say "no." One way of making it difficult to say "no" is to ask reality-based

(what-if) questions. These types of questions are used to get the respondent to think about the consequences of not agreeing.

EXAMPLE

Interviewer:

"What do you think will happen if we don't agree?"

"What do you think I will have to do from here?"

"What will you do?"

Volatile Interviews

A *volatile interview* is one that has the potential to bring about strong emotional reactions in the respondent. Typical volatile interviews involve close friends and relatives of a subject, co-conspirators, and similar individuals.

The personality characteristics of those involved in the volatile interview vary. There are, however, common personality characteristics associated with volatile interviews. Some individuals, by nature, are resentful of authority figures, such as fraud examiners and law enforcement officers.

A target's friends, relatives, and romantic interests often make for a difficult interview. They perceive that the fraud examiner is deliberately targeting someone close to them.

Physical Symptoms

In volatile interviews, the individual typically reacts rather than thinks, and frequently, the individual is openly hostile to the interviewer. Individuals experiencing heightened emotions frequently have a dry mouth and tend to lick their lips and swallow more frequently than normal. Throat clearing is also an audible sign of emotion. Restlessness can be indicated by fidgeting, shifting in a chair, and foot-tapping. People under emotional stress typically perspire more than normal.

Under stress, a person's complexion frequently changes. People might look red or flushed, or might appear to be pale. During stress, the heart beats more frequently, and a keen

observer can see the carotid artery—the large artery on each side of the neck—of an anxious individual actually pulsate.

If an individual in a normal situation maintains eye contact, his efforts to avoid eye contact could indicate that he is under stress.

It is important to realize, however, that physical symptoms are not present in all emotional situations.

Other Considerations

There should be two interviewers involved in potentially volatile situations. Having two people present provides psychological strength for the interviewers. Additionally, the second person can serve as a witness in the event that an interview turns bad.

Surprise should be employed in any interview that is considered potentially volatile. If the potentially volatile respondent is unaware that he is going to be questioned, he will therefore be unprepared. If the interview is not conducted by surprise, the interviewer runs the risk of the respondent not showing up, showing up with a witness, or showing up with counsel.

In a potentially volatile interview, the interviewer should ask questions out of their natural sequence. This is necessary to keep the volatile respondent from knowing the exact nature of the inquiry and where it is leading. Although the interviewer will endeavor to obtain information regarding who, what, when, where, why, and how, the order of the questions will vary from that of other interviews. This technique is especially important in situations where the respondent might be attempting to protect himself.

The hypothetical question is generally considered less threatening, and is, therefore, ideally suited for the potentially volatile interview. *Hypothetical questions* pose fictional situations, analogous to an issue in question, that clarify and highlight particular aspects of the inquiry. For example, if the fraud examiner is interviewing Mr. Smith regarding the acts of Mr. Jones, the interviewer should not ask, "*Did Mr. Jones do it?*" Instead, he should ask, "*Is there any reason why Mr. Jones would have done it?*"

Overcoming Objections

Volatile witnesses will voice numerous objections to being interviewed. Some of the most common objections (along with suggested responses) are listed in the following example.

EXAMPLE

Respondent:

"I don't want to be involved."

Interviewer:

The interviewer should answer this question by pointing out that he would not be there, asking questions, if the respondent were not involved. The interviewer should point out that he is saving the respondent trouble by discussing the matter "informally" (do not say "off the record").

Respondent:

"Why should I talk to you?"

Interviewer:

The interviewer should answer by saying that he is trying to clear up a problem and that the respondent's assistance is important.

Respondent:

"You can't prove that!"

Interviewer:

The interviewer should tell the person that he is not trying to prove or disprove anything; he is simply gathering information.

Respondent:

"You can't make me talk!"

Interviewer:

The interviewer should tell the person that he is not attempting to make him do anything; the interviewer is trying to resolve a problem, and would appreciate the help.

Closing Questions

In routine, informational interviews, closing the interview on a positive note is necessary. During interviews, the interviewer should ask closing questions for the following purposes: to reconfirm facts, to gather additional facts, and to conclude the interview.

Reconfirm Facts

It is not unusual for the interviewer to have misunderstood or misinterpreted the respondent's statements. Therefore, to ensure that the interviewer understood the information that the witness provided, he should review the key facts during the closing phase of the interview. However, the interviewer should not attempt to revisit all the information provided by the subject, only the facts that are most relevant.

EXAMPLE

Interviewer:

"Ms. Martin, I want to make sure I have my information straight. Let me take a minute and summarize what we've discussed."

Go over each of the key facts in summary form. When going over the facts, the interviewer should ask closed questions so that the witness can respond either "yes" or "no."

Gather Additional Facts

The closing questions phase should also seek to obtain facts previously unknown. This will provide the respondent further opportunity to say whatever he wants about the matter at hand.

People being interviewed rarely volunteer additional information regarding other witnesses or evidence. The interviewer should, therefore, provide the respondent an opportunity to furnish further relevant facts or opinions.

If appropriate, the interviewer can ask if there are other documents or witnesses that would be helpful to the case. The interviewer, however, should not promise confidentiality; instead, he should say, "*I'll keep your name as quiet as possible.*"

EXAMPLE

Interviewer:

"You have known Alice Cartwright for eight years, correct?"

"You knew Cartwright had some financial problems, is that right?"

"You suspected—but didn't know for sure—that Cartwright might have had an improper relationship with one of our vendors. Is that correct?"

*On vital facts provided by the respondent, add "*Are you sure?*"*

EXAMPLE

Interviewer:

"*Ms. Martin, are you sure you suspected Ms. Cartwright falsified invoices?*"

To obtain additional facts, ask the respondent if there is something else she would like to say. This gives the correct impression that the interviewer is interested in all relevant information, regardless of which side it favors. Try to involve the respondent in helping solve the case—"If you were trying to resolve this issue, what would you do?" This technique gives the respondent an opportunity to assist the interviewer, and it makes the respondent feel like a vital part of the interview.

In addition, asking the witness if there is anything else he would like to say opens the door for him to provide additional information that was not specifically asked for.

Similarly, asking the subject if he knows of someone else whom you might talk to can be helpful and lead to other potential sources of information.

EXAMPLE

Interviewer:

"Ms. Martin, there might be someone else I should talk to. Are there documents available that relate to this that we haven't already discussed? If I keep your name as quiet as possible, are there any suggestions you can give me about whom else I might talk to about this?"

OR

"Are there any other documents or evidence I might look for?"

OR

"If you were in my shoes, what would you do next?"

Conclude the Interview

Concluding the interview is important because it helps maintain goodwill and ensure future cooperation. At the conclusion, the interviewer should ask the subject if he believes he has been treated fairly. This is particularly important at the conclusion of an admission-seeking interview or when the subject has been uncooperative. The interviewer generally should ask this type of question as if it were perfunctory.

EXAMPLE

Interviewer:

"Ms. Martin, this is just a standard question. Do you feel that I have treated you fairly in this interview?"

In addition, the interviewer should ask for permission to call the subject if he has any additional questions; this leaves the door open for additional cooperation.

Finally, the interviewer should shake hands with the respondents and thank them for their time and information.

EXAMPLE

Interviewer:

"Ms. Martin, I know you have given your time and effort to help me. I appreciate it. Good-bye."

Assessment Questions

The closer you get to the admission-seeking interview, the greater the chance of facing deception. Witnesses might try to cover up what they know, and the target might lie to try to convince the interviewer that he is not guilty. When the interviewer believes that the respondent's answers might be deceptive, he should begin asking assessment questions.

Assessment questions seek to establish the respondent's credibility. They are used only when the interviewer considers previous statements by the respondent to be inconsistent because of possible deception.

Once the respondent has answered all questions about the event and the interviewer has reason to believe the respondent is being deceptive, the interviewer must establish a theme to justify additional questions. This theme can ordinarily be put forth by saying, "*I have a few*

additional questions." But when presenting a theme, the interviewer should not indicate that the questions serve a purpose other than seeking information.

In short, the assessment phase will form the basis of the interviewer's decision about whether to pose admission-seeking questions to obtain a legal admission of wrongdoing.

Assessment questions are designed primarily to get a verbal or nonverbal reaction from the respondent. The interviewer will then carefully assess that reaction.

In detecting deception during an interview, the interviewer must remember that the interviewee or target might already be under stress because of the situation. This does not mean he is lying. Darting eyes, shallow breathing, stuttering, or any of the other classic stress signs might be exhibited because the witness is afraid of the situation, not because he is fearful of being caught in a lie. For this reason, it is necessary for the fraud examiner to assess the normal behavior of the individual before assessing any clues to deception. Assessing the norm is also called *norming* or *calibrating the witness*.

Norming or Calibrating

Norming or *calibrating* is the process of observing behavior before critical questions are asked, as opposed to doing so during questioning. Norming should be a routine part of all interviews. People with truthful attitudes will answer questions one way; those with untruthful attitudes will generally answer them differently. Assessment questions ask the subject to agree with matters that go against the principles of most honest people. In other words, dishonest people are likely to agree with many of the statements, while honest people will not.

Suggestions for observing the verbal and physical behavior of the respondent include:

- Use your senses of touch, sight, and hearing to establish a norm.
- Do not stare or call attention to the person's behavior symptoms.
- Be aware of the respondent's entire body.
- Observe the timing and consistency of behavior.
- Note clusters of behaviors.

The best way to calibrate a witness is through the use of noncritical questions on background information, place of employment, and the like. If the witness displays general

nervousness or other verbal and nonverbal clues during this phase of questioning, subsequent indicators might not be reliable. The key is to observe changes in behavior when pertinent questions are asked.

Based on the respondent's reaction to the assessment questions, the interviewer then considers all the verbal and nonverbal responses together (not in isolation) to decide whether to proceed to the admission-seeking phase of the interview. Because it is easy to draw the wrong conclusions when evaluating signs of deception, no single behavior should be isolated and no single conclusion should be drawn from it. Behaviors should be considered together.

Physiology of Deception

It is said that everyone lies and does so for one of two reasons: to receive rewards or to avoid punishment. In most people, lying produces stress. The human body will attempt to relieve this stress (even in practiced liars) through verbal and nonverbal actions that provide clues.

Conclusions concerning behavior must be tempered by a number of factors. The physical environment in which the interview is conducted can affect behavior. If the respondent is comfortable, he might exhibit fewer behavioral quirks. If the respondent is biased toward the interviewer, or vice versa, this will also affect his behavior.

The more intelligent the respondent, the more reliable verbal and nonverbal clues will be. A higher level of intelligence breeds more consistency in responses from which deviations are more clearly recognizable. People of lower intelligence tend to be more erratic in their behavior, and thus meaningful deviations are more difficult to discern.

When attempting to detect deception through verbal and nonverbal actions, it is important to remember that signs of stress do not always mean that a subject is lying. While lying and deception do indeed cause stress, it is not necessarily true that all stress exhibited during an interview is caused by lying. An honest interview subject might feel stress simply by being asked pointed questions about uncomfortable subjects. It is important to consider the totality of evidence that an interview subject is being dishonest, rather than rely on individual behavioral indicators alone.

Behavioral clues are harder to read when the respondent is mentally unstable or is under the influence of alcohol or drugs. That is, people who are mentally unstable or are under the influence of drugs will be unsuitable to interview, and the behavioral clues of such individuals are unreliable.

Similarly, behavioral symptoms of juveniles are generally unreliable.

Additionally, racial, ethnic, and economic factors should be carefully considered when observing a respondent's behavior. Some cultures, for example, discourage looking directly at someone. Other cultures use certain body language that might be misinterpreted.

Also, while pathological liars are inherently difficult to identify as such, their behavioral cues are likely to be unreliable.

There are two basic types of communication: verbal and nonverbal.

Verbal Clues

Verbal clues refer to how an individual conveys information vocally, including tone, pitch, volume, and rate of speech. Verbal clues are those relating to wordings, expressions, and responses to specific questions. Verbal responses include spoken words and gestures that serve as word substitutes, including nodding or shaking the head to indicate "yes" and "no."

The following are some examples of verbal clues.

CHANGES IN SPEECH PATTERNS

Deceptive people often speed up or slow down their speech, or speak louder. A deceptive person might experience a change in his voice pitch because the vocal chords constrict as a person becomes tense. Deceptive people also have a tendency to cough or clear their throats during times of deception.

REPETITION OF THE QUESTION

Repeating the question is a means for a deceptive respondent to gain more time to think of what to say. The respondent might repeat the question verbatim, or he might frame the answer with a request to repeat the question (e.g., "What was that again?" or similar language). Conversely, a truthful subject usually does not have to contemplate his answer.

COMMENTS REGARDING INTERVIEW

Deceptive people will often complain about the physical environment of the interview room, such as, "It's cold in here." They will also sometimes ask how much longer the interview will take.

SELECTIVE MEMORY

In some cases, the deceptive person will have a fine memory for insignificant events, but when it comes to the important facts, he will say something like, "I just can't seem to remember."

MAKING EXCUSES

Dishonest people will frequently make excuses about things that look bad for them, such as, "I'm always nervous; don't pay any attention to that."

EMPHASIS ON CERTAIN WORDS

On frequent occasions, dishonest people will add what they believe to be credibility to their lies by use of emphasis.

OATHS

Dishonest persons frequently use expressions such as "I swear to God," "Honestly," "Frankly," or "To tell the truth" to add credibility to their lies.

CHARACTER TESTIMONY

A dishonest person will often request that the interviewer, "Check with my wife," or "Talk to my minister." This is frequently done to add credibility to a false statement.

ANSWERING WITH A QUESTION

Rather than deny the allegations outright, the dishonest person is more likely to answer with a question, such as, "Why would I do something like that?" As a variation, the deceptive person will sometimes question the interview procedure by asking, "Why are you tormenting me?"

OVERUSE OF RESPECT

Some deceptive people will go out of their way to be respectful and friendly. When accused of wrongdoing, it is improbable that a person will react in an overtly friendly and respectful manner.

EXAMPLE

Respondent:

"I'm sorry, sir, I know you're just doing your job. But I didn't do it."

INCREASINGLY WEAKER DENIALS

When an honest person is accused of something he did not do, that person is likely to become angry or forceful in making denials. The more the innocent person is accused, the more forceful the denial becomes. The dishonest person, in contrast, is likely to make a weak denial. Upon repeated accusations, the dishonest person's denials become weaker, to the point that the person becomes silent.

FAILURE TO DENY

Dishonest people are more likely than honest people to deny an event specifically. An honest person might offer a simple and clear "no," while the dishonest person will qualify the denial: "No, I did not steal $43,500 from the company on June 27." Other qualified denial phrases include "To the best of my memory" and "As far as I recall," or similar language.

AVOIDANCE OF EMOTIVE WORDS

A dishonest person will often avoid emotionally provocative terms such as *steal*, *lie*, and *crime*. Instead, the dishonest person frequently prefers "soft" words such as *borrow*, and *it* (referring to the deed in question).

REFUSAL TO IMPLICATE OTHER SUSPECTS

Both the honest respondent and the dishonest respondent will have a natural reluctance to name others involved in misdeeds. However, the dishonest respondent will frequently refuse to implicate possible suspects, no matter how much pressure the interviewer applies. This is because the culpable person does not want the circle of suspicion to be narrowed.

TOLERANT ATTITUDES

Dishonest people typically have tolerant attitudes toward miscreant conduct. The interviewer in an internal theft case might ask, "What should happen to this person when he is caught?" The honest person will usually say, "They should be fired/prosecuted." The dishonest individual is much more likely to reply, "How should I know?" or, "Maybe he is a good employee who got into problems. Perhaps he should be given a second chance."

RELUCTANCE TO TERMINATE INTERVIEW

Dishonest people will generally be more reluctant than honest ones to terminate the interview. The dishonest individual wants to convince the interviewer that he is not responsible so that the investigation will not continue. The honest person, in contrast, generally has no such reluctance.

FEIGNED UNCONCERN

The dishonest person will often try to appear casual and unconcerned, will frequently adopt an unnatural slouching posture, and might react to questions with nervous or false laughter or feeble attempts at humor. The honest person, conversely, will typically be very concerned about being suspected of wrongdoing, and will treat the interviewer's questions seriously.

Nonverbal Clues

Nonverbal clues refer to clues that are illustrated by an individual's body language. Nonverbal clues to deception include various body movements and postures accompanying the verbal reply. Some common types of nonverbal clues are discussed below.

FULL-BODY MOTIONS

When asked sensitive or emotive questions, the dishonest person will react differently than the honest person. The dishonest person will sometimes change his posture completely, as if moving away from the interviewer. In contrast, the honest person is more likely to lean forward toward the interviewer when questions are serious.

ANATOMICAL PHYSICAL RESPONSES

Anatomical physical responses are the body's involuntary reactions to fright, such as increased heart rate, shallow or labored breathing, or excessive perspiration. These reactions are typical of dishonest people accused of wrongdoing.

ILLUSTRATORS

Illustrators are motions made primarily with the hands that demonstrate points when talking. During nonthreatening questions, the respondent's illustrators might occur at one rate, and during threatening questions, the respondent's use of illustrators might increase or decrease.

INTERRUPT THE FLOW OF SPEECH

Often, deceptive people will take some action to interrupt the flow of speech. Most actions that are designed to interrupt the flow of speech are stress related. Examples include:

- Closing the mouth tightly
- Pursing the lips
- Lip and tongue biting
- Licking the lips
- Chewing on objects
- Placing hands over the mouth

Genuine smiles usually involve the whole mouth; false ones are confined to the upper half. People involved in deception tend to smirk rather than to smile.

HANDS OVER THE MOUTH

Dishonest people will commonly cover the mouth with the hand or fingers when being deceptive. This reaction goes back to childhood, when many children cover their mouths when telling a lie. This nonverbal clue is a subconscious effort to conceal the statement.

MANIPULATORS

Manipulators are motions like picking lint from clothing, playing with objects such as pencils, or holding one's hands while talking. Manipulators are displacement activities that reduce nervousness.

FLEEING POSITIONS

During the interview, dishonest people will often posture themselves in a *fleeing position*. In this position, the respondent's head and trunk might be facing the interviewer, but his feet and lower body might be pointing toward the door in an unconscious effort to flee from the interviewer.

CROSSING THE ARMS

Crossing one's arms over the middle zones of the body is a classic defensive reaction to difficult or uncomfortable questions. When a person places his hands across his body, it can be interpreted as a defensive gesture meant to conceal weakness. A variation of this behavior is crossing the feet under the chair and locking them. These crossing motions occur mostly when being deceptive. Some individuals, however, cross their body or legs to reduce stress.

REACTION TO EVIDENCE

In an attempt to show concern, the guilty person will display a keen interest in implicating evidence. The dishonest person will often look at documents presented by the interviewer,

attempt to be casual about observing them, and then shove them away, as if wanting nothing to do with the evidence.

Methodology of Assessment Questions

Assessment questions should proceed logically from the least to the most sensitive. The following questions illustrate the pattern that an interviewer might take in questioning a witness. In most examples, the question's basis is explained before the question is asked. The initial questions seek agreement. Also, the following questions assume the fraud examiner has some reason to believe the respondent, a company employee, has knowledge of a suspected fraud.

EXAMPLE

Interviewer:

"The company is particularly concerned about fraud and abuse. There are some laws in effect that will cost the company millions if abuses go on and we don't try to find them. Do you know which law I am talking about?"

EXPLANATION

Most individuals will not know about the laws concerning corporate sentencing guidelines, and will, therefore, answer "no." The purpose of this question is to get the respondent to understand the serious nature of fraud and abuse.

EXAMPLE

Interviewer:

"There are laws that can mean fines of more than $200 million against companies that don't try to clean their own houses. $200 million is a lot of money, so you can understand why the company's concerned, can't you?"

EXPLANATION

The majority of people will say "yes" to this question. In the event of a "no" answer, the interviewer should explain the issue fully and, thereafter, attempt to get the respondent's agreement. If that agreement is not forthcoming, the interviewer should assess why not.

EXAMPLE

Interviewer:

"Of course, these laws are not referring to a loyal employee who gets in a bind. They're talking more about senior management. Have you ever read in the newspapers about what kind of people engage in company misdeeds?"

EXPLANATION

Most people read the newspapers and are at least generally familiar with the problem of fraud and abuse. Agreement by the respondent is expected to this question.

EXAMPLE

Interviewer:

"Most of them aren't criminals at all. A lot of times, they're just trying to save their jobs or just trying to get by because the company is so cheap that it won't pay people what they are worth. Do you know what I mean?"

EXPLANATION

Although the honest person and the dishonest person will both probably answer "yes" to this question, the honest individual is less likely to accept the premise that these people are not wrongdoers. Many honest people might reply, "*Yes, I understand, but that doesn't justify stealing.*"

EXAMPLE

Interviewer:

"Why do you think someone around here might be justified in taking company property?"

EXPLANATION

Fraud perpetrators commonly attempt to rationalize their acts. Therefore, when compared to an honest person, a dishonest individual is more likely to attempt a rationalization, such as, "*Everyone does it,*" or "*The company should treat people better if they don't want them to steal.*" The honest person, in contrast, is much more likely to say, "*There is no justification for stealing from the company. It is dishonest.*"

EXAMPLE

Interviewer:

"How do you think we should deal with someone who got in a bind and did something wrong in the eyes of the company?"

EXPLANATION

Similar to other questions in this series, the honest person wants to "throw the book" at the perpetrator, while the culpable individual typically will say, "How should I know? It's not up to me," or, "If they were a good employee, maybe we should give them another chance."

EXAMPLE

Interviewer:

"Do you think someone in your department might have taken something from the company because they thought they were justified?"

EXPLANATION

Most people—honest or dishonest—will answer "no" to this question. The culpable person, however, will more likely say "yes" without elaborating. The honest person, if answering "yes," will most likely provide details.

EXAMPLE

Interviewer:

"Have you ever felt yourself—even though you didn't go through with it—justified in taking advantage of your position?"

EXPLANATION

Again, most people, both honest and dishonest, will answer this question "no." The dishonest person, however, is more likely to acknowledge having at least "thought" of doing it.

EXAMPLE

Interviewer:

"Who in your department do you feel would think they were justified in doing something against the company?"

EXPLANATION

The dishonest person will not likely furnish an answer to this question, saying instead that, "I guess anyone could have a justification if they wanted to." Conversely, the honest individual is more likely to name names—albeit reluctantly.

EXAMPLE

Interviewer:

"Do you believe that most people will tell their manager if they believed a colleague was doing something wrong, like committing fraud against the company?"

EXPLANATION

The honest person has more of a sense of integrity, and is much more likely to report a misdeed. The dishonest person is more likely to say "no." When pressed for an explanation, the dishonest person will typically say, "No, nothing would be done about it, and they wouldn't believe me anyhow."

EXAMPLE

Interviewer:

"Is there any reason why someone who works with you would say they thought you might feel justified in doing something wrong?"

EXPLANATION

This is a hypothetical question designed to make the wrongdoer think that someone has named him as a suspect. The honest person will typically say "no." The dishonest person is more likely to try to explain why someone would consider him a suspect by saying something like, "I know there are people around here who don't like me."

EXAMPLE

Interviewer:

"What would concern you most if you did something wrong and it was found out?"

EXPLANATION

The dishonest person is likely to say something like, "I wouldn't want to go to jail." The honest person, however, might reject the notion by saying, "I'm not concerned at all, because I haven't done anything." If the honest person

does explain, it will usually be along the lines of disappointing friends or family; the dishonest person is more likely to mention punitive measures.

TYPICAL ATTITUDES DISPLAYED BY RESPONDENTS	
Truthful	**Untruthful**
Calm	Impatient
Relaxed	Tense
Cooperative	Defensive
Concerned	Outwardly unconcerned
Sincere	Overly friendly, polite
Inflexible	Defeated
Cordial	Surly

INTERVIEWING SUSPECTS AND SIGNED STATEMENTS

Admission-Seeking Questions

The choice of when to conduct an admission-seeking interview of a suspect is critical. Normally, the interviewer should ask accusatory or admission-seeking questions when all of the following are true:

- There is a reasonable probability that the respondent has committed the act in question.
- All other reasonable investigative steps have been completed and as much information as possible has been developed from other sources.
- The interviewer can reasonably control the interview's place, time, and subject matter.

An assessment of culpability might be based on verbal and nonverbal responses to interview questions, as well as documents, physical evidence, and other interviews.

A transitional theme is necessary when proceeding from assessment-seeking questions to admission-seeking questions. In part, the theme should be designed to make the subject believe that he has been caught. Under the ideal circumstance, the interviewer should leave the room for a few minutes before proceeding to admission-seeking questions, saying that he has to leave to "check on something."

If the interviewer has incriminating documents, he can place copies of the documents inside a file folder and bring them back to the interview. If no documents exist, the interviewer might consider bringing a file folder filled with blank paper back to the interview.

EXAMPLE

When the interviewer returns to the room, the file folder is placed on the desk, and the interviewer asks, *"Is there something that you would like to tell me about_____?"*

OR

"Is there any reason why someone would say that you _____?"

If the interviewer has incriminating documents, he should hand the documents to the respondent and ask for "comments." He should not introduce the evidence or explain it. In about 20 percent of the cases, the subject will admit to incriminating conduct. If not, the interview must proceed. Once the interviewer is reasonably convinced of guilt, it might be appropriate to confront the respondent.

Purpose of Questions

Admission-seeking questions have at least three purposes. The first purpose is to distinguish innocent people from guilty individuals. A culpable individual will frequently confess during the admission-seeking phase of an interview, while an innocent person will not do so unless threats or coercion are used. In some instances, the only way to differentiate the culpable from the innocent is to seek an admission of guilt.

The second purpose is to obtain a valid confession. Under most jurisdictions' law, confessions must be voluntarily obtained. Generally, the fraud examiner should seek to obtain an oral and written confession. In some jurisdictions, such as the United States, oral confessions are as legally binding as written ones; however, written statements are more credible. A written confession is tangible proof of an admission, whereas an oral confession is more abstract. Written confessions also discourage culpable individuals from later attempting to recant their verbal confessions.

The third purpose of admission-seeking questions is to convince the confessor to sign a written statement acknowledging the facts.

Preparation

The admission-seeking interview should be scheduled when the interviewer can control the situation. It normally should not be conducted in a venue that is overly familiar to the subject and is best conducted by surprise.

Preparing the Interview Room

When preparing a room for an admission-seeking interview, it is important that the interviewer consider the privacy afforded by the room. The location should establish a sense of privacy. The door should be closed but not locked, there should be no physical barriers preventing the target from leaving, and the suspect should be made aware that he is free to leave. This is to avoid allegations of custodial interrogation.

Distractions should be kept to a minimum. Ideally, there should be no photographs, windows, or other objects in the room. Chairs should be placed about four to six feet apart, and the accused should not be permitted to sit behind any physical barriers, such as chairs, tables, or desks. This is to prevent a physical barrier from becoming a psychological barrier that might inhibit responses from the accused.

Note-Taking

Note-taking during an admission-seeking interview should be unobtrusive. In some situations, taking notes should be altogether avoided. Because the admission-seeking interview's ultimate goal is to obtain a signed statement in which the suspect admits guilt, it is not necessary to take extensive notes. Such notes can actually be distracting to the suspect and can reveal what points the fraud examiner believes to be important; thus, if the fraud examiner takes notes during the interview, he should do so in a way that does not reveal their significance.

Presence of Outsiders

It is usually not necessary to inform the subject that he may have counsel present. Of course, this right cannot be denied if the subject wishes to have an attorney present. If counsel is present, there should be an understanding that he will be an observer only; attorneys should not ask questions or object. Other than the subject and two fraud examiners, no other observers should be permitted in the admission-seeking interview because, among other reasons, the presence of third parties could have liability consequences. If the accused is in a union, a union representative (or a union attorney) might have the right to attend. However, this might present legal problems in allowing a third party to hear any allegations made.

Because it is very difficult to obtain a confession with witnesses present, the fraud examiner should consider whether the case can be proven without the admission-seeking interview. (Please refer to the Law section of the *Fraud Examiners Manual* for more information.)

Theme Development

A transitional theme is necessary when proceeding from assessment-seeking questions to admission-seeking questions.

People rarely confess voluntarily. People will confess to matters when they perceive that the benefits of confession outweigh the penalties. A good interviewer, through the application of sophisticated techniques, will be able to convince the respondent that the confession is in his best interest.

People generally will not confess if they believe that there is doubt in the accuser's mind regarding their guilt. Thus, the interviewer must convey absolute confidence in the admission-seeking interview—even if not fully convinced. The interviewer must make the

accusation in the form of a statement of fact. Accusatory questions do not ask, "Did you do it?" They ask, "Why did you do it?"

An innocent person generally will not accept the question's premise. People confessing need adequate time to come to terms with their guilt; obtaining admissions and confessions takes patience. Therefore, admission-seeking interviews should be conducted only when there is sufficient privacy and time is not a factor. The interviewer must not express disgust, outrage, or moral condemnation about the confessor's actions. To do so goes against the basic logic of obtaining confessions, which can be summed up as *maximize sympathy and minimize the perception of moral wrongdoing.*

The interviewer must offer a morally acceptable reason for the confessor's behavior. The interviewer cannot convey to the accused that he is a "bad person." Guilty people will almost never confess under such conditions. To obtain a confession, the interviewer must be firm, but he must also project compassion, understanding, and sympathy. The interviewer must attempt to keep the confessor from voicing a denial. Once the accused denies the act, overcoming that position will be very difficult.

The threat of a lawsuit is always present when allegations of wrongdoing are made against certain employees. It is, therefore, important that fraud examiners understand exactly what actions are permitted so that they can avoid potential liability. It is generally legal to accuse innocent people of misdeeds they did not commit as long as:

- The accuser has reasonable suspicion or predication to believe the accused has committed an offense.
- The accusation is made under conditions of privacy.
- The accuser does not take any action likely to make an innocent person confess.
- The accusation is conducted under reasonable conditions.

Steps in the Admission-Seeking Interview

Make a Direct Accusation

The admission-seeking interview begins with a direct accusation. The accusation should be made in the form of a statement; it should not be made in the form of a question.

Also, emotive words such as *steal*, *fraud*, and *crime* should be avoided during the accusatory process. The accusation should be phrased as though the accused's guilt has already been established, trapping the accused with no way out.

EXAMPLE

WRONG:

"We have reason to believe that you ..."

OR

"We suspect that you might have ..."

RIGHT:

"Our investigation has clearly established that you:

* *made a false entry (avoid* fraud*)*
* *took company assets without permission (avoid using* theft*,* embezzlement*, or* stealing*)*
* *accepted money from a vendor (avoid* bribe *or* kickback*)*
* *have not told the complete truth (avoid* lie *or* fraud*)"*

OR

"We have been conducting an investigation into _____, and you are the only person we have not been able to eliminate as being responsible."

Observe the Accused's Reaction

When accused of wrongdoing, the typical guilty person will react with silence. If the accused does deny culpability, those denials will usually be weak. In some cases, the accused will almost mumble the denial. It is common for the culpable individual to avoid outright denials. Rather, he will give reasons why he could not have committed the act in question.

Conversely, the innocent person will sometimes react with genuine shock at being accused. It is not at all unusual for an innocent person, wrongfully accused, to react with anger. In contrast to the guilty individual, the typical innocent person will strongly deny carrying out the act or acts in question.

Repeat the Accusation

If the accused does not strenuously object after the accusation is made, the interviewer should repeat the accusation with the same degree of conviction and strength.

EXAMPLE

Interviewer:

"As I said, Carmen, our examination has concluded that you are the person responsible. It is not so much a question of what you did, but why you did it."

Interrupt Denials

Both the truthful and untruthful person will normally object to and deny the accusations. But when compared to an innocent person, a culpable person is more likely to avoid issuing an outright denial ("I didn't do it.") and is more apt to provide the interviewer with explanations as to why he is not the responsible party.

EXAMPLE

Respondent:

"I wasn't even there the day that entry was made."

OR

"It could have been anybody."

OR

"I don't know what you're talking about."

Both the innocent and the guilty person will make an outright denial if forced to do so. Accordingly, the interviewer should not solicit a denial at this stage of the admission-seeking interview.

EXAMPLE

WRONG:

Interviewer:

"Did you do this?"

OR

"Are you the responsible person?"

RIGHT:

Interviewer:

"Why did you do this?"

Also, once the accused utters a denial, it becomes extremely difficult for him to change his response, because doing so would be an admission that he lied. The interviewer must prevent an outright denial, thereby making it easier for the subject to confess at a later time. An innocent person is unlikely to allow the interviewer to prevail in stopping the denial.

Fraud examiners can use several techniques to stop or interrupt denials, including delays, repeat interruptions, and reasoning.

DELAYS

One of the most effective techniques to stop or interrupt a denial is through a delaying tactic. To employ this technique, the interviewer should attempt to delay the outright denial; he should not argue with the accused.

EXAMPLE

Interviewer:

"Carmen, I hear what you are saying, but let me finish first. Then you can talk."

The innocent person usually will not let the interviewer continue to develop the theme.

REPEAT INTERRUPTIONS

Occasionally, it might be necessary to interrupt the accused's attempted denial repeatedly. Because this stage is crucial, the interviewer should be prepared to increase the tone of the interruptions to the point where he is prepared to say: "*Carmen, if you keep interrupting, I am going to have to terminate this conversation.*" The guilty individual will find this threatening, because she wants to know the extent of incriminating evidence in the interviewer's possession.

REASONING

If delays and repeated interruptions are unsuccessful, the interviewer might attempt to reason with the accused and employ some of the tactics normally used for diffusing alibis. Under these tactics, the accused is presented with evidence implicating him. The interviewer, however, normally should not disclose all the facts of the case, but rather reveal small portions incrementally.

EXAMPLE

Interviewer:

"I know what you say, Carmen, but that doesn't reconcile with these invoices here in front of me. Look at the invoice in the amount of $102,136. The facts clearly show you are responsible." (Do not ask the accused to explain the evidence at this point.)

OR

"Carmen, I have talked to many people before I sat down here with you. I am not asking you if you're responsible; I know you are. This is your opportunity to tell your side to

someone who can understand." (Do not disclose the identity or number of witnesses who have been interviewed.)

Establish Rationalization

Assuming the subject does not confess to the misconduct when faced with direct accusations, the interviewer should seek to convince the respondent that a confession is in his best interest. To do this, the interviewer must offer a morally acceptable reason that allows the accused to reconcile the misdeed with his conscience.

It is not necessary that the rationalization be related to the underlying causes of the misconduct. It is common and acceptable for the accused to explain away the moral consequences of the action by seizing onto any plausible explanation other than being a "bad person."

If the accused does not seem to relate to one theme, the interviewer should move on to another until one seems to fit. Thereafter, that theme should be developed fully. Note that the theme development explains away the moral—but not the legal—consequences of the misdeed. The interviewer is cautioned not to make any statements that would lead the accused to believe he will be excused from legal liability by cooperating.

Rather than being confrontational, the questions posed in the examples constantly seek agreement from the accused. The interviewer must strike a balance between being in control of the interview and still appearing compassionate and understanding. Again, no matter what conduct the accused has supposedly committed, the interviewer should not express shock, outrage, or condemnation.

Some common themes used to established rationalization are provided below.

UNFAIR TREATMENT

Probably the most common explanation for criminal activity in general, and internal fraud in particular, is unfair treatment and the accused's attempt to achieve equity. Studies have shown that counter-productive employee behavior—including stealing—is motivated primarily by job dissatisfaction. Employees and others feel that taking retaliatory action is important to their self-esteem. The sensitive interviewer can capitalize on these feelings by suggesting to the accused that he is a victim.

EXAMPLE

Interviewer:

"Carmen, I feel like I know what makes you tick. And I know it isn't like you to do something like this without a reason. You have worked hard here to get a good reputation. I don't think the company has paid you what you're really worth. And that's the way you feel, too, isn't it?"

OR

"Carmen, I've seen situations like this before. And I think the company brought this on itself. If you had been fairly treated, this wouldn't have happened; don't you agree?"

INADEQUATE RECOGNITION

Some employees might feel that their efforts have gone completely without notice by the company. As with similar themes, the interviewer should be empathetic.

EXAMPLE

Interviewer:

"Carmen, I have found out a few things about you. It looks to me that you have given a lot more to this company than it has recognized. Isn't that right, Carmen?"

FINANCIAL PROBLEMS

Internal criminals, especially executives and upper management, frequently engage in fraud to conceal their true financial condition—either personal or business. Here are examples of how to develop a theme involving financial problems as a motive. In the following example, Ethan is an executive of a company and is suspected of fraud.

EXAMPLE

Interviewer:

"Ethan, I was astonished to find out some of your investments have taken such a beating. I don't know how you managed to keep everything afloat as well as you did. You just did this to stay alive financially, didn't you, Ethan?"

OR

"Ethan, I have found out what you've been paid around here and, frankly, I was surprised. I thought it might be a lot more. No wonder you had to get involved in this. You pretty much needed to do this to survive, didn't you?"

ABERRATION OF CONDUCT

Many offenders believe their conduct constitutes an aberration in their lives and that it is not representative of their true character. The interviewer might establish this theme by applying the following examples.

EXAMPLE

Interviewer:

"Carmen, I know this is totally out of character for you. I know that this would never have happened if something wasn't going on in your life. Isn't that right, Carmen?"

OR

"Ethan, you've worked hard all your life to get a good reputation. I feel you wouldn't normally have done something like this; it just doesn't fit unless you felt like you were forced into it. You felt forced to do this, didn't you, Ethan?"

FAMILY PROBLEMS

Some people commit fraud because of family problems—financial woes caused by divorce, an unfaithful spouse, or demanding children. Men especially—who have been socially conditioned to tie their masculinity to earning power—might hold the notion that wealth connotes family respect. For their part, women have been found to commit white-collar crime in the name of their responsibility to the needs of their husbands and children. The skillful interviewer can convert this motive to his advantage by applying one of the following approaches.

EXAMPLE

Interviewer:

"Carmen, I know you have had some family problems. I know your recent divorce has been difficult for you. And I know how it is when these problems occur. You never would have done this if it hadn't been for family problems; isn't that right, Carmen?"

OR

"Ethan, someone in your position and with your ethics just doesn't do things like this without a reason. And I think that reason has to do with trying to make the best possible life for your family. I know it would be difficult for me to admit to my family that we're not as well off as we were last year. And that's why you did this, isn't it, Ethan?"

ACCUSER'S ACTIONS

Do not disclose the accuser's identity if it is not already known. But in cases where the accuser's identity is known to the accused, it can be helpful to blame the accuser for the

problem. The accuser can be a colleague, manager, auditor, fraud examiner, or any similar person. Alternatively, the problem can be blamed on the company.

EXAMPLE

Interviewer:

"Carmen, you know what these auditors are like. They are hired to turn over every stone. I wonder how they would look if we put them under a microscope. Compared to other things that are going on, what you've done isn't that bad. Right, Carmen?"

OR

"Ethan, I really blame a large part of this on the company. If some of the things that went on around this company were known, it would make what you've done seem pretty small in comparison, wouldn't it, Ethan?"

STRESS, DRUGS, AND ALCOHOL

Employees will sometimes turn to drugs or alcohol to reduce stress. In some instances, the stress itself will lead to aberrant behavior. The interviewer could establish a rationalization regarding stress, drugs, and alcohol similar to the following example.

EXAMPLE

Interviewer:

"Carmen, I know what you've done isn't really you. Inside, you have been in a lot of turmoil. A lot of people drink too much when they have problems. I have been through periods like that myself. And when things build up inside, it sometimes makes all of us do something we shouldn't. That's what happened here, isn't it, Carmen?"

OR

"Ethan, you're one of the most respected men in this company. I know you have been under tremendous pressure to succeed. Too much pressure, really. There is only so much any of us can take. That's behind what has happened here, isn't it, Ethan?"

REVENGE

Revenge can be effectively developed as a motive. In developing this theme, the interviewer attempts to blame the offense on the accused's feeling that he must "get back" at someone or something.

EXAMPLE

Interviewer:

"Carmen, what has happened is out of character for you. I think you were trying to get back at your supervisor for the time he passed you over for a raise. I would probably feel the same. That's what happened, isn't it, Carmen?"

OR

"Ethan, everyone around here knows that the board has not supported you in your efforts to turn this company around. I would understand if you said to yourself, 'I'll show them.' Is that what happened, Ethan?"

DEPERSONALIZING THE VICTIM

In cases involving employee theft, an effective rationalization technique is to depersonalize the victim. The accused is better able to cope with the moral dilemma of his actions if the victim is a faceless corporation or agency.

EXAMPLE

Interviewer:

"Carmen, it isn't like you took something from a friend or neighbor. I can see how you could say, 'Well, this would be okay to do as long as it was against the company, and not my coworkers.' Is that right, Carmen?"

OR

"Ethan, it's not like what you've done has really hurt one person. Maybe you thought of it this way: 'At most, I've cost each shareholder a few cents.' Is that the way it was, Ethan?"

MINOR MORAL INFRACTION

In many cases, the interviewer can reduce the accused's perception of the moral seriousness of the matter. But the moral seriousness should not be confused with the legal seriousness. Fraud examiners and interviewers should be careful to avoid making statements that could be construed as relieving legal responsibility. For example, the fraud examiner should not state: "It is not a big problem, legally. It's just a technical violation." Instead, the interviewer should minimize the moral side's importance. One effective way is through comparisons, such as those illustrated in the following examples.

EXAMPLE

Interviewer:

"Carmen, this problem we have doesn't mean you're a mass murderer. When you compare what you've done to things other people do, this situation seems pretty insignificant, doesn't it?"

OR

"Ethan, everything is relative. What you've done doesn't even come close to some of the other things that have happened. You're not Bernie Madoff, right Ethan.?"

OR

"I could see myself in your place. I probably would have done the same thing, wouldn't I?"

ALTRUISM

In many cases, the moral seriousness of the matter can be reduced by claiming the action was for the benefit of others. This is especially true if the accused views himself as a caring person.

EXAMPLE

Interviewer:

"Carmen, I know you didn't do this for yourself. I have looked into this matter carefully, and I think you did this to help your husband, didn't you?"

OR

"Ethan, you have a big responsibility in this company. A lot of people depend on you for their jobs. I just know you did this because you thought you were doing the right thing for the company, didn't you?"

GENUINE NEED

In a very small number of cases, fraud is predicated by genuine need. For example, the accused might be paying for the medical care of sick parents or a child, or he might have been affected by some other financial disaster. In those cases, rationalization techniques similar to the following examples might be effective.

EXAMPLE

Interviewer:

"Carmen, I don't know many people who have had so many bad things happen all at once. I can see where you thought this was pretty much a matter of life or death, right, Carmen?"

OR

"Ethan, you're like everyone else: You have to put food on the table. But in your position, it is very difficult to ask for help. You genuinely needed to do this to survive, didn't you, Ethan?"

Diffuse Alibis

Even when the accused is presented with an appropriate rationalization, it is likely that he will continue to deny culpability. When the interviewer is successful in stopping denials, the accused frequently will present one or more reasons why he could not have committed the act in question. In these situations, the interviewer must quickly and decisively diffuse these alibis by convincing the accused of the weight of the evidence against him.

The purpose of diffusing alibis is to convince the accused of the weight of the evidence against him. Fraudsters usually have a keen interest in material that tends to implicate them.

Alibis generally can be diffused by displaying physical evidence, discussing the testimony of witnesses, or discussing the subject's prior deceptions.

DISPLAY PHYSICAL EVIDENCE

It is common for most guilty people to overestimate the amount of physical evidence. The interviewer wants to try to reinforce this notion in the way the evidence is laid out to the accused. The physical evidence—usually documents in fraud matters—generally should be displayed one piece at a time, in reverse order of importance. In this way, the accused does not immediately know the full extent of the evidence. When the accused no longer denies culpability, the interviewer should stop displaying evidence.

Each time a document or piece of evidence is laid out to the accused, the interviewer should note its significance. During this phase, the accused is still trying to determine how to react to being caught. The interviewer should, therefore, expect that the accused will attempt to lie his way out of the situation. Like denials, the interviewer should stop the alibis and other falsehoods before they are fully articulated.

Once the alibis are diffused, the interviewer should return to the theme being developed.

EXAMPLE

Respondent:

"I couldn't have done this. I am not responsible for paying invoices."

Interviewer:

"Here is one of the invoices in question [display document]. *We never received the merchandise."* (Don't mention whether you have talked to the accounts

payable department or whether you have subjected the invoice to any document analysis.)

"Look, Carmen, it is useless for you to try to deny the truth. We have lots of evidence. Let's just try to work this out, but you've got to help me, okay?" (Don't accuse the person of lying—this just prolongs the process.)

DISCUSS THE TESTIMONY OF WITNESSES

Another technique for diffusing alibis is to discuss the testimony of witnesses. The objective is to give enough information about what other people would say without providing too much. Ideally, the interviewer's statement will create the impression in the accused's mind that many people are in a position to contradict his story.

The interviewer is again cautioned about furnishing enough information to the accused so that he can identify the witnesses. This might place the witness in a difficult position, and the accused could contact the witness in an effort to influence testimony. The accused could take reprisals against potential witnesses.

EXAMPLE

Respondent:

"I couldn't possibly have done this. It would require the approval of a supervisor."

Interviewer:

"In normal situations it would. The problem is that your statement doesn't hold up. There are several people who will tell a completely different story. I can understand how you would want me to believe that. But you're only worsening the situation by making these statements. If you will help me on this, you'll also be helping yourself. Understand?"

DISCUSS THE ACCUSED'S PRIOR DECEPTIONS

The final technique is to discuss the accused's deceptions. The purpose is to appeal to the accused's logic, not to scold or degrade. This technique is sometimes the only one available if physical evidence is lacking. As with other interview situations, the word *lying* should be avoided.

EXAMPLE

Respondent:

"There is no way I could have done this. I didn't have the opportunity."

Interviewer:

"Carmen, here is the situation: You know what you've done, and so do I. I can understand it is difficult for you to admit. But if all the facts have to be presented, everyone will reach the same inescapable conclusion: You are responsible. If you continue to deny what you've done, you'll just make the situation worse. You understand that, don't you?"

Present an Alternative Question

After the accused's alibis have been diffused, he normally will become quiet and withdrawn. Some people in this situation might cry. If this occurs, the interviewer must be comforting. The interviewer should not discourage the accused from showing emotion. Generally, such reactions indicate that the accused is considering whether he should confess.

At this point in the interview, the interviewer should present an alternative question. The alternative question forces the accused to make one of two choices, both of which imply guilt. One alternative provides the accused a morally acceptable reason for the misdeed; the other paints the accused in a negative light. Regardless of which answer the accused chooses, he is acknowledging guilt.

EXAMPLE

Interviewer:

"Carmen, did you plan this deliberately, or did it just happen?"

OR

"Carmen, did you just want extra money, or did you do this because you had financial problems?"

OR

"Carmen, did you just get greedy, or did you do this because of the way the company has treated you?"

Obtain a Benchmark Admission

Again, the alternative question forces the accused to make one of two choices, both of which constitute a *benchmark admission* (i.e., an answer that implies guilt). So, either way the accused answers the alternative question—either yes or no—he will make a culpable

statement, or a benchmark admission. Once the benchmark admission is made, the subject has made a subconscious decision to confess.

The questions for the benchmark admission should be constructed as leading questions so they can be answered "yes" or "no"; alternative questions should not be asked in a way that requires some type of explanation. That will come later. The accused might also answer in the negative.

EXAMPLE

Respondent:

"I didn't do it deliberately."

OR

"I didn't do it just because I wanted extra money."

OR

"No, I'm not just greedy."

In cases where the accused answers the alternative question in the negative, the interviewer should press further for a positive admission.

EXAMPLE

Interviewer:

"Then it just happened on the spur of the moment?"

OR

"Then you did it to take care of your financial problems?"

OR

"Then you did it because of the way you've been treated here?"

If the accused does not respond to the alternative question with the benchmark admission, the interviewer should repeat the questions or variations thereof until the subject makes the benchmark admission. It is important for the interviewer to get a response that is tantamount to a commitment to confess.

Reinforce Rationalization

Once the benchmark admission has been made, the interviewer should reinforce the confessor's decision by returning to the theme for his rationalization. This will help the confessor feel comfortable and will let him know that the interviewer does not look down upon him.

After reinforcing the subject's rationalization, the interviewer should make the transition into the verbal confession, where the details of the offense are obtained.

EXAMPLE

Interviewer:

"Carmen, I am glad to hear that you had a good reason to do this. That reinforces what I thought all along—that you were caught up in extraordinary circumstances. When was the first time you did it?"

Obtain a Verbal Confession

The interviewer should transition to the verbal confession when the accused furnishes the first detailed information about the offense. There are three general approaches to obtaining the verbal confession: chronologically, by transaction, or by event. The approach taken should be governed by the circumstances of the case.

Once the interviewer has obtained a verbal confession, he must probe gently for additional details—preferably details that only the subject knows.

During the admission-seeking interview, it is best to first confirm the general details of the offense. For example, the interviewer will want the accused to provide estimates of the amounts involved, name other parties involved in the offense, and give the location of physical evidence. After these basic facts are obtained, the interviewer can return to the specifics, in chronological order.

Because of the psychology of confessions, most confessors will lie about one or more aspects of the offense even though they confirm overall guilt. When this happens during the verbal confession, the interviewer should make a mental note of the discrepancy and proceed as if the falsehood had been accepted as truth.

Such discrepancies should be saved until all other relevant facts are provided by the accused. If the discrepancies are material to the offense, then the interviewer should either resolve them at the end of the verbal confession or wait and correct them in the written confession. If not material, such information can be omitted from the written confession.

INFORMATION TO OBTAIN DURING THE VERBAL CONFESSION

The following items of information should be obtained during the verbal confession.

THE ACCUSED KNEW THE CONDUCT WAS WRONG

It is imperative that the interviewer obtain an admission that the accused knew the conduct in question was wrong early in the process. This information will confirm the essential element of intent. *Intent* (i.e., the state of mind with which something is done) is required in all matters involving fraud. Not only must the confessor have committed the act, he must have known the conduct was wrong and intended to commit it. This information can be developed as illustrated in the following example.

EXAMPLE

***Interviewer*:**

"Carmen, now that you have decided to help yourself, I can help you, too. I need to ask you some questions to get this cleared up. As I understand it, you did this, and you knew it was wrong, but you didn't really mean to hurt the company; is that right?"

(Note that the question is phrased so that the confessor acknowledges intent, but "didn't mean to hurt" anyone. Make sure the question is not phrased so that the confessor falsely says that he "didn't mean to do it.")

FACTS KNOWN ONLY TO CONFESSOR

Once the intent question is solved, the questioning turns to those facts known only to the confessor. These facts include—at a minimum—the accused's estimates of the number of instances of wrongful conduct and the total amount of money involved. The questions should not be phrased so that the confessor can answer "yes" or "no."

In fraud matters especially, it is common for the accused to underestimate the amount of funds involved, as well as the number of instances. This is probably because of the human mind's natural tendency to block out unpleasant matters. If the subject provides an estimate of these items, the interviewer should be skeptical of the figure's accuracy. If the accused's response is "I don't know," start high with the amounts and gradually come down.

EXAMPLE

***Interviewer*:**

"Carmen, how many times do you think this happened?"

***Respondent*:**

"I don't have any idea."

***Interviewer*:**

"Was it as many as 100 times?"

***Respondent*:**

"No way!"

***Interviewer*:**

"How about 75 times?"

***Respondent*:**

"That's still too high. Probably not more than two or three times."

***Interviewer*:**

"Are you pretty sure, Carmen?" (If the accused's estimates are too low, gently get her to acknowledge a higher figure. But do not challenge the accused by calling her a liar.)

***Respondent*:**

"Maybe three times, but certainly not more than that."

MOTIVE FOR OFFENSE

Motive is the moving power that prompts a person to act. Motive, however, should not be confused with intent, which refers to the state of mind of the accused when performing the act. Motive, unlike intent, is not an essential element, and criminal law generally treats a person's motive as irrelevant. Even so, motive is relevant for other purposes: It will often guide the interviewer to the proper rationalization, it further incriminates the accused, and it is important for a successful prosecution. Therefore, it is best that the interviewer elicit the suspect's motive when obtaining a verbal confession. The motive might be the same as the theme the interviewer developed earlier—or it might not. The most common response is "I don't know." The interviewer should probe for additional information, but if it is not forthcoming, then attribute the motive to the theme developed earlier. The motive should be established in a manner similar to the following example.

EXAMPLE

***Interviewer*:**

"Carmen, we have discussed what might have led you to do this. But I need to hear it in your words. Why do you think you did this?"

WHEN OFFENSE COMMENCED

The interviewer will want to know the approximate date and time that the offense started. This is usually developed by a question similar to the following.

EXAMPLE

Interviewer:

"Carmen, I am sure you remember the first time this happened."

***Respondent*:**

"Yes."

***Interviewer*:**

"Tell me about it."

***Respondent*:**

"Around the middle of January of last year."

***Interviewer*:**

"Carmen, I admire you for having the courage to talk about this. You're doing the right thing. Tell me in detail about the first time."

WHEN/IF THE OFFENSE WAS TERMINATED

In fraud matters, especially internal fraud, the offenses are usually continuous. That is, the fraudster seldom stops before he is discovered. If appropriate, the interviewer should seek the date the offense terminated. The question is typically phrased as follows:

EXAMPLE

***Interviewer*:**

"Carmen, when was the last time you did this?"

DETERMINE IF OTHERS WERE INVOLVED

Although most frauds are solo ventures—committed without the aid of an accomplice—the interviewer should determine whether others were involved. To obtain this information, the interviewer should not ask if anyone else was involved; instead, he should phrase the question in a way similar to the following examples.

EXAMPLE

***Interviewer*:**

"Carmen, who else knew about this besides you?"

By asking who else "knew," the interviewer is not only asking for the names of possible conspirators, but also about others who might have known what was going on and failed to report it. This question should be worded as "*Who else knew?*" rather than "*Did someone else know?*"

OBTAIN PHYSICAL EVIDENCE

Physical evidence—regardless of how limited it might be—should be obtained from the confessor. In many instances, illicit income from fraud is deposited directly in the perpetrator's bank accounts. The interviewer will typically want to ask the confessor to surrender his banking records voluntarily for review. It is recommended that either (1) a separate written authorization be obtained or (2) specific language be added to the confession noting the voluntary surrender of banking information. The first method is generally preferable.

If there are other relevant records that can be obtained only with the confessor's consent, permission to review those should be sought during the oral confession. In some instances, it might be advisable to delay this step until the written confession is obtained. The request for physical evidence from the confessor can be set up like the following examples.

EXAMPLE

***Interviewer*:**

"Carmen, as part of wrapping up the details, I will need your banking records (or other physical evidence). You understand that, don't you?"

***Respondent*:**

"No, I don't."

***Interviewer*:**

"Well, I just need to document the facts and clear up any remaining questions. You have decided to tell the complete story, including your side of it. I just want to make sure the facts are accurate and fair to you. We want to make sure you're not blamed for something someone else did. And I want to report that you cooperated fully and wanted to do the right thing, okay?"(Avoid the use of the word *evidence* or references to higher tribunals, such as *courts* or *prosecutors*.)

***Respondent*:**

"Okay."

***Interviewer*:**

"Where do you keep your bank accounts?" (If the interviewer knows of at least one bank where the confessor does business, the question should be phrased: *"Carmen, where do you do business besides Florida Marine National Bank?"*)

***Respondent*:**

"Just Florida Marine."

***Interviewer*:**

"I'll need to get your consent to get the records from the bank if we need them. Where do you keep the original records?" (Do not ask the accused's permission to look at the records; rather, tell her the records are needed. Let the accused object if she has a problem with it.)

DISPOSITION OF PROCEEDS

The interviewer should find out what happened to any illicit income derived from the misdeeds. It is typical for the money to have been used for frivolous or ostentatious purposes. It is important, however, that the confessor sees his actions in a more positive light; the interviewer should avoid comments or questions relating to an extravagant lifestyle.

EXAMPLE

***Interviewer*:**

"Carmen, what happened to the money?" (Let the accused explain; do not suggest an answer unless the confessor does not respond.)

LOCATION OF ASSETS

In appropriate situations, the interviewer will want to find out if there are unspent or available assets that the confessor can use to reduce losses. Rather than ask the accused "*Is there anything left?*" the interviewer should ask "*What's left?*"

EXAMPLE

Interviewer:

"Carmen, what do you have left from all of this?"

Respondent:

"Not much. I used most of the money to cover my husband's bills and financial problems. A little money and a boat that is paid for is all I have."

Interviewer:

"Well, whatever it is, this whole thing will look a lot better if you volunteered to return what you could, don't you agree?" (Remember, do not specifically promise the confessor leniency; it will typically invalidate the confession.)

SPECIFICS OF EACH OFFENSE

Once the preliminary information is obtained, the interviewer should return to the specifics of each offense. Generally, to do this, the interviewer should start with the first instance and work through the events in a chronological and logical fashion.

Because these questions seek information, they should be openly phrased so that the answer is independent of the question. It is best to seek the independent recollections of the confessor first before displaying physical evidence. If the confessor cannot independently recall, documents can be used to refresh his recollection. It generally is best to resolve all issues on each instance before proceeding to the next instance. In determining the specifics of the offense, the interviewer should usually ask:

- Who has knowledge of this transaction?
- What does this document mean?
- When did this transaction occur?
- Where did the proceeds of the transaction go?
- Why was the transaction done?
- How was the transaction covered up?

WRITTEN CONFESSIONS

Once the verbal confession is obtained, it should be reduced to a short and concise written statement that contains only enough detail to validate the confession. For more information on the points that should be covered in every written confession, see the discussion on signed statements that follows.

Interviewing is difficult, and few can master the process without considerable practice. The preceding techniques, when properly employed, can immeasurably aid in developing truthful, reliable, and legally valid information.

Signed Statements

The signed statement should reduce the verbal confession into a short, concise written statement. The interviewer should prepare the statement and present it to the confessor for his signature. The statement should be prepared before the confessor leaves the interview. There should be no attempt to make the statement longer than necessary, and it should rarely exceed two or three handwritten pages.

Contents of a Signed Statement

The following points should be included in every signed statement.

Voluntariness of Confessions

In criminal law, a *confession* is an admission of guilt by the accused party. Generally, all confessions must be voluntary to avoid admissibility issues. For example, in the United States, involuntary confessions will be inadmissible as evidence in court.

Accordingly, the signed statement should contain language expressly stating that the confession is being made voluntarily. The voluntariness of a confession should be set forth specifically in the first paragraph of the signed statement, as well as the date of the interview.

Intent

As part of the elements of proof, most crimes require the fact that the confessor knew the conduct was wrong and intended to commit the act. Thus, the signed statement should contain language indicating the subject knowingly and intentionally committed the act and that the subject knew the act wrong.

This can best be accomplished by using precise language in the statement that clearly describes the act (e.g., "*I wrongfully took assets from the company that weren't mine*" versus "*I borrowed money from the company without telling anyone*").

As a general rule, strong emotive words such as *lie* and *steal* should be avoided, as the confessor might balk at signing a statement containing such terms. Still, the wording must be precise. The following are suggested wordings:

EXAMPLE

Instead of:	**Use:**
Lie	*I knew the statement/action was untrue.*
Steal	*I wrongfully took the property of _____ for my own benefit.*
Embezzle	*I wrongfully took _____'s property, which had been entrusted to me, and used it for my own benefit.*
Fraud	*I knowingly told _____ an untrue statement and he/she/they relied on it.*

Approximate Dates of Offense

The signed statement should also include the approximate dates of the offense. Unless the exact dates of the offense are known, the word *approximately* must precede any dates of the offense. If the confessor is unsure about the dates, language to that effect should be included.

Approximate Amounts of Losses

The signed statement should also include the approximate amounts of losses, making sure they are labeled as such. It is satisfactory to state a range of losses ("probably not less than $____ or more than $____").

Approximate Number of Instances

The statement should also include the approximate number of instances. This number is important because it helps establish intent by showing a repeated pattern of activity.

Willingness to Cooperate

The signed statement should also include language indicating the subject's willingness to cooperate. This type of language is important because it makes it easier for the confessor to sign a statement that he perceives to portray him in a more favorable light. The confessor can convert that natural tendency by emphasizing cooperation and willingness to make amends.

EXAMPLE

"I am willing to cooperate in helping undo what I have done. I promise that I will try to repay whatever damages I caused by my actions."

The Confessor's Moral Excuse

The confessor's moral excuse should be included, but the fraud examiner should ensure that the wording of the excuse clause does not diminish legal responsibility.

EXAMPLE

WRONG:

"I didn't mean to do this." (This implies a lack of intent.)

RIGHT:

"I wouldn't have done this if it had not been for pressing financial problems. I didn't mean to hurt anyone."

Acknowledgement That the Confessor Read the Statement

The confessor must acknowledge that he read the statement, and he should initial all the pages of the statement. Any errors should be crossed out and the correct information should be inserted; then, the confessor should be asked to initial the changes, thus providing yet further indication that the confessor has carefully reviewed the statement.

Truthfulness of Statement

The written statement should state specifically that it is true. This adds weight to it. However, the language should also allow for mistakes.

EXAMPLE

"This statement is true and complete to the best of my current recollection."

Key Points in Signed Statements

There is no legal requirement that a statement must be in the handwriting or wording of the declarant. A statement's *wording* should be precise, and because the fraud examiner usually knows how to draft a valid statement, it is generally not a good idea to let a confessor draft the statement himself.

Declarants should read and sign the statement without undue delay. Thus, fraud examiners should not ask the confessor to sign the statement; instead, they should say "*Please sign here.*" Although there is no legal requirement to have a witness present when the confessor signs a written statement, it is a good idea to have two people witness the signing of a statement. Likewise, there is no need to have the statement notarized.

There should not be *more than one written statement for each offense.* If facts are inadvertently omitted from the signed statement, they can later be added to the original statement as an addendum. For legal purposes, prepare separate statements for unrelated offenses. This rule applies because the target might be tried more than once—once for each offense.

Also, fraud examiners should preserve all notes taken during an interview, especially those concerning a confession. Having access to pertinent notes can aid in a cross-examination regarding the validity of a signed statement. Stenographic notes, if any, also should be preserved.

Once a confession is obtained, substantiate it through additional investigation, if necessary.

Criteria-Based Statement Analysis

When collecting witness accounts or conducting interviews concerning a particular fraud case, fraud examiners must continually assess how honest the interviewee has been. Criteria-based statement analysis is a post-interview tool used to determine how truthful a subject has been. In contrast to the kinesic interview, which focuses on analyzing the subject's body language or nonverbal clues, statement analysis examines the subject's language.

Statement analysis is based on the notion that when humans speak, whether intentionally or unconsciously, they specifically select the language they use. In general, the verbal clues that a subject offers while speaking are just as prominent as any nonverbal clues. The tense that

an interviewee uses is often an indication that the interviewee knows more than he is letting on.

For instance, Susan Smith, who was convicted of murdering her two sons in 1995, claimed that a carjacker forced her out of her car and drove away with her two children in the back seat. When the children's father spoke of the missing toddlers, he spoke of them in present tense; when Smith mentioned them, she referred to her boys in the past tense, indicating that she knew they had passed away. Upon interrogation, Smith confessed to driving her car into a lake, drowning her children inside.

Parts of Speech

During a statement analysis, the main items of interest are the particular words used by the subject and any changes in their usage. Breaking down the subject's sentences carefully might reveal many undetected tendencies of the subject's speech.

Pronouns

Pronouns are words used in place of a noun. They are used to indicate association (we, they), cast blame (her fault, their decision), and—perhaps most relevant to statement analysis—to show possession (our, my, his, her).

The noun that is replaced by a pronoun is the antecedent. The proper identification of a pronoun's antecedent is crucial, although there are situations in which the antecedent is ambiguous or simply cannot be determined.

EXAMPLE

> *"During lunch, Serena and Dawn went into Liam's office. When they left, she was carrying a file full of documents."*

In the above example, does the pronoun *she* refer to Serena or Dawn? Perhaps there is further context that might assist in making the determination, but without the ability to ask the subject for clarification, the antecedent remains uncertain.

When describing an incident or situation, a truthful subject will most likely use the pronoun "I." If the subject is guilty of an offense or involved in some fashion, that person will attempt to distance himself from the situation by removing the "I" from his statement.

Often, the "I" will be replaced by "we," as though the subject had little involvement in or was not responsible for the situation.

EXAMPLE

"I went to the grocery store with my girlfriend, but I didn't steal any of the items."

"We went to the grocery store, but we didn't steal anything."

The subject's subconscious reasoning for using "we" is to remove himself from the situation as much as possible. By swapping "we" for "I" in the sentences, the perpetrator hopes to deflect attention or blame.

In a situation in which the subject uses "we" constantly, the subject is indicating to the interviewer that the subject has some sort of relationship with another party in the situation. If, for example, the subject continually refers to "my girlfriend and I" rather than "we," this indicates a lack of personal involvement with the girlfriend. Fraud examiners can use this pronoun usage to determine whether the interviewee is involved in a fraudulent situation with other employees.

Possessive Pronouns

Possessive pronouns are pronouns that show ownership. When an interviewee gives bogus statements concerning an event, he will often drop the possessive pronoun to shift the blame to an exterior force.

EXAMPLE

"I got on my register at 10:30. I was working at my register when I was called away by my supervisor. When I returned to the register, the register was open and the cash was gone."

In this statement, the subject referred to the register as "my register" up until the controversial act took place. At that point, "my register" becomes "the register," indicating that the subject no longer wants to be associated with a corrupted register. This pronoun switch indicates that the subject is being less than truthful.

Additionally, when considering pronouns, it is prudent to note any changes in form, such as from *I* to *we*, or from *my* to *our*. This could indicate that the speaker is seeking to alleviate

responsibility for the activity being discussed. Furthermore, a change from a naturally concise plural pronoun such as *we*, to an extended iteration, such as *my coworker and I*, might indicate missing information or a contentious event that resulted in depersonalizing the relationship.

Verbs

Verbs are words that describe an action, occurrence, or state of being. They are an important part of statement analysis; the tense that the interviewee uses when talking about past events will shed light on whether he is recalling the incident or making it up. When the subject is recalling a past event, he should use past tense verbs when recounting the story.

EXAMPLE

"My wife and I left the house at 7:00, went to dinner, and then saw a movie. We returned to the house after the movie was over."

Generally, a subject will use past tense verbs when recalling a past event, but if he begins being deceptive, he generally will change the verb tense. Typically, the verb tense will change at the moment at which the subject stops recalling a past event and starts improvising a false account.

EXAMPLE

"My wife and I left the house at 7:00, went to dinner, and then saw a movie. We return to the house and as we pull up to it, we see shattered glass on the driveway."

Verb tense is also crucial concerning the whereabouts of another person (e.g., cases involving possible kidnapping). If the person interviewed continually refers to the missing person in the past tense, there is a good chance that the missing person has been harmed. Again, the Susan Smith case is a textbook example of how verb tense usage can lead to a confession.

Balance of the Statement

When most interview subjects recount an event, their version will be naturally balanced. The subject will spend a fairly equal amount of time telling what happened before the event, what took place during the event, and what happened during the aftermath. To get a rough estimate of how balanced a subject's account is, fraud examiners should look at the amount

of time or number of sentences a subject spends on each topic. If any of the portions of the account are exceptionally short, the subject is almost certainly lying.

By performing this type of analysis, the fraud examiner can also determine what elements are absent from the story in a short amount of time.

In their work titled *Criteria-Based Statement Analysis*, German psychologists Max Stellar and Guenter Koehnken identify a number of separate criteria that the fraud examiner can consider when attempting to analyze a just-completed interview.

General Characteristics

The following are general characteristics of an interview that a fraud examiner should consider:

- *Logical structure*: The fraud examiner first examines the statement for "plot holes," checking to ensure that the recounting of events is chronologically correct and does not contain contradictions.
- *Unstructured production*: The fraud examiner should examine the subject's unstructured production at the beginning of the interview by allowing the subject to recount the event without influence or questioning. Generally, an honest person will not tell an interviewer exactly what has taken place in complete chronological order, from start to finish. It is much more likely that the honest individual will recount the events in a scattershot fashion, and the scattered facts and details will eventually mesh into a complete version. But when a subject can sit down and describe past events in complete detail, from beginning to end, it is likely that the subject rehearsed his story.
- *Quantity of details*: During an interview, an honest subject is more likely to recall more details than a dishonest subject. This is because most subjects who fabricate stories cannot bolster their accounts with many details.

Specific Content

Fraud examiners should be mindful of the following specific content:

- *Contextual embedding*: This is based on the premise that a truthful subject's statement will be tightly woven with incidental details, such as the subject's daily routine, habits, or family relationships. A deceptive subject is much less likely to associate an event with such seemingly insignificant details, choosing to focus only on covering up the major event that is being discussed.

- *Descriptions of interaction*: The truthful subject is likely to have some description of the actions and emotions involved with the described incident or people involved in the incident.
- *Reproduction of conversation*: Often, a subject will become animated when repeating any conversation related to an incident. When this occurs, the subject is generally telling the truth because it is difficult for a fraudster to improvise cohesive dialogue.
- *Unexpected complications during the incident*: Descriptions of incidents that disrupt the event, such as a sudden halt or interruption of the event, indicate that the subject is speaking truthfully.

Peculiarities of Content

Fraud examiners should consider the following peculiarities when analyzing an interview:

- *Unusual details*: The appearance of quirky but believable details lends credibility to the subject. Fabricated statements rarely contain these types of descriptions.
- *Superfluous details*: A subject who provides details that are not essential or even related to the recalled event are often speaking truthfully. A deceitful subject is often so preoccupied with lying that he will excise this type of information from the story.
- *Accurately reported details misunderstood*: When a witness describes details that he does not understand or comprehend, but that the interviewer does understand, it is likely that the witness is telling the truth.
- *Related external associations*: This criterion focuses on points at which the subject relates his particular experience with some personal or external experiences. When the subject makes a relationship between the event and something that has occurred in his life, he is likely being honest.
- *Accounts of subjective mental state*: The subject who provides descriptions of feelings and emotions is likely being truthful. When a subject cannot provide such information during an interview, it is likely that the subject has not thought through his deceptive story very thoroughly.
- *Attribution of perpetrator's mental state*: The honest subject will often recount the perceived mental state of the perpetrator, suggesting what the subject believes the perpetrator was thinking or feeling at the time of the event.
- *Spontaneous corrections*: An interview subject might often correct himself during the course of the interview, altering earlier details or events. When a subject does this, it is likely that he is being truthful. The deceptive subject wants to project honesty and does not want to correct himself because, in his mind, doing so would give the appearance of deceit.
- *Admitting lack of memory*: This criterion is similar to spontaneous corrections. An honest interviewee will often acknowledge not remembering certain details. A dishonest subject,

however, generally will not acknowledge a lack of knowledge about certain details because he wants to be as complete as possible.

- *Raising doubts about one's own statements*: A deceitful interviewee will almost never raise any concerns about whether his statements are correct. If the subject raises concerns about the accuracy of his statements, he is probably telling the truth.
- *Self-deprecation*: If the subject provides any self-incriminating or personally unflattering details during the interview, it might indicate that he is credible. In contrast, a person who attempts to fabricate a story is unlikely to paint an unsavory picture of himself and therefore will not make self-incriminating or unflattering statements.

COVERT EXAMINATIONS

A *covert operation* is an investigation technique designed to obtain evidence by use of agents whose true role is undisclosed to the target. There are two major forms of covert operations: *undercover operations* and *surveillance operations*.

Several distinctions define these two types of covert operations. Undercover operations seek to develop evidence directly from people involved in the offense through the use of disguise and deceit. Rather than waiting for the information to come by other routes, there is a conscious decision to seek it out. In contrast, surveillance operations use the skills of observation to determine the activity of individuals. Surveillance operations are designed to gather information. For example, a surveillance operation might involve observing a suspect from afar while he meets with a potential co-conspirator. Alternatively, the investigator might pose as the co-conspirator's agent and engage the suspect in conversation in an attempt to gather information; this would be an example of an undercover operation.

Covert operations require the highest degree of skill and planning. Used in a timely manner with great care, a covert operation can produce results that cannot be achieved in any other way. Used incorrectly or handled badly, covert operations can lead to embarrassment, serious financial liability, injury, and even death.

Disguise and deceit in undercover operations are well recognized by the courts as a legitimate function of public and private law enforcement, provided the undercover operation is based on sufficient probable cause. Covert operations cannot be conducted as aimless searches for information. Justification for conducting the operation must be legally sound and defensible and must not violate a person's reasonable expectation of privacy.

Before conducting a covert operation, it is essential that the basis for the operation be committed to writing, preferably in a memo (see the "Report Writing" chapter). The memorandum should clearly state:

- The information upon which the covert operation will be based
- The information that is expected to be gained from the operation
- The identities of suspects, if known
- Operatives under the fraud examiner's care, custody, or control (confidential sources' identities should not be disclosed, but such sources should be referred to with a symbol)

A fraud examiner is undercover when he officially abandons his identity as a fraud examiner and adopts one designed to obtain information from people who do not realize his true identity. The assumed identity might involve adopting another name or it might require an elaborate cover. The aim should be to avoid being compromised, to minimize danger to the fraud examiner, and to ensure the operation's success.

Information sought in a covert operation might include the location of markets for stolen goods, the subject's methods of operation, detailed personal data on all subjects, and any other relevant information. Information should be developed with care to avoid alerting the targets or their associates. Only those people who need to know should be informed of the undercover investigation.

Establishing an Identity

Some covert examinations will call for fraud examiners to fabricate cover stories to conceal their true identities. The story should help the fraud examiner gain the subject's confidence, but it should rarely, if ever, be wholly fictitious. The fraud examiner should be from a city with which he is familiar, but not from the subject's home city. Arrangements should be made to have key people in the fictitious history corroborate the undercover fraud examiner's claims.

Particular attention should be paid to items carried by the undercover fraud examiner, such as pocketbooks, watches, rings, tokens, suitcases, ticket stubs, miscellaneous papers, matches, letters, and sums of money. Documents and identity cards should show the appropriate amount of wear and tear. The fraud examiner should be able to explain how each item came into his possession.

There should be a natural contact between the undercover fraud examiner and the subject. The background story should contain elements that will bring the suspect and the fraud examiner together without any contrived effort. A mutual interest in hobbies, sports, and other leisure activities can provide an opportunity for getting acquainted. The fraud examiner should not pose as an authority on a subject unless he is totally qualified. Many times a fraud examiner's admitted lack of knowledge—but interest in—a given subject will help make the subject feel important and not threatened.

According to Timothy J. Walsh, a security expert, the following situations are those in which covert operations have traditionally worked well:

- There is reliable information about criminal activity or asset losses, but insufficient detail for prevention or apprehension.
- Losses are known to be occurring in an area, but there is no information as to how they are occurring or who is responsible.
- It is desirable to gather information concerning personal relationships or to identify the contacts made with or by certain people.
- It is desirable to compare actual practices with supposed or required practices.
- It is important to obtain information in an indirect manner from people believed to possess it.

Covert operations should be used when there is no other practical way to obtain necessary information.

Objectives

According to Paul O'Connell in an article for *Security Management*, one of the first steps in initiating an undercover operation is to identify the investigation's objectives.[1] The objectives must specifically identify what the operation is designed to discover, such as the identity of the fraudulent worker responsible for a specific crime.

The specific objectives of a covert operation depend on the type of investigation being conducted. For example, the objectives in the surveillance of a warehouse would not be the same as those in surveillance designed to determine if someone is receiving a kickback. However, all covert operations have similar general objectives:

- *To obtain evidence of a past, current, or future crime*: This evidence usually bears on the culpability of individuals. If an operative in a covert investigation is posing as a thief, for example, actual thieves might confess their involvement to him, unaware that their conversations were being recorded.
- *To identify those engaged in possible illegal activity*: If, for example, cash is missing, a covert investigation or surveillance might disclose who is committing the offense. Thereafter, the covert operation might be discontinued and the evidence gathered by more traditional means.

[1] O'Connell, E. Paul. "Is a Ruse the Best Route?" *Security Management*. December 1995, 26–30.

- *To recover illegal gains*: If an accounts payable clerk has been stealing to purchase an automobile, locating the car might permit recovery through civil litigation.
- *To identify co-conspirators*: If an employee is in collusion with another employee, a covert operation might lead to the second individual's identity.
- *To identify the modus operandi*: Again, in the case of missing goods, the perpetrator's identity might be known or suspected, but the internal control deficiencies permitting the theft might be unknown. A covert operation might discover the missing link.

Problems in Covert Operations

In addition to the legal problems a fraud examiner might encounter, a covert operation involves some of the most costly and risky work a fraud examiner can undertake. Such operations consume great amounts of time and human resources. They should be used only with extreme care and as a last resort. If an investigation can be conducted in any other way, the fraud examiner should stay away from covert operations.

Restrictions on Electronic Recordings

Some countries have laws that impose restrictions on electronic audio or video recording. In some countries, it is illegal to record a conversation unless the person creating the recording has the consent of both parties. What is or is not permissible will vary by jurisdiction. To ensure that no laws are violated, fraud examiners must consult with legal counsel or receive proper training specific to that jurisdiction before making any audio recording surreptitiously.

The laws on electronic recordings, however, may even vary within the same country. To illustrate, consider the applicable laws in the United States and Canada.

Restrictions on Electronic Recordings in the United States

In the United States, there are laws governing audio or video recordings of people without their knowledge or consent. The general rule in the United States is that it is legal to photograph, film, and record people in public places, but the laws vary depending on the type of recording.

Most U.S. states have eavesdropping laws that prohibit surreptitious recording of private oral conversations. In most states, making an audio recording of people's private conversations with eavesdropping devices (supersensitive microphones that listen from behind closed

doors, for example) is illegal. Generally, recording private conversations to which one is not a party is illegal unless the recording party has obtained the consent of those involved in the conversation. In some states, it is unlawful to make an audio recording or to listen in on a conversation unless the person making the recording is a party to that conversation. In other states, it is lawful to record any conversation as long as one party to the conversation consents.

It might, however, be legal to record *public conversations,* which are communications that are open and accessible to anyone. In contrast to public conversations, *private conversations* are communications that a person reasonably expects to be private and confidential. Thus, whether a conversation is private depends on whether the parties have a "reasonable expectation of privacy" in the given circumstances. People behind closed doors generally have a reasonable expectation of privacy. Law enforcement investigators may record private conversations (e.g., with wiretaps) if they obtain a warrant or court order.

If a fraud examiner uses operatives or witnesses to record telephone or other oral conversations, he should obtain written consent from them.

Photographing or recording video of someone in a public place is legal in the United States, provided that the person being photographed or recorded does not have a reasonable expectation of privacy in such a place. For instance, a restroom or locker room might be a "public place," but people have a reasonable expectation of privacy that they will not be recorded in such locations.

It is generally legal to take a video recording of a person in public if the recording is not to be used for commercial purposes (i.e., it will not be sold, exhibited, or otherwise used for financial gain) and does not record the accompanying sound; however, such a recording is subject to all of the laws and rules regarding recording audio conversations if the video records any part of a conversation. That is, if a person's words are recorded on video, the law treats the video recording like a recorded audio conversation. Thus, a fraud examiner might be prohibited from recording a conversation if he is not a party to it or he does not have consent from the participating parties.

In summary, the laws governing audio and video recordings in the United States can be confusing and complex. Fraud examiners should contact legal counsel if they have any doubts about creating a recording.

Restrictions on Electronic Recordings in Canada

Like the United States, Canada has laws that place restrictions on electronic recordings. As in the United States, it is legal to take a photograph of anything and anyone on public property, but it is illegal to photograph a person who has a reasonable expectation of privacy.

Also, in Canada, the general rule is that it is illegal to record private conversations. The law, however, varies depending on whether the person recording the conversation is a party to the conversation or is merely eavesdropping.

Section 184 of the Criminal Code of Canada makes it illegal to record private communications, but it provides an exception where a party to the conversation consents to the recording. Accordingly, in Canada, individuals can record conversations to which they are parties, but they cannot record the conversations of others unless they obtain the consent of one of the parties to the conversation.

Entrapment

Many jurisdictions recognize the legal defense of entrapment. *Entrapment* occurs when law enforcement officers or government agents induce a person to commit a crime that he is not previously disposed to commit. Entrapment also poses a legal problem in covert operations, particularly in undercover operations, because the defendant might not be found liable if it appears that he was improperly induced to commit the crime. Therefore, it is imperative that covert operations be properly predicated, and again, covert operations must not be used for aimless searches for information performed without notions of what might be uncovered—practices commonly referred to as "fishing expeditions."

EXAMPLE

A storeowner was concerned because his inventory costs were unusually high in relation to sales. He hired a private investigator to pose as a contract driver and deliver and pick up merchandise to and from the store. The investigator proceeded to offer kickbacks to all employees in the shipping department if they would allow him to leave without signing for the merchandise. One employee took the bait, and was subsequently arrested for theft. The case was thrown out because of entrapment. The courts ruled that there was no reason to believe, simply because of a high sales cost, that merchandise was being stolen. Furthermore, the investigator had no suspect in mind; he was simply "fishing."

Surveillance

Surveillance is the planned observation of people, places, or objects. It is normally concerned with people. Places and objects observed are usually incidental to the primary interest of gathering information about certain people.

There are two general types of surveillance: mobile and fixed. Mobile surveillance is sometimes referred to as "tailing" or "shadowing," and fixed surveillance is referred to as a "stakeout" or "plant." Mobile surveillance can be done on foot or by vehicle and is carried out when people being observed move from location to location. A fixed surveillance is used when a person or activity remains in one place, although the observers might move from one vantage point to another in the immediate area.

Surveillance, whether by foot or vehicle, is predominantly an exercise in common sense, skill, tact, and ingenuity on the observer's part. Carefully planned and properly executed surveillance can be of tremendous value in an investigation; conversely, lack of preparation, poor timing, and unsound surveillance practices can undermine an otherwise well-executed case.

Surveillance can be a valuable technique. It can be used to locate residences, businesses, or other places of interest to the investigation, and it can be used to locate places where criminal activity is conducted. It can also produce important evidence concerning the scope and nature of a person's activities.

Surveillance activities, however, must be carefully recorded. Detailed notes and logs, video recorders (often with special lenses and light sources), sound recordings, and miniature electronic listening devices must be used appropriately.

Two Methods of Surveillance

There are two basic methods of surveillance: loose surveillance and close surveillance. *Loose surveillance* is used when targets do not need to be kept under constant observation. Loose surveillance should be discontinued if the subject becomes suspicious. *Close surveillance* is used when subjects need to be kept under continuous observation, even if it appears that the subjects have become suspicious.

Circumstances might require a fraud examiner to change from loose to close surveillance. It helps to develop a surveillance plan, but the fraud examiner must observe and interpret the circumstances to decide which tactic to employ. If the plan calls for loose surveillance until a specified act is complete, after which the subject is to be put under close surveillance or apprehended, the observer must determine when the specific incident has taken place.

Preparation

Again, before conducting surveillance, fraud examiners should develop a surveillance plan. The observer's attire should conform to the area or group being surveyed. Dress should be conservative, unless conservative dress is not appropriate for the area. Attire should not be loud or flashy so that if the subject notes the observer, it will be less likely that he will form any lasting impression. Minor changes in outer clothing or hand-carried items might alter the overall impression and help prevent recognition by the subject.

Two or more observers working together need complete agreement about the surveillance techniques and schedule. Discreet signals will help each observer understand any given situation.

Planning is essential, but the observers' adaptability and ingenuity are vital. Observers should be chosen for both aptitude and resourcefulness. They must have poise, patience, and endurance. Prior to the surveillance, the observer should prepare and document a cover story that will stand up under scrutiny. This cover story should provide the observer with a reasonable excuse for being in the area and for doing what has to be done there.

Electronic Equipment

Fraud examiners should consider using electronic surveillance equipment when conducting surveillance. For surveillance on foot, transmitting and receiving devices can easily be hidden on the person without arousing suspicion. Transmitters can be concealed in packages, briefcases, or on the person. Light-gathering binoculars and/or metascope equipment for night surveillance should be used if necessary.

Basic Precautions

When conducting surveillance, an observer should refrain from making abrupt, unnatural moves that could attract attention. Observers should also avoid disguises such as false beards, which are impractical, hard to maintain, and easily detectable. The observer should

not look directly into the subject's eyes. Inexperienced observers must overcome the tendency to believe that they have been identified because the subject glances at them several times.

The geography of the area where surveillance is to take place should be studied carefully. The observer should know the location of cul-de-sacs, dead-end streets, or alleys to avoid being trapped or discovered. The investigator must recognize that knowing when to discontinue surveillance to avoid a confrontation with the subject is as important as any other skill required for effective surveillance. Investigators must be circumspect about taking conspicuous actions to maintain surveillance and recognize that losing the subject is not equivalent to failure.

A suspicious subject might suddenly reverse course, enter a dead-end street, board and suddenly depart from public transportation, or engage in a variety of other evasive actions. The observer can counter these strategies by following approved surveillance techniques.

Techniques of Foot Surveillance

One-Person Surveillance

One-person surveillance is best for fixed surveillance. If a moving one-person surveillance must be used, the observer should follow the subject on the same side of the street and keep fairly close. Crowd and street conditions will dictate the appropriate distance. When the subject turns a corner in an uncrowded area, the observer should continue crossing the intersecting street. By glancing up the street in the subject's direction, the observer can note the subject's position and actions.

If conducting surveillance in a crowded area, it might be necessary to decrease the surveillance distance. Unless the subject is standing just around the corner, surveillance can be continued from the same side of the street. Do not turn a corner immediately behind the subject. When operating across the street from the subject, circumstances will dictate whether to operate forward, to the rear, or abreast of the target. The observer should be abreast of the target when he turns a corner to observe any contact with individuals or entry into a building.

Two-Person Surveillance

In the two-person surveillance technique, which is also known as the *A-B* surveillance technique, there are two observers. The first observer, known as the "A" observer, is stationed directly behind the target. The A observer follows the target. The second observer, known as the "B" observer, follows A either on the same side of the street or from across the street. When both observers operate from the same side of the street and the subject turns a corner, A continues in the original direction and crosses the intersecting street. From a vantage point, A signals the correct moves to B. When B is operating across the street and the subject turns a corner to the right, B will cross the street behind the subject and take up the A position. This move should be prearranged. No signals should be necessary. All visual signals should be discreet and consistent with the environment. Should the subject turn to the left and cross the street toward B, B should drop back to avoid meeting the subject. B should keep A in sight to observe signals indicating his next move.

Three-Person Surveillance

In the three-person surveillance technique, which is also known as the *A-B-C* surveillance technique, there are three observers. The A-B-C technique of surveillance is intended to keep two sides of the subject covered. A follows the subject. B follows A and concentrates on keeping him, rather than the subject, in sight. The normal position for B is behind A. C normally operates across the street from the subject and slightly to his rear, enabling C to observe the subject without turning his head. Variations, such as having both B and C across the street or all three of the observers behind the subject on the same side of the street, might be necessary because of crowded conditions or traffic. In this technique, if the subject turns a corner, A continues in the original direction, crosses the intersecting street, and then signals instructions to the other observers from that vantage point. Either B or C can be given the A position, and A might take up the original C position and continue his observation of the subject from across the street.

In another variation of the three-person technique, both A and B might continue in the original direction and cross the street. A signals C to take up the A position. B then crosses the street again and assumes his former B position. A assumes the C position. In the third situation, when C notices that the subject is about to turn a corner, C signals what positions to assume to both A and B.

Other Techniques

There are other ways to lessen the chance of an observer being identified by the subject. One method is known as the *leap-frog method*. In this method, the observers change places with each other by either pre-arrangement or signal.

Another method is the *progressive surveillance method*. This method is used when extreme caution is necessary. With this technique, the subject is followed a certain distance and then the surveillance is discontinued and the time noted. The next day, another observer picks up the subject at the time and place where the surveillance was previously discontinued, and again follows the subject for a short distance. This continues for days until the surveillance is completed.

Techniques of Vehicle Surveillance

General

Vehicle surveillance demands preparations additional to those that are required for foot surveillance. The observer must use a dependable vehicle that is similar to the types of vehicles commonly found in the area where the surveillance will take place. For example, the observer might use a panel truck, automobile, or a large truck or trailer. The vehicle's license should be of the relevant jurisdiction where the surveillance will take place. Consideration should be given to gasoline, water, first-aid equipment, and road-map requirements.

Whenever possible, combining foot and vehicular surveillance can be advantageous. By using both methods, the observers will likely remain more alert. When a subject parks his vehicle and remains in it, an observer on foot can better monitor the subject's actions and those of passersby.

As in foot surveillance, vehicular surveillance requires inconspicuous actions. Observers should generally stay in the same lane as the target to avoid having to make turns from the wrong lane. If the situation allows, observers should change direction, perhaps going around a block to break continuity before the suspect becomes suspicious. At night, it is difficult for the observers to be sure they are following the right vehicle. The target's car can be kept in sight better if it is distinctive. Also, the observer should configure the dome light of his car so that the light will not show when a door is opened. Additionally, headlights and license-plate lights can be wired to allow them to be turned on or off.

One-Vehicle Surveillance

When one vehicle is used, it must remain close enough to allow the observers to monitor the subject's actions, but far enough behind to avoid detection. When a subject's car stops, one observer should follow his actions on foot. The subject normally will not expect to be tailed by a person on foot while he is using his car. When the subject turns a corner, the observers can make one of two possible moves. First, they can continue in the original direction, cross the intersecting street, and make a U-turn; the subject will take little interest in a car turning into the street behind him coming from the opposite direction. An alternative would be to continue in the original direction, cross the intersecting street, and continue around the block.

Two-Vehicle Surveillance

This technique uses two vehicles to follow the subject at different distances on the same street, similar to the "A-B" foot-surveillance method. This technique can be varied by having one vehicle going in the same direction as the subject on a parallel street while receiving radio-transmitted directions from the observers directly behind the subject. This technique is more flexible because the two vehicles can change places from time to time.

Fixed Surveillance

Fixed surveillance, or a stakeout, is used when the subject remains stationary. In fixed surveillance, the observer can move around for closer observation. When one observer is detailed to watch a place with more than one exit, he might have to move about considerably. When preparing for a stakeout, the base of operations should be well planned. The base might be a store, apartment, house, automobile, or truck. A thorough—but cautious—area reconnaissance should be conducted. Necessary equipment should be readily available, such as binoculars, electronic investigative aids, cameras, and sound recording devices.

Aerial Surveillance

Aerial surveillance refers to the observation of a place, person, group, or ongoing activity from an aerial vehicle, and it includes satellite surveillance and surveillance with unmanned aerial vehicles (also known as drones).

Satellite Surveillance

Satellite data may be used for surveillance. With relative ease, a fraud examiner can obtain detailed satellite images from nearly anywhere in the world.

Plant security lends itself to satellite imagery. In addition to providing much of the same information as conventional satellite photographs, multispectral imagery can detect muddy ground, paths taken by people and vehicles, and other information that might help identify potential security problems.

Satellite imagery can be especially useful in surveillance if it is combined with more traditional types of photographic intelligence. This is especially true for large estates or industrial sites where aerial photography is prohibited. It also can be beneficial in a covert operation.

Satellite imagery can help to determine ways to penetrate a site, develop a map of the grounds, and identify important areas. In addition, satellite imagery can be used to investigate areas that are too remote, expensive, or dangerous to send operatives.

Obtaining satellite imagery is simple if the target's location is known. Satellite imagery is widely available online. Google Earth, for example, provides highly-detailed aerial or satellite images for most urban areas in the United States, Canada, and the United Kingdom, as well as industrialized parts of most countries. Additionally, Google Street View and some other services offer street-level images of urban areas, allowing ground-level viewing with 360-degree rotations. In some instances, the interior of a commercial property is mapped and made available by the proprietor, thus allowing investigators the ability to see inside of a building remotely. These images are updated only periodically, but they can be helpful in numerous ways. For instance, suppose a fraud examiner is trying to determine whether a suspect is living beyond his means. When he views the suspect's long-term address via one of these services, the fraud examiner sees a luxury home and several expensive cars in the driveway. These images thereby provide the fraud examiner with potential leads. Similarly, if a fraud examiner suspects that someone is operating a shell entity, using a ground-level view of the listed address might help to detect red flags (empty lot, lack of signage, lack of expected equipment, etc.).

There are some concerns about the legality involving the use of satellite-derived information. Satellite surveillance, for example, might violate privacy laws; however, privacy laws vary

between jurisdictions, and they vary as to whether air and satellite surveillance is legal. Therefore, the fraud examiner should make sure to check the jurisdiction in which the surveillance is being conducted.

In the United States, for example, the Supreme Court has never taken a position on whether the Fourth Amendment, which guarantees the right of all citizens to be free from unreasonable searches and seizures by government authorities, places limits on government use of satellite surveillance, but it has allowed government agents to conduct warrantless aerial surveillance from manned aircraft.

Aerial Surveillance with Unmanned Aircraft

Unmanned aerial vehicles (UAVs), or *drones*, are becoming more popular, and they are a powerful surveillance tool. Drones can be used to observe people in public places, and they can be used to conduct aerial surveillance of locations that are difficult to access.

Drones can range in size and form, and they can be equipped with a wide range of surveillance technologies, such as high-powered cameras; radar technologies; night vision; and infrared, ultraviolet, and thermal-imaging. Thus, drones can be used to collect and store vast amounts of information.

The law on the use of drones for surveillance, however, is unsettled, and drone surveillance implicates several legal matters, especially when conducted over or near private property. A drone flight could constitute a privacy violation, a trespass, or a nuisance. And due to the way that drones collect information, these devices present unique privacy challenges.

Aerial Surveillance Law

Although aerial surveillance can provide valuable information, the use of such technology does raise important questions and concerns about privacy. Accordingly, before fraud examiners use aerial surveillance technologies, they must address the privacy implications of their use and ensure that such technologies are used in accordance with privacy laws and guidelines.

Unfortunately, aerial surveillance law varies among jurisdictions, and it is largely unsettled. The following are examples of how such law applies in various countries.

AERIAL SURVEILLANCE LAW IN THE UNITED STATES

Aerial surveillance law in the United States is unsettled. It is not clear as to what extent the Fourth Amendment, which guarantees the right of all citizens to be free from unreasonable searches and seizures by government authorities, places limits on government use of satellite surveillance or drone surveillance. The Supreme Court has never taken a position on these issues, but it has allowed government agents to conduct warrantless aerial surveillance from manned aircraft.

In general, the Fourth Amendment does not prohibit the government from conducting warrantless aerial surveillance of a home or its curtilage—the area of land attached to a house—so long as the government is conducting the surveillance from public navigable airspace. The U.S. Supreme Court addressed aerial surveillance in a series of cases in the 1980s:

- In *California v. Ciraolo*, 106 S.Ct. 1809, 1810 (1986), the Supreme Court ruled that the government did not violate the Fourth Amendment when it engaged in the warrantless aerial observation of a person's backyard.
- In *Dow Chemical Company v. United States*, 106 S.Ct. 1819 (1986), the court enunciated standards regarding the legality of aerial photography. It expressed concern about satellite surveillance, but did not establish any legal distinction between aerial photography and satellite surveillance.
- In *Florida v. Riley*, 488 U.S. 445 (1989), the Supreme Court ruled that government agents do not need a warrant to observe an individual's property while flying in publicly navigable airspace.

Although the Supreme Court has addressed the legality of warrantless aerial surveillance while flying in publicly navigable airspace, U.S. law is unclear about the operation of aerial surveillance vehicles below navigable airspace, which, as a general rule, includes airspace below 500 feet.

Additionally, aerial surveillance in private places is more likely to violate privacy laws than such surveillance in public spaces because individuals' expectation of privacy is greater in private places than in public spaces.

Also, many states have added laws that impose regulations on the use of drones.

AERIAL SURVEILLANCE LAW IN CANADA

The use of aerial surveillance might conflict with Canadian privacy law, in which an individual's privacy may be protected by, among other things, the Canadian Charter of Rights and Freedoms, common law, federal law (e.g., the Privacy Act and the Personal Information Protection and Electronic Documents Act), and provincial law. But currently, privacy laws in Canada are primarily focused on protecting personal information that is collected by government and commercial businesses.

As in the United States, use of aerial surveillance in Canada is more likely to conflict with privacy laws when in private places than in public spaces. This is because people have a greater expectation of privacy in private places than they do in public spaces.

Drone use is restricted in Canada. Commercial drone use is subject to licensing approvals and safety parameters set by Transport Canada, which is responsible for regulating civil aviation in Canada, but such restrictions do not apply to drones that are flown for recreational purposes. Military drones, however, fall under the authority of the Department of National Defence (DND).

Also, Canada has restrictions on the use of drones over urban areas.

AERIAL SURVEILLANCE LAW IN GERMANY

The use of aerial surveillance in Germany implicates several laws. In particular, conducting aerial surveillance over private property that belongs to a third-party brings the personality rights of the third party into play. The personality rights, which include the right to privacy, are derived from the Basic Law for the Federal Republic of Germany.

Also, the restrictions that apply to the use of GPS tracking devices to conduct surveillance can be applied to the use of drones for surveillance.

What is more, the use of drones is regulated in Germany, but civilian drones that are used for recreation are subject to less stringent standards than those used for commercial purposes. The commercial use of drones requires a permit from the relevant federal state authority, and such authorization is granted only if the drone use will not violate data protection rights.

Night Surveillance Equipment

Night viewing devices allow users to observe events occurring in darkness. Basically, there are two types of night vision devices: *active* and *passive*. Active systems put out their own light source, an infrared beam, which is visible to the user through the systems' infrared scope. Active systems are advantageous because with active devices, users can see in total darkness. There are, however, disadvantages to active systems. Some disadvantages include limited range and the fact that the infrared beam is visible to anyone looking through an infrared scope or through a passive night viewing device.

Passive systems electronically amplify whatever existing light is in the environment, such as moonlight or sky glow. This is why such units sometimes are referred to as *starlight scopes*.

Night viewing devices can be attached to cameras to obtain evidence that will stand up in court, and television recordings, movies, and still photos can all be obtained using night viewing devices.

Sources and Informants

Sources and informants both serve the same purpose—to provide information to help develop a case. However, there are notable differences between confidential sources and confidential informants. The terms should not be used interchangeably.

A *confidential source* furnishes information as a result of occupation or profession and has no culpability in the alleged offense. For example, confidential sources might include barbers, attorneys, accountants, and law enforcement personnel. A *confidential informant* has a direct or indirect involvement in the matter under investigation, and he might be culpable. The distinction between the two sources is their involvement in the offense. Informants can pose treacherous legal issues for the fraud examiner.

Tom Melsheimer, a former U.S. prosecutor, suggests that secretly photographed or recorded conversations provided by an informant are the most convincing type of evidence. This information is generally accepted as something that is sure to be successful for a criminal prosecutor, because there is little that a white-collar criminal can dispute when caught in the act of a fraud.

Types of Informants

In the book *Criminal Investigations*, authors Paul B. Weston and Kenneth M. Wells identify several different types of informants: the basic lead, the participant, the covert, and the accomplice/witness.

Basic Lead Informants

This type of informant supplies information to the police about illicit activities that they have encountered. The reasons that the informant decides to supply information are varied; some informants simply want to "do their part" to stop an unscrupulous activity, while others are interested in harming the criminals against whom they are informing. For instance, many informants in the drug, prostitution, or illegal gambling areas are involved in those areas as well and intend to eliminate some of their competition. Whatever the reason, these informants' only role in a covert investigation is to supply law enforcement with information.

Participant Informants

The participant informant is directly involved in gathering preliminary evidence in the investigation. The informant in this instance not only supplies an investigation with information, but the informant is also involved in setting up a "sting" operation, initiating contact with the criminal for arrest purposes. A participant informant is just what the name suggests—a participant in the investigation of criminal activity.

Covert Informants

A covert informant also supplies information on criminal behavior to authorities. The difference between covert informants and other types of informants is that a covert informant is one who has been embedded in a situation or scenario for a number of years and is called upon only sporadically for newly uncovered information (i.e., tip-offs) and leads. These types of informants are often referred to as *moles* because of the nature of their insulated situation as inside sources. Weston and Wells identify two instances in which covert informants are commonly used: In organized crime and hate-extremist group investigations, covert informants are often culled to get information about upcoming criminal activities by such groups.

Accomplice/Witness Informants

The accomplice/witness informant is called upon often to provide information on criminal activity. Unlike other types of informants, the accomplice/witness informant would be

prosecuted for an offense if he did not give investigators information. The accomplice informant is often persuaded to "spill the beans" on a co-conspirator in exchange for a promise of leniency from the government.

Objectives of Source and Informant Information

There are three essential procedures when using sources and informants. First, keep the informant's identity as confidential as possible. Second, independently verify the information provided by the source or informant. Third, develop witness and documentary evidence from independently verified information. For example, an informant might indicate that a particular suspect committed fraud. If the fraud examiner conducted an interview and got a confession out of the suspect, the information is no longer dependent on the informant's claim.

If the confidential source or informant has provided documents, names of potential witnesses, or other evidence, all reasonable steps must be taken to protect the identity of that source. Care should be taken to ensure that questioning of other witnesses is done in a manner that does not reveal its origin. This can usually be accomplished by phrasing questions in a certain way. For example, Pilar Espinosa furnished confidential information about Liam Barrett, the co-owner of Barrett Brothers Construction Company. When the fraud examiner confronts Barrett, he does not want him to know that he has talked to Espinosa.

EXAMPLE

WRONG:

"Mr. Barrett, someone told me you were bribing building inspectors for special treatment."

RIGHT:

"Mr. Barrett, I have information indicating you are bribing building inspectors for special treatment."

In the above example, the investigator made the confrontation direct, but he did not reveal the origin of the information. If Barrett presses the fraud examiner to learn how he obtained such information, the fraud examiner should keep the information confidential. See the example that follows.

Mr. Barrett:

"Who did you get that *information from?"*

Examiner:

"Emails I have from your company's records, plus other inquiries conducted in this matter."

If necessary, in this example, the fraud examiner would display the evidence from witnesses and documents that would not reveal the source or informant's identity. The information from the source or informant is basically useless unless the fraud examiner can verify its authenticity and independently corroborate it. Suppose a source furnishes the fraud examiner with copies of documents showing that Barrett Brothers Construction Company's building code violations dropped by 80 percent since the bribery allegedly began. This kind of evidence would corroborate the source's story. If a source told the fraud examiner that Barrett frequently had drinks with Eric Whitaker, the city's chief building inspector, the fraud examiner would want to find out some way to verify this information.

Recall that the third objective when using sources is to develop the witness's information and other evidence so that it makes a cohesive case.

Recruitment of Sources and Informants

Fraud examiners should keep in mind the need to develop sources. Business and financial institution executives, law enforcement and other governmental personnel, medical and educational professionals, and internal and external auditors are good contacts for fraud examiners.

The fraud examiner should make contacts in the community well in advance of needing information; this is simply good public relations. If the fraud examiner receives an allegation and needs confidential information, he might obtain assistance from a source cultivated earlier.

Additionally, sources need to feel confident that they can share information without being compromised. In theory, the source will never have to testify; he has no firsthand knowledge. Firsthand information comes from a witness or document.

The fraud examiner might also meet sources when tracking leads during a specific investigation. He might interview a stockbroker from whom the target purchased stock who does not want his identity revealed. The fraud examiner should not encourage a person to provide confidential information, but rather try to get reports on the record. But if the fraud examiner promises confidentiality for a source's information, he must abide by that promise.

Active recruitment of informants is generally not desirable because doing so might appear unseemly to a jury. It is better to encourage an informant to come forward. It is desirable to develop an informant relationship, but such relationships must be handled carefully. The fraud examiner must clearly document the adequate predication for an informant's involvement.

Generally, the most serious questions concerning informants will focus on their culpability. There have been cases where the informant is guiltier than the target. The court might rule that the informant's information cannot be introduced.

Motives of Sources and Informants

Sources

In some instances (but not many), the source might want money or other consideration for furnishing information. The fraud examiner should not initially volunteer any compensation. It is better to have the source request it. This is to avoid any allegation of misconduct against the fraud examiner for paying for information.

Sources have their reasons for providing information. Often, they provide information because they have a sense of moral obligation or because they like and trust the fraud examiner and want to help. Unfortunately, sources might also provide information for far less altruistic reasons, such as having a grudge against the target.

Informants

Informants, especially incidental ones, commonly want something in return for their information. They often take the view that their involvement has personal risk, and they want to be compensated for their contribution. The informant is likely to be predisposed to sell information to the highest bidder.

Informants are motivated by different things. Often, an informant is motivated to pursue the target, not because of any sense of morality, but because the informant and the target are closely involved. One of the most common reasons informants supply information is because they are involved in the offense, and by furnishing information on the target, they can diffuse suspicion from their own activities. The informant might also feel that the criminal activity in which he is involved has become too extreme, so he might report the information hoping for leniency or a reduced sentence. In other situations—such as a drug dealing case—an informant might furnish information because the target is the competition. In many instances, the fraud examiner initially does not know the truth about the informant.

The fraud examiner must also be aware of the overzealous informant. Melsheimer cautions that most of the recently catalogued cases concerning the abuse of informants were the result of "involved informants who are private citizens, self-motivated to satisfy their law enforcement sponsors at virtually any cost." To ingratiate themselves to investigators, these informants will often engage in unscrupulous activities to provide the information they think the investigators are looking for. Accordingly, before obtaining information from this type of informant, the fraud examiner must lay out the ground rules for the informant. Otherwise, the fraud examiner will risk suffering embarrassment (and punishment).

Legal Considerations

As noted, dealing with sources and informants is fraught with legal pitfalls. The fraud examiner should consider potential consequences in all interactions with sources and informants. The fraud examiner might be able to trust a source, but he can rarely trust an informant. Also, fraud examiners should always document their contacts with sources and informants in case problems arise.

Many jurisdictions guarantee the accused the right to confront his accuser. For example, the Sixth Amendment to the U.S. Constitution affords subjects in a criminal investigation the right to confront (cross-examine) the witnesses against them. This right to confront is an absolute right of the accused; it guarantees persons accused of crimes the opportunity to face the government's witnesses in the case against them and challenge the witnesses' testimony. Similarly, Article 6 of the European Convention on Human Rights, which protects the right to a fair trial, guarantees those accused of crimes the right to examine witnesses against them or have them examined. Likewise, in Canada, the right to make full answer and defense is a

principle of fundamental justice, and this right encompasses a number of things, including the right for criminal defendants to examine witnesses against them.

The fraud examiner will usually not be able to testify to what a source or informant said because doing so would violate the general rule against hearsay evidence (i.e., in general, statements made out of court and not based on a witness's direct knowledge are not admissible). In general, a witness can testify only to what he knows; he cannot testify about what someone else has said.

If the fraud examiner decides to pay an informant or source, he should make the payment in cash and obtain a receipt. If the source will not sign a receipt, do not pay him. There have been numerous instances where a receipt was not obtained and the informant subsequently denied receiving funds or challenged the amount paid. If this happens, the fraud examiner will have to defend himself without proof; indeed, some investigators have been accused of having embezzled the payments. Payments should only be made on a cash-on-delivery-of-information basis.

The fraud examiner should obtain the information and verify it before he turns over any money. If he fails to do this, he might become the victim of a scam.

Sometimes, an informant will claim entrapment as a criminal defense, especially when the informant is doing things at the behest of law enforcement. Remember, entrapment occurs when law enforcement officers or government agents induce a person to commit a crime that he is not previously disposed to commit. The entrapment defense asserts that the target is innocent and was unlawfully lured into a crime that he otherwise would not have committed. An entrapment defense can best be overcome by ensuring that the source or informant only gathers information and plays a limited role in the case.

In rare instances, informants have attempted to harm or work with organized crime to harm investigators. They also might falsely claim that the investigators violated some law during the process, such as physical abuse or extortion. Considering these risks, fraud examiners who use informants should not meet them alone. Preferably, face-to-face meetings should be conducted by two members of the investigation team and should take place in an environment they can control, such as their office.

Reporting Contacts

It is recommended that all contact with informants and sources be reported on a memorandum, although the confidential source or informant's identity should not be included in the report. Instead of including the source or informant's identity, the fraud examiner should use symbols to denote the source's identity. It is further recommended that sources be preceded with an "S," followed by a unique identifier (i.e., source #1 would be "S-1"; source #2 would be "S-2"). The symbols for informants would then be "I-1" and "I-2."

Generally, disclosure of the identities of sources and informants should be on a strict need-to-know basis. For that reason, the person's identity should be maintained in a secure file with limited access, and it should be cross-indexed by the source's symbol number. The reliability of the source, if known, and whether the person is in a position to furnish relevant information should be noted in writing.

EXAMPLE

"A source of unknown reliability, but in a position to furnish relevant information (hereinafter referred to as S-1), advised as follows:"

OR

"An informant of known reliability and in a position to furnish relevant information (hereinafter referred to as I-2) advised as follows:"

Private (i.e., non-government) fraud examiners are not in a position to promise leniency to people involved in the commission of a crime or tort. To do so is serious misconduct and a violation of the Certified Fraud Examiner's Code of Professional Ethics. Promises of leniency can only come from the prosecutor or the courts. The fraud examiner may truthfully tell the informant that his cooperation will be made known to the authorities and that people who cooperate are generally treated better.

Promises of Confidentiality

Whether working in private or government sectors, fraud examiners are generally not in a position to offer unqualified confidentiality to informants. Therefore, any promises made to an informant or source should be qualified with the caveat that no absolute assurances of confidentiality can be given. For example, a fraud examiner might say that he cannot guarantee that the source's identity will be kept secret, but that he will do so if possible. In the case of a fraud examiner who is employed by a governmental agency, there might be an

absolute duty not to hold sources and informants in confidence. In many law enforcement agencies, an investigator might not have informants or sources who are unknown to the agency. Investigative agencies also regularly share information on criminal investigations with prosecutors, including the identity of the source of information. The same regulations and considerations could govern business entities.

EXAMPLE

During an examination of Donny Kirkland, a division manager at QRS Technology, you contact Reece Sutter, one of Kirkland's coworkers. Sutter will talk to you only in confidence. You know QRS Technology's policies are to prosecute all criminal offenses. Sutter seems to be the key to making a case against Kirkland. You believe you can independently verify the allegations Sutter furnishes, but you will not be certain until you talk to him. It might be necessary to call on Sutter to testify against Kirkland in order to make the case.

WRONG:

"Mr. Sutter, I promise I will not tell anyone that you talked to me."

RIGHT:

"Mr. Sutter, I promise I will not tell Mr. Kirkland that you talked to me."

The second type of promise above is a conditional promise; the fraud examiner will not directly tell Kirkland, but that does not mean someone else will not. At some point, informants and sources often become witnesses. Under no circumstances should a fraud examiner promise a source or informant that his identity will not become known.

Ethical Considerations with Informants

Using covert or accomplice informants is not a light undertaking, and it can raise ethical issues. Depending on the type of crime involved, the situation can put people at risk—particularly the informant.

For instance, in 2012, government investigators busted a money laundering operation with ties to the Zeta drug cartel in Mexico. Law enforcement officials turned several culpable informants within the organization, using threats of prosecution for failure to cooperate in the investigation. These informants fed important information to authorities, helping to obtain search and arrest warrants. At one point, one of the informants pleaded to be released from his informing duties because he was afraid that he had aroused the suspicions of the

criminals and was about to be killed. The agents insisted that he continue, and he reluctantly did so. Shortly after, his remains were found in his own burnt-out car.[2]

While turned informants like the one just mentioned are not being forced to act (they could opt for a probable conviction instead), fraud examiners who use informants need to carefully consider the potential consequences. The two biggest factors are the likelihood of detection and the likely response (e.g., loss of contact or death). A certain level of risk is inherent in the operation, and it can be difficult to differentiate an informant's reasonable complaint from a mere attempt to escape the cooperation requirement. However, informants who are harmed may refuse or be unable to continue cooperating, and ill treatment can reduce the credibility of the agency for future cooperation.

Additionally, it is best not to use sources and informants in ongoing crimes as "double agents." Such action is inherently risky and places the fraud examiner in the position of having to defend the actions of the source or informant—actions that, in most cases, the fraud examiner cannot control. This leaves the case open to attack during legal proceedings. If it appears critical that the source should be used as an agent, get the approval of the prosecutor or attorney before proceeding.

Use of Operatives

Operatives are subject to greater control than informants are. In a typical scenario, a source or informant advises that information exists or that a crime is currently being committed. The informant's motives might or might not be altruistic. For example, a warehouse worker approaches the fraud examiner and says that a coworker is stealing inventory. The informant wants money for his assistance in apprehending the thief. The fraud examiner does not know if the informant is telling the truth or trying to divert attention from himself.

The informant suggests that he secretly record a conversation with the thief, getting the suspect to admit to the theft. If an informant conducts the investigation under the fraud examiner's direction, he then becomes an operative. To demonstrate a worst-case scenario involving an operative, consider the following example. Without the fraud examiner's knowledge or consent, the informant plants a recording device in the break room at the warehouse and records conversations to which he is not a party (assume that in the

[2] http://tinyurl.com/8nxnju2

jurisdiction, this is a violation of the law regarding interception of communication). Although the recording was made without the fraud examiner's knowledge or consent, the case is nonetheless compromised. The informant might insist that he recorded the conversations at the fraud examiner's request, thereby forcing the fraud examiner to defend himself.

Most operatives lack the training to conduct an investigation, and they cannot, in many instances, be trusted. It is vital that operatives be properly monitored and supervised. Obtain background information on the operative to determine his degree of culpability in the offense, if any. Make certain that the operative clearly understands the objectives of the covert operation, and ensure that he is regularly debriefed before and after critical meetings with the target. Be careful that the operative does not take any action without proper authorization.

SOURCES OF INFORMATION

Generally, the fraud examiner's initial efforts in any fraud examination are best spent identifying, collecting, and securing all possible relevant documents. Documents provide the foundation of the fraud examination case and help build the investigation's structure. Documents can be evidence in establishing that a fraud was committed, in determining the nature and scope of the fraud, and in identifying the parties responsible.

Internal sources—those generated and housed within the subject organization—are often the only resource for certain types of documents, such as accounting and business tax records, copies of canceled checks, or employee personnel files, unless the fraud examiner has the subject's consent or a legal order to obtain those documents from other parties. In most fraud examinations, a large proportion of the documentary evidence will come from inside the organization at issue, but fraud examiners should remember that external sources can also help provide information necessary to conduct a successful examination. External sources can be particularly crucial in helping investigators locate missing assets; locate witnesses and suspects; determine ownership in vendors, competitors, and other related parties; research the suspects' assets and financial condition; and document the suspects' lifestyle and background information. All of this information will help an investigator build a case and will provide the basis for conducting interviews and obtaining confessions later in the investigation.

When external documents are needed, fraud examiners should consider accessing public and nonpublic records, commercial databases, the Internet, social media sites, media records, third-party sources, and other valuable sources.

The fraud examiner must be certain that information obtained is done so legally. Evidence obtained illegally may be excluded from use at trial, and it might give rise to liability. In U.S. criminal cases, for example, illegally obtained evidence falls under the exclusionary rule, which states that evidence obtained illegally will be excluded from use at trial (see the Law section of the *Fraud Examiners Manual*). And although the exclusionary rule does not apply in civil cases or to evidence obtained by private (or non-governmental) entities, obtaining evidence through illegal means might give rise to civil liability or other sanctions.

Most countries, however, are not inclined to create an automatic exclusionary rule like the one found in U.S. law; instead, they leave it up to the trial judge to determine whether illegal

conduct has reached the level of requiring that evidence be excluded from trial. For example, English law does not render relevant evidence inadmissible by the fact that it was obtained illegally, but it does grant English courts the discretion to exclude evidence where the interests of justice so demand. Similarly, Australia employs a balancing test to determine whether illegally obtained evidence can be used at trial. The balancing test provides that courts consider factors such as the seriousness of the misconduct, the seriousness of the crime, and the power of the evidence.

Public Versus Nonpublic Records

There are many types of public and nonpublic records that can aid a fraud examiner's efforts, and this discussion examines the difference between these types of records.

Public Records

Public records are documents that a governmental agency is required to keep by law or that are necessary to discharge the duties imposed by law. Each agency or governmental unit is responsible for many different functions that might require them to maintain unique information.

Public records, which can be accessed by the public and are thus available to anyone who wishes to use them, can be useful to fraud examiners for a number of reasons. They can supply invaluable background information on employees, suspects, and witnesses. They can also be used to corroborate or refute witness statements, help investigators track the flow of stolen cash or other assets, and aid in efforts to recover losses.

Of course, not all government records are open to the public, and the fact that a document is a public record does not mean it can be accessed without restriction. Sometimes a person must show a certain need to access a public record. Generally, such restrictions are in place to prevent certain personal information from being openly available. Some public records, like birth records, contain personal information that could be used to commit crimes like identity theft.

Also, public records are different from publicly available information. *Publicly available information* is information that has lawfully been published or broadcast to the public for

consumption. Unlike public records, publicly available information is not kept by government organizations.

Public records can be obtained from a number of sources. These records can be searched manually or online through governmental agency websites and online public databases. There also are many commercial search firms that will perform public records searches for a fee. Business and commercial indexes, such as Dun & Bradstreet (D&B) and Dow Jones Business Information Services, also can be searched for business credit and other information. However, the fraud examiner should be aware that accessing public records through a third-party service is regulated in many jurisdictions. There might be prohibitions against certain kinds of searches, while other searches can trigger a duty to inform the subject about the nature of the search.

To conduct a public records search, the fraud examiner must have information about the subject. The better informed the fraud examiner is about the subject he is investigating, the easier his search will be. The following items are essential for searching public records for information about an individual:

- The subject's correct name
- The subject's date of birth
- The subject's government identification number (e.g., Social Security number, social insurance number, National Insurance number, or national identification number)
- The subject's last known address

Other relevant items of information include:

- The identities of the subject's close relatives and friends
- The names of the subject's close relatives

Accordingly, at the outset of a search, the fraud examiner should compile everything known about the subject. When compiling such information, the fraud examiner should address certain issues, including:

- What is the subject's full name?
- Does the fraud examiner only know a last name? Is that name so common that a search will return thousands of possibilities? What are some ways of narrowing possible first names for the individual?
- What is the person's approximate age or date of birth?
- Does the person have a criminal background?

- Has the person been sued or sued someone?
- Has the person owned a business?
- Does the person have tax liens?
- Does the person have a professional license (e.g., contractor, accountant)?

Much of the basic information about an individual can be found in audit documents, business records, personnel records, court records, the Internet, and conversations with people who know the subject.

Similarly, when conducting a public records search of a business, the fraud examiner should consider the following:

- Is the business incorporated?
- Where does the company do business?
- What type of business is it?
- Has the business sued or been sued?
- Does the business have real property?
- Does the company finance equipment?
- Does the company charge sales tax (if applicable in the jurisdiction)?
- Is the organization required to make filings that are available to the public?
- How long has the company been in business?

Once the fraud examiner has basic information about the subject, he can use it to search public records and gain intelligence.

Nonpublic Records

In addition to public records, nonpublic records—financial or otherwise—might be needed to prove fraud or to provide leads in a fraud examination. Nonpublic records include information about a person or business considered to be private and confidential.

But unlike public records, nonpublic records are not available to the public, and because members of the public and, by extension, fraud examiners do not have an absolute right to see these personal records, obtaining access might be difficult or impossible.

Moreover, individuals generally will not willingly give their private records to a fraud examiner, and often, the authority of institutions to disclose nonpublic records is restricted by law.

Yet, despite the limitations on obtaining such records, there are a few basic methods that fraud examiners can use to obtain bank records:

- Obtain consent from the individual to whom the records pertain.
- Obtain a subpoena or other legal processes, such as depositions, interrogations, and document requests, if a legal action is filed.
- Obtain a search warrant, although search warrants are only available to law enforcement.

For more information on gaining access to nonpublic records, see the more detailed section on "Nonpublic Records" later in this chapter.

Local Records

The specific information available in public records varies considerably by jurisdiction, but local government agencies often maintain general records. Many of these local resources will be of use in fraud examinations. These records are often helpful for asset and person location, as well as for finding out who owns or is associated with a particular property, individual, or organization. The following are some local sources of records and the type of information they contain.

Building Inspector Records

The following information is generally available through a municipal or regional building inspector's office:

- Building permits showing the names of the applicants, the address of construction, the estimated costs, and the name of the builder or contractor
- Blueprints and plans showing construction details that are often submitted with applications for building permits
- Building inspectors' reports containing information regarding compliance with construction specifications

Building Permit Records

If a business or individual constructs a new building or makes improvements to an existing building, there should be a building permit on file with the local building authority. In addition, before most businesses can open their doors, the local agencies might require that they possess certain permits. In many cases, the person applying for permits will be the owner or someone traceable to the owner. The local fire department might require permits ensuring that the business complies with the fire code. The local health department typically

requires permits for restaurants or other businesses that serve food. Planning and zoning departments enforce regulations regarding the types of businesses and their locations.

Health and Fire Department Records

Health and fire department records are another source of records often available at the local level. Many local health or fire departments conduct routine inspections of businesses for health and safety code or fire code violations. These inspection records might contain valuable information about the business, its operations, the employees, and the owners.

Birth and Death Records

Some local health records agencies maintain birth and death records. The content and availability of these records varies widely, but they might include the name of the individual, address, sex, age, race, birthplace, birthdate, death place, date and time of death, government identification number, close family members, occupational information, medical certificate, and coroner's certificate. If such records are not available locally, there might be a state/provincial or national health office that maintains them.

Public School Records

School systems sometimes maintain teachers' biographies, showing personal background, education, and former employment. They also might maintain student records, showing biographies (in some school districts), grades, and disciplinary actions.

Coroner's Register

A local coroner's register generally contains the name or a description of the deceased; the date of inquest, if any; property found on the deceased and its disposition; and the cause of death. In the United States, the coroner's register is usually located at the county level.

Voter Registration Records

Voter registration records are not public in all jurisdictions, but if they are available, they might contain useful information. Usually, much of the information contained in such records is withheld from the public for privacy purposes, but voter registration records might contain a person's date of birth, mailing address, and political affiliation.

Utility Records

Depending on the location, utilities might be managed by government agencies, private companies, or nonprofit organizations. Although the recent trend has been to restrict access to utility records, the fraud examiner should check with the relevant utility management organization in the subject's area to see what, if any, information is available. Utility records might contain the customer's contact information, even if that number is unlisted. In addition, the fraud examiner should check the names of the subject's friends or relatives.

Marriage Records

Marriage license records and applications include information on previous marriages, maiden names, addresses, and dates of birth. These records are often maintained at the local level (such as the county clerk's office in the United States) where the license was issued.

Court Records

Court records are another common direct and indirect source of information for fraud examinations. Many jurisdictions allow fraud examiners to search court records, and there are also a variety of services that compile and search such records.

In most jurisdictions, most of the papers filed in civil suits are accessible as public records; however, criminal and juvenile actions might not be as open to review. In addition, criminal conviction records are generally available to the public. For employee screening, make sure that conducting criminal background checks is legal in your jurisdiction for the type of position (check applicable law).

A great deal of litigation occurs each year, and many people might be subject to judicial action, voluntarily or not. These records, if available, can provide revealing data about a subject, including:

- The location of individuals
- Identifying pending actions
- Uncovering closed cases
- Insight into marital status (family)
- Tracing sources of funds (probate)
- Identifying financial conditions (bankruptcy)
- Litigation history

- Outstanding judgments
- Criminal history (generally more limited than civil records)

Court Levels

To perform court records searches, fraud examiners need to be familiar with the structure of the jurisdiction's court system. Most jurisdictions implement a tiered court structure, where minor offenses and causes of action (e.g., small claims) are held in one set of courts, and more serious offenses or issues are held in another set. Similarly, a jurisdiction might have courts that are divided based on local/municipal, state/provincial, and central/federal levels of government.

To illustrate, consider the structure of the U.S. court system. In the United States, state and local courts are generally divided into jurisdictions that encompass a single county in a single state. In each state, there are usually three levels: trial courts, appellate courts, and a supreme court. The primary trial-level federal courts are called district courts, with federal Courts of Appeals as the next level and the U.S. Supreme Court as the highest court in the country. Many countries have a similar model of fact-finding lower courts, with issues of appeal being reviewed by higher courts.

Court records are typically maintained by a clerk or administrative office of the court that heard the case. However, there might be an agency that maintains records from multiple court levels. Therefore, to conduct a thorough search of court records, fraud examiners might need to search at multiple court levels.

It is rare for there to be a central public database that maintains all court records at every level of a jurisdiction, and there are no parties that maintain a comprehensive database of court records on a global basis (despite what some records merchants might claim). However, for law enforcement purposes, some countries share available criminal records with authorities in other countries. For example, the European Criminal Records Information System (ECRIS) was established in 2012 to aid in the exchange of criminal records in the national registers of European Union countries.

Also, there are various other sources for obtaining court records, such as public records data vendors, but such vendors might have records that are not up-to–date, accurate, or complete.

Civil Court Records

Courts keep records of civil cases, which are noncriminal legal proceedings involving two or more parties, and many civil records are publicly available to search. Civil courts often maintain various types of records relating to civil cases, such as liens, name changes, and divorces. Civil court records generally include the complaint (identifying the plaintiffs, the defendants, and the cause of action), the answer to the complaint, and the judgment rendered. The availability of these records will vary from country to country, and there might be privacy laws that restrict reporting and transfer of such information.

Relevant civil records can be difficult to obtain because the fraud examiner might not know if or where a person was involved in a civil dispute. Civil disputes can be heard by a court where the subject resides, where another party to the suit resides, where the underlying events occurred, or at another proper venue per the parties' agreement.

The key to locating civil court records is knowing the correct spelling of the subject's name, where the person currently lives, and where he lived in the past.

Depending on the type of suit, civil court records will provide potentially valuable information. Various types of civil suits are discussed here.

Personal Injury Suit Records

Records for a personal injury suit, for example, will often contain an accident report, injury history, statements of the involved parties, and the financial settlement of the case. They can be helpful to identifying income streams (in the case of an injured party) or financial straits (in the case of a party that must pay an award).

Financial Suit Records

Financial lawsuits are those that involve financial law. The records of such suits might contain information on the defending litigant's debtors and creditors, business history, or ability to perform its obligations under a contract.

Divorce Records

Divorce court records might contain valuable information relating to bank accounts, employment, investment income, and other sources of income. Also, divorce records might contain a statement of assets that includes information on bank account holdings, retirement funds, artwork, coin collections, and so on. Moreover, divorce records might contain the

place and date of marriage; the filing date; the filing type; the locations, names, ages, and birthdates of the divorced parties; the names (and ages) of any children the divorced parties have; and the properties owned by the divorced parties. Also, the complaint filed to start the lawsuit might identify the attorneys in the action and contain the parties' signatures.

Divorce records, however, are not available publicly in every jurisdiction.

In the United States, divorces are state court actions, and divorce records can be obtained from the county court in which the divorce decree was granted.

Criminal Court Records

Criminal records can be very valuable, but their availability varies considerably between jurisdictions. In many jurisdictions, most or all criminal records are not available to the general public. As a global trend, the typical approach is to allow individuals to access their own criminal records, but require the subject's consent if another party (e.g., an employer) wants to access such records. There are, however, many exceptions to this model. For instance, in the United States and Canada, most criminal records are publicly available.

Criminal courts will maintain records of criminal filings and criminal convictions, but these types of records should not be confused with each other. Criminal filings are the records of criminal actions the government files against individuals, and therefore, there might be criminal filing records for an individual even if the person was not found guilty of a crime. Criminal conviction records, however, only include records of a final judgment of guilt for a criminal offense.

Criminal court records might provide information describing the offenses and charges filed. These records also might contain the complainant's signature; a transcript of the proceedings made or prepared by a court official; the names of the witnesses; the names of the prosecuting and defense attorneys; and the probation and release decisions, which might include a background investigation of the defendants.

Usually, the particular government recordkeeper will have a defined period for holding criminal records, and the length of time these records are kept often depends on the severity of the offense. Likewise, some crimes might be expunged from the record. Therefore, the

fact that a records search turns up no results does not necessarily mean that the subject has no criminal history.

In the United States, there is no national criminal records database available to the general public, but because most criminal actions are state court actions, records of state court criminal actions can be obtained from the county court in which the case was filed.

Probate Records

Some jurisdictions have separate probate courts to determine the dispersal of assets after a subject's death. The probate court conducts an investigation to verify any debts owed by an individual's estate and sees to the dispersal of assets after all debts are paid. Probate court records include documents filed to show the dispersal of assets after a subject's death.

The debts left in an individual's estate will give the investigator information on the following:

- Names of individuals with an interest in the deceased's estate
- The subject's financial position at the time of death

The dispersal of assets will reveal:

- The names and addresses of heirs to the deceased
- Some indication of the value of the property willed to them

Bankruptcy Records

Many jurisdictions provide bankruptcy records to the authorized parties or the general public. Bankruptcy proceedings generally occur in the jurisdiction in which the debtor resides. It is common for countries to have separate bankruptcy courts that handle most or all of such cases. The information available in bankruptcy records varies, but here are some common items:

- The bankruptcy filing document, which might include the subject's government identification number; street address and primary place of business; location of principal assets of business; type of business; name of legal representative; estimated amount of assets; estimated number of creditors, liabilities, and employees; financial data; and a list of corporate shareholders
- Claim documents by creditors listing the amounts that the debtor allegedly owes
- A final accounting that shows which claims were paid
- A descriptive list of the debtor's property at the time of filing (e.g., real estate, personal property, investments, accounts receivables, etc.)

- Filings that describes the debtor's income and expenditures
- The bankruptcy plan (some jurisdictions allow bankrupt parties to reorganize businesses or participate in a debt reduction plan, as opposed to liquidating all assets)
- Details from a fraud examination if the bankrupt party was suspected of bankruptcy fraud

When checking bankruptcy court records, the fraud examiner should remember to check not only the individual or business filing for bankruptcy, but also any related businesses, principals, employees, or relatives.

Property Records

Real property records are extremely important, and in many jurisdictions, property records are relatively easy to access and contain a vast amount of information. It is common for real property records to be found at the local level of government, but some jurisdictions might keep them at a centralized location. In the United States, records of real property transactions are usually maintained at the county level, but depending on the state, might be at the state level.

Property records can identify unknown assets or reveal property transfers to relatives, friends, or other legal entities. Information contained in these records can include property address, owner name, purchase price at last transaction, legal description, value, mortgage information, lien holder, contractors who have worked on the property (if a mechanic's lien has been filed), and deed type.

Accordingly, fraud examiners can review real property records to identify the subject's main residence, land that adjoins the main residence, vacation homes, or other land.

Moreover, property records pertaining to leases and the sales or purchases of business assets might reveal an entity's income and expenses. Leases might also identify hidden relationships.

When an individual purchases real estate, he becomes a registrant in real property records, property tax records, and tax assessor records (if applicable).

Real Property Records

Most jurisdictions have a land registry office that maintains various information on real property and its owner(s). Both the level of government where these records are found and the information they contain will vary by jurisdiction, but the following information is often present:

- Documents pertaining to real estate transactions—including deeds, grants, transfers and mortgages of real estate, releases of mortgages, powers of attorney, and leases that have been acknowledged or approved
- Mortgages on personal property
- Security interests or liens on property
- Wills admitted to probate
- Official bonds
- Notices of mechanic's liens
- Transcripts of judgments that are made liens on real estate
- Notices of attachment on real estate
- Land cadaster (a registry of land surveys that specifically detail each plot of real estate in an area and may contain information about value, ownership rights, and other details)
- Papers in connection with bankruptcy
- Certified copies of decrees and judgments of courts of record
- Other documents permitted by law to be recorded
- Historical sale prices
- Residences and addresses of the buyer and seller
- Identity of the party financing the property, if applicable
- Improvements to a property

The increased awareness of identity theft has led to most jurisdictions taking measures to prevent the publication of a person's government identification number in public real estate records.

Property Tax Records

In addition, many jurisdictions assess property taxes and require parties that purchase real estate to register as a taxpayer with the jurisdiction's property tax records system. There might also be a tax assessor that keeps records on real property and owners of such property. These records can provide:

- An idea of the estimated value, for tax purposes, of the property listed
- The identity of the owner of a vacant piece of land or a piece of property, if ownership is unknown

- The name of the last person to pay taxes on the property
- Legal descriptions of property
- Delinquency status of taxes
- Names of former property owners

When searching real property and tax records, the fraud examiner should always look for any additional names listed on the documents. Frequently, the name of the attorney or notary public who verified the documents is listed, providing another potential source of information.

Commercial Searches

Many commercial database vendors compile and provide access to real property records, and fraud examiners can use these databases to obtain real property information. However, the fraud examiner should make sure that the data vendor is actually active in the jurisdiction where the records are sought. Additionally, some jurisdictions are known for keeping unreliable property records, which can make property records searches difficult or impossible.

Business (Corporate) Filings

Basic business organization—whether for businesses with a single owner or large corporations—is generally governed under the laws of the country in which the entity is organized. Most jurisdictions require business entities to file various types of records that contain information that might be useful in a fraud examination, and generally, such filings are available to the public.

Organizational Filings

If an individual wants to conduct business in a name other than his own, the law requires that he file documents to claim ownership of that name. These documents can include an entity's organizational filing.

Companies are formed by submitting some type of organizational filing to the government, which might be referred to in various ways in different jurisdictions (e.g., articles of incorporation, corporate constitution, corporate charter, etc.). These company records are generally public records and will include:

- Corporate name
- Ownership information
- Nominal stock value
- Names of initial shareholders
- Names of the directors and officers
- Registered agent
- Location of the principal office
- Date of incorporation
- Standing/status

This information will permit the investigator to review a corporate structure, identify the registered agent, and trace incorporation dates. The records will often include limited partnership information as well. The examiner can also use these records to verify the jurisdiction in which a company is registered as a corporation.

Most jurisdictions require that foreign corporations (corporations which were incorporated in another jurisdiction) be registered with the domestic business organization agency if the foreign corporations transact business in that jurisdiction. For example, if a corporation that was chartered in Country A wishes to transact business in Country B, it must create a business organization filing in Country B.

Tax-Related Filings

Generally, tax records, including tax returns, are private. In most countries, including the United States, corporate tax returns are not public records. In fact, among countries in the Organisation for Economic Co-operation and Development (OECD), only Japan, Norway, Sweden, and Finland provide some form of public access to corporate tax returns.

Nevertheless, it might be possible to obtain tax information about businesses, especially publicly traded ones, without having access to their returns. In general, publicly traded companies must file regular statements with government securities agencies, and such records, which are often made public, can provide information on a company's tax filings.

Law enforcement officials might be able to gain access to corporate, business, and personal tax returns. These records might unwittingly reveal hidden assets or investments. Loans to or from officers, stockholders, or related entities should be examined closely. Also, mortgages, notes, and bonds shown as liabilities on a corporate return should be investigated.

In addition, some tax revenue departments require certain businesses to obtain licenses or permits, such as a sales tax permit. The licenses and the applications are often public record. If the business is delinquent in the payment of its taxes, the relevant tax investigator or collector might be able to provide inside information concerning the business.

Other Agency Records

There are several other government agencies or associations that perform similar functions that are useful for gathering information on businesses, other organizations, and individuals.

Records of Secured Transactions

Commercial filings are records that can help fraud examiners identify personal property that an individual or business has financed. Banks, finance companies, and other lenders will generate records or recorded filings of financial transactions conducted with individuals and businesses, such as purchases of household furniture, appliances, boats and yachts, automobiles, aircraft, and business equipment. To secure repayment, the financing party retains an interest in the debtor's property. This interest is referred to as a *security interest* or a *charge*, depending on the jurisdiction. To document this interest, the creditors might create a commercial filing, which will be publicly searchable in some jurisdictions. In jurisdictions where commercial filings are not public record, access might be restricted to those who have a relationship with the debtor or creditor.

These filings might help to identify:

- Name(s) of the debtor or joint debtors
- Current address of the debtor
- Name of the financial lender or creditor
- Type of collateral pledged as security
- Date of filing and continuations

Commercial filings and supporting documents can help fraud examiners uncover hidden ownership or relationships between parties by viewing the names of all listed debtors and their addresses. The fraud examiner might find information linking individuals to the companies they own or discover information about a company's subsidiaries, branch offices, or parent company. Additionally, discovering financed assets can reveal information about a person or organization's financial condition.

Commercial Filings in Common Law Jurisdictions

Many fraud examinations involve parties or assets in foreign jurisdictions, and commercial filing searches might be useful. However, the availability of such searches largely depends on whether the relevant jurisdiction is a common law or civil law country.

The majority of countries in which commercial filings are publicly searchable are common law systems. In these jurisdictions, a government agency typically maintains a register of commercial filings where defined items of personal property with security interests must be registered. The purpose of these filings is to put purchasers of personal property on notice if the property is subject to a security interest.

The method of searching these records varies by jurisdiction, but usually is done through the agency that maintains the records. Records are typically searched by the debtor's name or the organization's title. Here are examples of how searches are performed in a few countries with public commercial filings:

- Australia: The Personal Property Securities Register, maintained by the Australian Financial Security Authority, provides a database where details of security interests can be searched.
- Bermuda: A public "register of charges" is available to search filings of charges against assets of a Bermudian company or located or created domestically.
- Canada: Each common law province and territory in Canada passed a version of legislation entitled the Personal Property Security Act to govern commercial filings, and commercial filings are searchable at the provincial or territorial level.
- United Kingdom: Certain businesses are required to register charges against their assets through the "Registrar of Companies," maintained by the Companies House.
- United States: The Uniform Commercial Code (UCC) governs commercial filings. UCC filings are maintained and searchable at the state level by each secretary of state.

As with most public records, there are also commercial vendors who organize and provide searches of such records.

Searching Commercial Filings in Civil Law Jurisdictions

Civil law countries rarely have a public registration system for commercial filings. Security interests in civil law systems might involve filings, but they are typically not public information. Commercial filings in these countries are typically private agreements between the creditor and debtor. When commercial filings are maintained, they usually are not in a

centralized database, so searching on a broad scale is not feasible. Generally, access to commercial filings in civil law countries will be restricted to those with a relationship with the parties involved in a past or potential transaction.

Also, unlike the filings in most common law countries, the filings in civil law countries are usually against the asset and not the person or entity.

Regulatory Securities Records

Documents submitted by public companies and others who are required by law to file with securities regulators might contain valuable information. While jurisdictions treat the concept of securities differently, governments or self-regulatory bodies generally set rules for the issuing and trading of certain types of securities. Among the most common and important rules are disclosure requirements for companies with publicly traded securities. These rules are designed to make sure that investors are reasonably informed about stock that they purchase.

Beyond helping investors, these disclosures typically are made public, and they can provide a wealth of information about the filing company, including its type of business, history, organizational structure, auditor, balance sheets, and income statements.

Different securities regulators have varying disclosure requirements, but these records might include the following information:

- Corporate financial statements
- Identification of officers and directors
- Identification of significant owners (e.g., those with more than 10 percent of a business's stock)
- A description of the registrant's properties and businesses
- A description of the significant provisions of the security to be offered for sale and its relationship to the registrant's other capital securities
- Identification of events of interest to investors
- Identification of accountants and attorneys
- A history of the business

Fraud examiners should keep in mind that if a public company does not report to its domestic securities regulator, it might still be registered with regulators of foreign exchanges. Even if the company has minimal or no presence in the foreign jurisdiction, it might still be

registered there to benefit from foreign investment. Therefore, searching multiple exchanges might be necessary for conducting a thorough securities records search.

In the United States, companies with publicly traded securities are required by law to file with the Securities Exchange Commission (SEC). SEC filings are public, and they may be obtained from EDGAR (Electronic Data Gathering, Analysis, and Retrieval). EDGAR is a system that collects SEC filings, and it performs automated collection, validation, indexing, acceptance, and forwarding of SEC filings.

Employee/Labor Department Records

A country's department of labor or equivalent agency typically maintains information concerning labor arbitrations, collective agreements, and other labor records, and many of these records might be public.

Professional Associations and Licensing Boards

Many government agencies or professional bodies maintain records identifying individuals holding special licenses or memberships. These can include:

- Medical practitioners, such as doctors, dentists, and nurses
- Social workers
- Attorneys
- Certified Public Accountants or Public/Chartered Accountants
- Real estate licensees
- Notaries
- Law enforcement personnel
- Firefighters
- Security guards
- Stockbrokers
- Teachers
- Insurance agents
- Private investigators
- Bail bond agents
- Travel agents
- Barbers and cosmetologists
- Contractors, engineers, electricians, and architects

Also, the regulatory or licensing agency might have the authority to suspend or revoke the licenses necessary for the business to operate.

Many professional organizations maintain their own listings of members or licensees. However, they might be reluctant to provide information beyond the person's name and current standing in the association.

Other Regulatory Agencies

At the regional or federal level, the following records may also be found:

- Auto licenses, auto transfers, and sales of vehicles
- Civil service applications
- Driver's licenses
- Health department records
- Inheritance and gift tax returns
- Name changes
- Occupancy and business licenses
- Parole officers' and probation departments' files
- Personal property tax returns
- School and voter registrations
- Regional income tax returns
- Welfare agency records

Nonpublic Records

Types of Nonpublic Records

As previously stated, *nonpublic records*—information about a person or business that is considered to be private and confidential—might be needed in some fraud examinations. Some of the most valuable types of nonpublic records include:

- Banking records
- Tax records
- Credit records of individuals (but not business credit reports, as this information is generally not protected)
- Phone records
- Credit card account records
- Personal health care records

Banking Records

Bank records are perhaps the single most important external source of financial information available to a fraud examiner. However, they typically require consent or a legal order to obtain. In addition to their use as evidence for fraud, banking records might provide leads on a subject's sources of funds, expenditures, and personal affairs. These records help the fraud examiner construct a paper trail to prove the fraud.

Some of the types of banking records that should be reviewed, if available, are:

- Account opening documentation
- Monthly account statements
- Checks written on the account
- Loan files
- Safe deposit box records
- Currency transaction reports
- Bank collection department records
- Mortgage loan files

Tax Records

Tax records might provide indirect evidence of illicit payments, such as profits or losses from business ventures that a suspect has not informed fraud examiners of, or interest and dividends on hidden certificates of deposit and bank accounts. Such records might also show deductions and expenses, such as real estate taxes, which could lead to previously unknown funds or assets. Government investigators generally have broader access to these documents, while private parties will usually have to obtain the subject's consent or take legal action to obtain them.

Credit Records of Individuals

The ability to store large volumes of data digitally spawned an entire industry of parties who process and disseminate information about individuals and organizations. Practically all lines of business have specialized credit-reporting associations that can provide credit information on individuals and businesses, including trade information, designation of lenders and creditors, types of businesses, date accounts were opened, terms of payment agreed upon, highest credit, balance owed, and paying habits. Some credit reports also give the name of the bank the subject does business with and the size of the subject's accounts.

Credit reports and personal data are provided by third-party vendors that go by various names depending on the jurisdiction, such as "credit reporting agencies" or "data controllers." These agencies are local, national, or global institutions that collect data from various sources on individual consumer creditworthiness or other information and report that data to their members or subscribers. In the United States, the third-party vendors that collect credit information are known as credit reporting agencies, and most consumer (i.e., individual) credit information is collected and maintained by three national credit reporting agencies: Equifax, Experian, and TransUnion. Generally, a subscription is required to obtain information from the three national credit reporting agencies, and because the big three agencies do not share data among themselves, there will be differences between the records from each credit bureau.

In the case of consumer (individual) credit records and personal data, a growing number of jurisdictions regulate both how such information is collected and stored, as well as who may access this information and for what purpose. In many cases, the consumer must be notified and must consent to the use of the report. Members of the European Union have especially strong data privacy requirements and require foreign parties who are requesting personal data about individuals within the European Union to verify that the information will be properly managed.

The United States also regulates credit records, and the dissemination of credit information is governed by the Fair Credit Reporting Act (FCRA). The FCRA places restrictions on when a consumer credit report can be obtained and used. In many cases, the consumer must be notified or must consent to the use of the report for employment purposes.

In jurisdictions that regulate credit information and personal data, a fraud examiner will generally need a legally acceptable reason for accessing such information from third parties. However, simply suspecting an individual of fraud is generally not sufficient grounds for obtaining credit and personal data regarding the person from a reporting agency or data controller. The specific exceptions for allowing the processing and dissemination of credit and personal data vary, but some common circumstances include when:

- The individual has given consent.
- It is necessary for the extension of credit or to enter into a contract with the subject.
- It is necessary to protect the subject's vital interest.
- It is necessary to comply with other legal requirements.

- An employer is conducting a background check for hiring or other employment purposes (consent is still required in many jurisdictions).
- It is necessary to serve the public interest.

Credit reporting agencies typically maintain the following information:

- Consumer information, such as address, age, family members, employers, income levels, length of employment, the extent of other obligations, and the like
- Account information, such as payment schedules, items purchased, defaults (if any), and buying habits
- Marketing information, such as customers broken down by age, sex, income levels, and other classifications
- Information on current and former employers

Information on a business organization's creditworthiness may also be obtained from credit reporting agencies. The responses for such searches might include payment trends from creditors, public records, banking information, and key facts as to the type of business and ownership. But unlike consumer credit information, business credit information is generally not subject to legal protections.

Generally, credit-reporting agencies obtain their information from the following sources:

- Consumers, primarily from filling out application forms for credit
- Public records, which provide information on bankruptcies, court judgments, foreclosures, divorces, criminal convictions, and registered agreements
- Major credit grantors and collection agencies, which, as subscribers, regularly send their credit files electronically to the credit bureaus, resulting in files that include the account number, outstanding balance, and an indication of whether a payment was made on time

Many credit grantors and collection agencies only report payment information, and some creditors, like utility companies, only report delinquent activity.

Phone Records

Telephone records can provide valuable insight into fraud examinations. For example, telephone records might provide contacts with real estate brokers or sellers, identify charge calls from vacation spots or contacts with co-conspirators, or provide other leads to assets and expenditures.

Generally, a person's private phone lines, such as home phone and personal mobile devices, will be considered private. Therefore, to access the records for these lines, investigators will need consent from subjects, a warrant or subpoena, or another legal order.

Some phone records, however, might be accessible. For example, if a fraud examiner is conducting an internal investigation and the employer keeps business phone records, the fraud examiner might not have to obtain permission or a legal order to access these records. Whether the records are private will depend on the facts and the laws of the relevant jurisdiction. Often, the expectation of privacy regarding business phone records can be eliminated by having the employee sign a document upon being hired that acknowledges that phone calls, other electronic communications, and metadata may be recorded and reviewed by the employer. However, this may be prohibited in some jurisdictions, so employers should consult with legal counsel.

Credit Card Account Records

Credit card account records can be helpful when conducting a fraud examination. Credit card receipts will track the subject's travels and expenditures. An extremely high balance on a credit card might indicate a motive for the crime or provide circumstantial evidence of hidden income. Even modest credit card charges might provide leads to identifying hidden assets (e.g., charges for boating supplies purchased at a marina might indicate a need for further investigation to determine whether the subject owns an expensive boat).

Personal Health Care Records

Health care records are valuable in several types of fraud cases, particularly those involving insurance or false claims regarding medical goods and services. They can also be relevant to a person's financial situation. However, unless the fraud examiner has the subject's consent or is in a special position to access health care records (e.g., as an employee of a medical provider), this information is often not available without a legal order.

Gaining Access to Nonpublic Records

Nonpublic records are not available to the public and, therefore, might be difficult to obtain. Despite the limitations on obtaining personal records, fraud examiners might be able to obtain nonpublic records by using one or more of the following methods.

Requesting the Records

The simplest way to obtain relevant documents is to request them. This usually works for fraud examiners representing large organizations that are important customers to the party with the information. Vendors and other customers of the company conducting the investigation might cooperate voluntarily if they have nothing to hide (or think that incriminating evidence cannot be found) and are anxious to maintain good relations with the company. A subject can consent to produce the records or execute a written consent for the fraud examiner to obtain such records from banks, credit agencies, or the taxing authority.

Consent

If might be possible to obtain nonpublic records through consent from the entity to whom the records pertain. Although unlikely, a target might voluntarily produce certain records (e.g., if he is innocent, thinks he is innocent, or thinks the investigators will not find relevant evidence in such records) or execute a consent to obtain such records from banks, credit agencies, or the government.

Subpoena or Other Legal Processes

Subpoenas and other legal processes, such as depositions and document requests, are available if a civil or criminal action is filed. For example, a wronged organization may file a civil or administrative action or make a criminal referral so that records can be subpoenaed or obtained by a legal order (e.g., a search warrant). In a civil case, both private and public parties may obtain records such as bank accounts, brokerage accounts, travel, credit card, credit agencies, and telephone toll records by subpoena or other legal order.

However, records obtained while executing a search warrant or similar legal order usually are available only to the government during the underlying investigation, and perhaps thereafter if not disclosed at trial. In addition, law enforcement agencies may also subpoena records, but, depending on the jurisdiction, might not disclose the contents of such records with the victim or third parties.

In most jurisdictions, third-party organizations that maintain nonpublic records, such as banks and hospitals, are usually prohibited from revealing such records without express authorization from the subject or a legal order.

Demand as a Condition of Continued Business

Similarly, an organization may demand that a supplier, vendor, or agent turn over relevant documents as a condition of continued business. Taking this action is legal, in appropriate circumstances. Of course, management and counsel should be consulted before such demands are made, particularly if the other party has a contractual relationship with the demanding organization.

Exercise Audit Clause Rights

An audit clause allows parties to a contract the right to access another party's books. Thus, absent subpoena power, fraud examiners might need to use audit clause rights to access contractor and subcontractor records and financial accounts.

Unfortunately, most audit clauses are too narrow to provide useful information. However, if properly constructed, an audit clause can be a powerful method by which on-book information can be obtained.

Improper Pretexting

Fraud examiners should not conduct a search of the sources of information without being familiar with the privacy laws of the relevant jurisdictions. Being familiar with privacy laws, however, can be difficult because jurisdictions approach privacy in different ways. There are some legal issues that fraud examiners should determine at the outset of a case.

One method that fraud examiners should be particularly cautious with is pretexting, which is a criminal offense in some circumstances. Broadly defined, *pretexting* is the act of impersonating someone else or making false or misleading statements to obtain, sell, or buy information about a person or organization. Under the broad definition, pretexting for non-fraudulent purposes is not always illegal, but it should be used with caution. For example, if a fraud examiner is trying to locate a witness or a suspect, he might call the person's relative and pretend to be an old friend who is requesting the individual's phone number. This type of pretexting might be permissible. However, it is more often illegal to use pretexting to obtain certain types of information, such as financial records and phone history records.

Several jurisdictions have prohibited pretexting against financial institutions, even if no fraudulent intent is present. In the context of financial institutions, pretexting is the act of obtaining or attempting to obtain customer information from financial institutions through these deceptive tactics. Some individuals used pretexting as a means to gather financial

information about a subject. Pretexters would contact a financial institution and pretend to be the customer or someone else authorized to obtain financial information and basically trick the financial institution into providing information about the subject.

Fraud examiners should not impersonate a member of law enforcement, nor should they impersonate an actual person (particularly the individual being investigated). To do so may lead to charges of identity theft. Before engaging in any type of pretexting activity, investigators should consult with legal counsel to determine whether the information sought is protected by the laws of the jurisdiction, as well as whether the planned impersonation method is legally acceptable.

Other Non-Government Sources

Associations and Lobby Groups

Associations and lobby groups have information about their member firms. Two of the best sources are the Better Business Bureau and the chamber of commerce.

Better Business Bureau

A number of Better Business Bureaus are located throughout the globe. They are sponsored by local businesses and offer a variety of services, including background information on local businesses and organizations. The bureaus generally keep information about criminal rackets, cons, and their operators and can provide information about the business reputations of local groups.

Chamber of Commerce

A government's chambers of commerce generally have directories of local businesses, and they also have information regarding reputations of local businesses and operators. Chambers of commerce might be organized by community, city or town, region, state, or nation.

Abstract and Title Companies

Often, abstract and title companies maintain records of individual transactions, and they typically publish and distribute papers to attorneys, real estate brokers, insurance companies,

and financial institutions. These papers contain information about transfers of property, locations, mortgage amounts, and release of mortgages.

Bonding Companies

Bonding companies provide bonding services, including surety bonds, license bonds, permit bonds, bid bonds, and so on. To become bonded, an entity will have to submit an application for a bond with a bonding company. The application for a bond contains the applicant's (person or firm) financial statement and data. The information contained in a bond application is essentially the same information that is required in loan applications (though in greater detail).

Credit Card Records

Credit card records often contain valuable information concerning the individual debtor, but laws and regulations must be checked before obtaining these records. Information on expenditures can be obtained from firms such as MasterCard, American Express, Diners Club, Discover, and Visa. This information usually requires a subpoena or court order.

Stockbrokers

Stockbrokers maintain client information in a manner similar to financial institutions, especially those who have margin accounts. They maintain records of transactions for all clients. These records are generally private, but can be obtained with a legal order, if relevant to litigation.

Western Union

Western Union is a non-bank money transfer provider, and it stores records for paid money orders in Minneapolis, Minnesota. These records contain the original telegram, by purchaser or sender, and bank drafts by Western Union. Western Union retains orders for less than $1,000 for two years and orders of $1,000 or more for six years. For private parties, these records will require a legal order to obtain.

Vehicle History Checks

In many countries, individuals can conduct vehicle history checks to find out various details about a vehicle's past. A vehicle history check might show the following information about a vehicle:

- When its inspection expires
- The date it was first registered
- Its color
- Its engine size
- Its year of manufacture
- Whether it has been reported as stolen
- The number of previous owners
- Whether it has any odometer discrepancies

International Air Transport Association

The International Air Transport Association is an international industry trade group of leading airlines, and it has information on all international matters dealing with aviation security, including counterterrorism efforts worldwide. It also monitors and attempts to prevent fraud against airlines, such as ticket fraud.

International Foundation for Art Research

The International Foundation for Art Research (IFAR) is a nonprofit organization established in 1969 to help prevent the circulation of forged and misattributed works of art. IFAR offers an authentication service to help resolve controversies concerning the authenticity of works of art. IFAR also publishes quarterly journals on authentication research, art law, theft and recovery, and an extensive listing of recently reported stolen and missing art and antiques. The IFAR's website is www.ifar.org.

International Association of Insurance Supervisors

The International Association of Insurance Supervisors (IAIS) is a voluntary organization of insurance regulators and supervisors from more than 200 jurisdictions in nearly 140 countries. The IAIS seeks to promote effective and consistent supervision of the insurance industry to foster safe and stable insurance markets and global financial stability.

Accessing Information Online

Fraud examiners now have a number of online investigative resources available through their personal computers. Not so long ago, fraud examiners had to travel to a physical location to search for public records. Fraud examiners today, however, have enough information

available through different online sources to conduct entire inquiries without leaving their computers.

A great deal of information can be accessed through the Internet for little or no cost, and this discussion focuses on ways fraud examiners can use the Internet to obtain information about assets, people, businesses, and fraud in general. Specifically, this discussion outlines a five-step approach to using the Internet in fraud examinations and touches on finding information online using search engines, databases, the deep Web, the Internet archives, and social networking sites; using online sources to conduct specific types of searches; using newspaper/media databases to find information online; and using other nontraditional methods for finding information on the Internet.

Five-Step Approach to Using the Internet in Fraud Examinations

The following is a five-step approach for using the Internet in fraud examinations:

- Compile everything known about the subject (e.g., name, age, national identification number, current address, past addresses, phone number, employer, family members, marital status, and hometown).
- Conduct searches on major search engines.
- Search social networking sites.
- Analyze data to identify leads for guidance on which items to focus on in subsequent searches.
- Investigate each lead using search engines and other online sources, separating out those that seem valuable, those that require more development, and those that should be eliminated.

Using Internet Search Engines to Find Information

The most basic way to find information on the Internet is to execute searches using search engines or metasearch engines.

Search Engines

Search engines are programs that search websites and documents for specified keywords and return a list of sites and documents where the keywords were found. For instance, if a user searches for the keyword *fraud,* the search engine will return a list of sites and documents related to fraud (such as the Association of Certified Fraud Examiners website, located at www.ACFE.com).

To provide such tools, search engines have automated robots, called crawlers or spiders, that systematically browse the World Wide Web to index the contents of the Internet to facilitate fast and accurate information retrieval.

Although search engines are one of the most basic ways to find information on the Internet, they can be erratic in the information they return; what is more, fraud examiners must verify all information they obtain through the Internet.

There are several prominent search engines on the Internet, and each functions in a different way. A few of the more popular engines are described here.

GOOGLE

Google is the most-used search engine in the United States, and it has advanced search capabilities. When a user conducts a Google search, the search engine's software ranks individual Web pages according to how often the page is linked to by others, determining the page's "importance" by the number of links and the identity of the linking page. It also uses information it gathers about the user, such as location, to predict what the user wants and prioritize the list of search results. Google is a good source for finding targeted information on a particular topic. Additionally, learning Google-specific search operators will provide the investigator with an extremely powerful tool for online investigations.

BING

Bing (formerly Live Search, Windows Live Search, and MSN Search) is the current Web search engine from Microsoft. Bing automatically groups search results in different categories, depending on the type of searches users are conducting. Bing also provides the ability to save and share search histories via Windows Live SkyDrive, Facebook, and email.

In addition to providing many of the same search resources found in other popular engines (e.g., it provides searches specific to travel, video, pictures, and maps), Bing has several useful features. For example, Bing maintains an ongoing history of searches, giving researchers a way to identify what they looked up and in what order. And Bing's image search is easier to manage than others because it displays more images on the results screen. The Bing search engine also powers the Yahoo! Search function.

ASK.COM

Formerly AskJeeves, Ask.com is a good site for beginners and for general queries. The engine leads users through questions to help narrow the search, and also searches six other search sites. (For similar services, see the section on metasearch engines that follows.) Ask.com's ability to interpret natural language makes it easy to use, though constructing precise queries can be difficult for the same reason.

DUCKDUCKGO

DuckDuckGo is an Internet search engine that uses information from crowdsourced websites to obtain its results. Unlike other search engines, DuckDuckGo does not record user information, does not generate search results based on a user's previous interests, and is not cluttered with ads.

Metasearch Engines

Metasearch engines are programs that send user requests to several search engines and display the results. Some of the more common metasearch engines are described here.

DOGPILE

Dogpile sends a query to a customizable list of search engines, directories, and specialty search sites (e.g., Google, Yahoo! Search, Bing, Ask.com) and then displays the results from each search engine individually. Once the results are retrieved, the innovative metasearch technology used by Dogpile goes to work removing duplicates and analyzing the results to help ensure that the best results top the list. The Comparison View feature lets users compare results from the leading engines with the click of a button.

MAMMA

Mamma is a "smart" metasearch engine; every time users type in a query, Mamma simultaneously searches a variety of engines, directories, and content sites; properly formats the words and syntax for each; compiles their results in a virtual database; eliminates duplicates; and displays them in a uniform manner according to relevance.

SPUTTR

Sputtr uses metasearch technology to search the Internet's top search engines and standalone websites, including Google, Yahoo! Search, Bing, Ask.com, Twitter, Facebook, Youtube, and others.

Advanced Search (Boolean) Operators

Although search engines return results instantly and with little effort, the simplicity of these tools often removes the benefits of more complex searching techniques. Thus, to tap the Internet's information sources, fraud examiners must know how to construct proper queries; that is, fraud examiners have to know how to ask for what they want. All search engines have limitations, but the most serious impediment to locating good information is the user's lack of search skills.

The best way to use a search engine is to use two, or possibly three, keywords that best describe the topic; but often, such searches will return too many or irrelevant results, and in such situations, users can employ advanced search operators (or Boolean operators) to gain more control over the search results. *Advanced search operators* are query words or symbols used in search engine queries to instruct search engines to perform special actions when executing a search. Advanced search operators increase the precision of a search phrase. They help search engines better understand exactly what the user is looking for, and they improve a search and return relevant links faster. By using search operators, users can get more accurate search results and reduce the time it takes to find relevant sources.

Different search engines operate differently, and therefore, search engines use different search operators. To determine a search engine's advanced search capabilities, consult its service's FAQ or search help page.

This section examines the advanced search features of Google and Bing because they provide some of the most robust and useful tools for fraud examiners conducting online searches.

GOOGLE OPERATORS

The following is a list of Google search operators. Note, however, that the list includes operators that are not officially supported by Google and are not listed in Google's online help. In addition, Google might change how certain operators work, or it might do away with them completely.

Operators	Search Results	Example
OR (all upper case)	Placing OR between two words will return pages containing either one, several, or all of the search terms.	[fraud OR Ponzi] will return pages in which either one or both of the words *fraud* or *Ponzi* appears.
AND (all upper case)	Placing AND between two words will return pages containing both terms.	[budget AND report] will find pages with *budget* and *report*.
""	Placing quotation marks around a word or set of words will return pages containing the exact word or set of words.	["holy cow"] will return pages in which the exact phrase *holy cow* appears.
-	Placing the minus sign before a word will return pages that do not contain the term.	[fraud -Ponzi] will return pages in which the word *fraud* appears but will exclude references to Ponzi.
define:	Placing define: before a keyword will return definitions for the particular term.	[define:fraud] will show definitions for *fraud*.
site:*URL*	Using a keyword and placing site: before a URL will return pages in which the URL contains the keyword.	[fraud site:virtuallibrarian.com] will return pages on virtuallibrarian.com that contain fraud.
filetype:	Using a keyword and filetype:*suffix* will return items of a particular filetype that match the keyword.	[fraud filetype:pdf] will restrict the results to PDF files with the term *fraud*.
link:	Using link:*URL* will return pages that link to the specified URL.	[link:virtuallibrarian.com] will return pages with links to virtuallibrarian.com.
intitle:	Using intitle:*term(s)* returns sites containing the term in their title.	[intitle: mortgage fraud] will return only documents that contain the words *mortgage* and *fraud* in the title.
allintext:	Using allintext:*term(s)* returns pages containing all the search terms in their text.	[allintext: fraud skimming materiality] will return only pages in which the words *fraud*, *skimming*, and *materiality* appear in the text of the page.

*	Using an asterisk (*) within a query will allow Google to treat the asterisk as a placeholder for one or more unknown words.	["fraud * alert"] tells Google to find pages containing a phrase that starts with *fraud,* followed by one or more words, followed by *alert.*
AROUND(n)	Using AROUND(*n*), where *n* is an integer, between two terms will return pages where the terms are within a certain number of words of each other.	[fraud AROUND(3) alert] will limit the results to those pages where *fraud* appears within three words of *alert.*

In addition, Google operators can be combined. For example, the query [site:hp.com filetype:pdf "5010 LaserJet" printer FAQ] will search for an Adobe Acrobat PDF file of frequently asked questions regarding the 5010 LaserJet printer located on the Hewlett Packard website.

There are numerous other operators and search techniques that work with each Google search service. A good resource for lesser-known Google operators and search tips is www.googleguide.com.

BING OPERATORS

Although Bing and Google share some of the same search resources (e.g., quotation marks, minus sign, OR, AND, site:, filetype:, and intitle:), Bing has search operators that are unique to its search capabilities.

Operators	Search Results	Example
contains:	Searches for pages where there's a hyperlink to a file with the extension	[swimming dolphin contains:wmv] will find wmv clips of dolphins swimming.
inanchor:	Returns pages that contain the specified terms in the link anchors of Web pages	[inanchor: useful fraud sites] searches for pages that are called useful fraud sites by others.
inbody:	Restricts results to those containing all the search terms specified in the body	[inbody: securities fraud] will return only documents that contain the words *securities* and *fraud* in their body.

ip:	Finds websites hosted by a specific IP address	[IP:198.46.34.22] finds websites hosted by the specified IP address.
prefer:	Adds emphasis to a search term to help focus the search results	[fraud prefer:Ponzi] specifies the type of fraud that the user wants to find.
url:	Using a keyword and placing url: before a URL will return pages in which the URL contains the keyword	[url:virtuallibrarian.com fraud] will return pages on virtuallibrarian.com that contain fraud.
NOT (all upper case)	Placing NOT before a word will return pages that do not contain the term	[fraud NOT Ponzi] will return pages in which the word *fraud* appears but will exclude references to Ponzi.
near:(I)	Using near:(n), where *n* is an integer, between two terms will return pages where the terms are within a certain number of words of each other	[fraud near:3 alert] will limit the results to those pages where *fraud* appears within three words of *alert*.

Additional Tips When Using Internet Search Engines to Find Information

The following is a list of additional tips and guidelines for searching the Internet for information:

- Use more than one search engine. Everyone has their favorite search engine, but relying on one search engine is not sufficient because every search engine collects and catalogues information differently.
- Be clear about what is being looked for. Define the search topic as clearly and succinctly as possible.
- Use unique, specific keywords. Be specific when entering search terms.
- Use nouns for keywords.
- Use format terms (e.g., transcript, document, report, statistics, pdf, policy, dictionary) in addition to subject words.
- Exclude articles (e.g., a, an, the) and pronouns (e.g., he, she, it, they) from search terms, unless they are part of a key phrase.
- Use correct spelling and include alternative spellings (e.g., colour and color).
- Use filters to focus searches. Filters tell search engines to screen out specified types of pages or files.

- Check all the tips and features of any search engine to be used and make use of them.
- Increase the number of results displayed per page.
- Customize searches using advanced search operators, such as the minus (-) operator and quotation marks, to narrow the search results.
- Search for phrases. Search for a sequence of words in a specific order, using quotation marks around the phrase.
- Search for base words (drop suffixes) to avoid excluding relevant pages.
- Use metasearch engines if early searches are unfruitful.
- Set a time limit for searching, and when that amount of time has elapsed, stop and try another method.
- Use a browser's find feature to find a word or phrase on a Web page and help navigate search results.

Using Online Databases to Find Information

Any public records search should include searches of online databases.

Sources of Public Records

Public records can be obtained from a number of online databases. Typically, public records can be searched online through governmental agency websites, public record vendors' websites, and investigative service companies.

GOVERNMENT SOURCES

Many governments provide access to databases available through their websites, and these databases are numerous and varied. Government databases compile records from various levels, and most can be readily accessed from a home computer after subscribing to their services. The costs associated with these databases can be equally varied. There are several access options available, and a fraud examiner should be prepared to use any and all, separately or in combination. Keep in mind, however, that it might be necessary to spend time examining the actual documents to get the whole picture.

In the United States, for example, various state and federal government agencies are repositories of public records and provide access to the records. The types of records maintained by government repositories include state government records, lobbyists' records, Securities and Exchange Commission (SEC) records, and federal government contract information. The problem for those performing public record searches, however, is that the

records are spread among federal agencies, separate states, and different levels of government within states (i.e., local, county, and state levels).

PUBLIC RECORD VENDORS

Additionally, fraud examiners can search public records using public record vendors with proprietary databases. Unlike public databases available through governmental websites, public record vendors generally contain a broad range of information that can be searched from any location. Public record vendors usually contain such diverse information as court records, real estate records, lien records, corporate records, and telephone listing information.

Because public record vendors provide access to diverse information, fraud examiners can use them for many different types of searches. These databases can also uncover specific records from multiple jurisdictions in a short amount of time.

Although public record vendors generally do not provide any more information than can be accessed from other sources, they have two distinct advantages—search speed and constant access.

Generally, accessing information held by public record vendors is not free, and these companies use different pricing structures. Public record vendors might charge an initial access fee, monthly membership fees, or a one-time access fee, and some operate on a "pay as you go" principle that allows users to pay only for the searches they conduct. Therefore, it is important that fraud examiners shop around to get the best deal for their level of usage.

Furthermore, those performing public records searches should be fully informed about public record vendors. First of all, many of their records are incomplete because not all government bodies allow the vendors open access to certain records, such as criminal records. Therefore, turning up no convictions in a public data vendor search does not necessarily mean that the person has no criminal history. Additionally, the information on these sites can be inaccurate, out of date, or otherwise incomplete. In addition, some public data vendor websites are just scam operations that will charge for bogus searches.

The bottom line regarding public data record sites is that the person conducting a search needs to confirm the legitimacy of the site by reading reviews, articles, and so forth. Second,

given that some records are not available, search conductors should attempt to collect public records from original sources when possible.

There are several companies that provide varying levels of public record information, and a description of some of these companies and the records they provide are discussed later.

INVESTIGATIVE SERVICE COMPANIES

There also are many investigative service providers that offer various services for public records searches, and for some practitioners, it might be economical to enlist the aid of service companies, information brokers, and professional online investigators. These companies will conduct research for fraud examiners, typically using online and physical sources. Although the cost of using the services of such companies will be higher than using a public records vendor, the entities might be the best choice for those who sporadically conduct public records searches.

Limitations of Online Public Database Searches

Despite the advantages of using online databases to find information, online databases have some downsides as well. For one thing, a public records database will tell the researcher whether a particular record, or some of the information contained in that record, exists, but generally, such databases will not provide a copy of the actual public record. For example, a fraud examiner can conduct a property record search to find out that John Doe owns the property at 7/25 Adelaide St., Brisbane City, QLD 4000 Australia; however, if he needs a copy of the actual deed, he will have to retrieve it from the appropriate government office.

For another thing, there is a wealth of information now available through public record vendors, but accessing information online is never a full substitute for an examination of the public record itself. Such companies have to get their information from somewhere, and often, their records come directly from the government. But if the information in the government's records was incorrect, it will be incorrect in the public record vendor's database as well.

Also, if a fraud examiner accesses certain types of personal information through an online service, he might be subject to laws that govern the collection, dissemination, and use of consumer credit information. For example, in the United States, the Fair Credit Reporting Act (FCRA) prohibits consumer reporting agencies from releasing personal information about an individual (e.g., information about the consumer's character, general reputation,

personal characteristics, or mode of living) to third parties without authorization, and it limits disclosure of consumer credit information, such as a subject's credit history, to third parties.

Thus, before accessing such information, fraud examiners should always consult with counsel.

The following is a brief list of several limitations of conducting searches for public records using online databases, including:

- Online coverage of public records varies widely from jurisdiction to jurisdiction, and therefore, there are many degrees of accessibility to public records between jurisdictions.
- Online public records searches are limited in the area they cover. Therefore, when looking for information on a subject, fraud examiners often must search for public records in multiple jurisdictions.
- Often, online public records are brief abstracts of the original public record.
- The source of the information compiled in an online database must be reliable.
- Fraud examiners must validate information retrieved from online databases to determine if it is accurate and up-to-date.
- The public records compiled in an electronic format might cover only a limited period.
- Online searches can be erratic in the information they return.

Popular Public Record Database Vendors

There are a number of commercial database vendors that offer wide access to public records. Fraud examiners can shop various services to find the one that meets their needs in the most cost-effective manner. In some instances, it might be necessary to use more than one service to get accurate and complete information. These companies get their information from various sources and on various update schedules, so a search in any one database might return different results than a search done elsewhere.

Listed below is information about some of the more commonly used commercial database vendors.

DUN & BRADSTREET

Dun & Bradstreet (D&B) is a business information service provider. D&B is probably one of the most comprehensive and diverse sources available, with facts on more than 130 million companies in more than 190 countries. D&B is renowned for products like *Business*

Information Report and *Industry Norms and Key Business Ratios,* both excellent tools. It is located at www.dnb.com.

KOMPASS

Kompass is a business-to-business (B2B) information system on companies and for companies, providing access to a database with information on millions of companies from numerous countries worldwide. Users can search Kompass to determine a company's executives, addresses, corporate structure, key personnel, turnover rate, description, product names, product services, trade names, brand names, and branch locations. Kompass is located at http://us.kompass.com.

HOOVER'S

Hoover's, a D&B company, is a one-stop reference for business information. Hoover's provides comprehensive, up-to-date business information for professionals who need intelligence on U.S. and global companies, industries, and professionals. Hoover's is located at www.hoovers.com.

SKYMINDER

SkyMinder provides public information on global markets and on millions of companies in numerous countries. It is a Web-based service that aggregates various company databases, such as those from D&B, Jordans, Thomson Financial, and Hoover's. SkyMinder also offers company credit and financial information on millions of companies worldwide. For more information, visit www.skyminder.com.

BUREAU VAN DIJK

Bureau van Dijk (BvDEP) provides a wide range of company information products, and it is one of Europe's leading publishers of electronic business information. For fraud examination purposes, the most relevant service is ORBIS, a global database with information on millions of companies worldwide. With descriptive information and company financials, ORBIS contains extensive detail on items such as news, market research, ratings, country reports, scanned reports, ownership, and mergers and acquisitions. For more information on BvDEP, visit www.bvd.co.uk.

LEXISNEXIS

LexisNexis is one of the leading electronic data firms in the world. Users can obtain access to public records, media publications, and annotated court cases and records. For more information, visit www.lexisnexis.com.

KNOWX

KnowX is a product of the LexisNexis Risk and Information Analytics Group, and it offers easily navigable public records searches in various categories, including asset searches, adverse filings, property valuation, and people- and business-locator tools. Users can also verify licenses, conduct background checks, and look up a company's history. KnowX can be found at www.knowx.com.

DCS INFORMATION SYSTEMS

DCS Information Systems is an established source for investigative information. DCS provides online investigative solutions for businesses and government—from financial institutions to law enforcement or investigators. DCS provides information comprising public records and publicly available information. Its AmeriFind online resource system is separated into three areas:

- PrimeData provides banking and finance information.
- QuickFind serves general investigations, security, and fraud prevention and detection.
- FraudTracer serves insurance fraud investigations and claims.

DCS Information Systems is located at www.dcsinfosys.com.

INSPERITY EMPLOYMENT SCREENING

Insperity Employment Screening, formerly US Datalink, is an employee background check service. Insperity is one of the only companies that use manual searches to obtain information. For example, Insperity uses its network of researchers to search local courts for the requested information, as opposed to using potentially out-of-date and inaccurate online databases that other online investigative databases use. Therefore, if a fraud examiner has the time to wait for an inquiry, Insperity might be the most reliable option. Insperity can be found at www.insperity.com/screening.

CSC

CSC is a Web-based due diligence service. It is a great database for retrieving information about businesses. CSC can produce a business's financial statements, records pertaining to corporate status, business credit, and licensing information. Commercial filings, bankruptcy, judgments, and corporate good-standing searches are just a few of their services. CSC is located at www.cscfinancialonline.com.

EXPERIAN

Experian is one of the major providers of consumer credit information in the United States, and it provides services on consumer and business credit, direct marketing, and real estate information services.

Some of the services provided by Experian include:

- Business Snapshot Reports that summarize credit histories—including payment patterns and legal filings—of small businesses or contractors.
- Precise ID with Knowledge IQ consist of scoring, analytics, and knowledge-based authentication, and it provides real-time and online validation, verification, and fraud assessment of names, addresses, Social Security numbers, dates of birth, driver's licenses, and telephone numbers.

Experian is located at www.experian.com.

EQUIFAX

Equifax is also one of the big three credit reporting companies in the United States. It sells a variety of products, including consumer credit reports, insurance reports, business credit reports, analytics, demographic data, and software. It also develops products for businesses aimed at stopping credit fraud and identity theft schemes.

Equifax is located at www.equifax.com.

TRANSUNION

TransUnion is another one of the big three credit report companies in the United States, and it offers credit information and services for consumers and businesses alike. More specifically, TransUnion is a global provider of business intelligence services with technology-based intelligence products, including innovative credit-decision and fraud-prevention tools, advanced target-marketing products, risk and profitability models, and portfolio management.

TransUnion is located at www.transunion.com.

SEARCH SYSTEMS

Search Systems is a U.S. public records directory with thousands of searchable public record databases. Its search capabilities include business information, corporate filings, property records, deeds, mortgages, criminal and civil court filings, inmates, offenders, births, deaths, marriages, unclaimed property, and professional licenses. One of its many directories, the criminal records and offenders search, has access to criminal records, and its Search Systems Premium offers instant access to bankruptcy, judgment, and tax liens. For more information, visit http://publicrecords.searchsystems.net.

WESTLAW

Westlaw is an online legal research service, and it provides access to a comprehensive and current collection of public records. Its People Finder database directory contains information on individuals compiled from numerous public sources, including telephone directories, publishers' mailing lists, change of address files, real estate filings, utility records, public demographic and consumer household data, voter registration records, driver's license data, federal and state death records, and credit header data. For more information, visit www.westlaw.com.

Using the Deep Web to Find Information

The *deep Web* (also known as the *invisible Web*) refers to Web content that is not indexed by standard search engines. There are a number of reasons why the deep Web exists. For one thing, there are places where Web crawling robots cannot enter. These deep Web resources include websites without any links pointing to them, certain file formats that search engines cannot handle, sites that have been blocked from Web crawler access, password-protected sites, and information stored in databases. Also, search engines limit the depth of their crawl on a website. Moreover, Web crawling robots cannot crawl as quickly as pages are added or updated.

Web search engines compile indices of only a relatively small portion of pages that are available on the Web, and therefore, search engines only search a small portion of the Web. In fact, estimates speculate that Google indexes less than 1 percent of the Internet. Accordingly, the majority of online resources are actually deep Web resources that users cannot access by using a standard search engine. And because search engines only search a small portion of the Web, the deep Web is an important resource for fraud examiners.

There are many sites designed to dig into the deep Web. SearchSystems.net, for example, provides access to more than 55,000 public records and legal databases worldwide.

Tor Web Browser

Some Web addresses are only accessible through the Tor Web browser. Tor is a truncated word for "the onion router," which is software that layers encrypted communications (like the layers of an onion) and offers increased anonymity to users. Tor works by bouncing users' communications around a distributed network of computers all around the world, making it difficult or impossible to determine who is requesting particular data from a website. It prevents someone who is monitoring the user's Internet use from knowing what sites the person visits, and also prevents the visited sites from learning the user's location. Sites with a .onion address are designed to only be accessible by people using a Tor Web browser.

Tor is a neutral tool that can be used for both legitimate and illegitimate purposes. For instance, a person who wanted to blow the whistle on fraud at their organization while remaining anonymous might use the Tor technology to report the issue. However, there are also many services accessible by Tor that are criminal in nature. Perhaps the most popular was the Silk Road, where users could purchase drugs and other contraband online. The Silk Road was shut down by authorities in 2013, but several other black market websites replaced it shortly after the bust (including a nearly identical site called Silk Road 2.0 that was shut down in 2014).

The Tor browser can be downloaded at www.torproject.org. The services that require Tor tend to want to remain hidden from typical Internet users, so they can be difficult to find unless a person knows what he is looking for. Additionally, the names and addresses of services change often. Users should also be cautious when exploring .onion sites, as many are scam sites or have malicious software.

Using the Internet Archives to Find Information

Fraud examiners can also search the *Internet archives*—archived versions of Web pages that have since been updated or are no longer available online.

The most popular tool for searching the Internet archives is the Wayback Machine, located at www.archive.org. The Wayback Machine allows users to see archived versions of Web pages throughout time. It contains Web pages archived from 1996 to the present.

Fraud examiners can use the Wayback Machine to find historical information, such as:

- A photo posted on a website that has been removed
- Content, views, writing, and opinions rescinded by an author
- A company's old job ads, statements, affiliations, or product lines

When fraud examiners are looking at archived sites, they should always search for what is not there—this is what is important. Also, when looking at archived sites, fraud examiners should look for any evidence of unusual activity and compile it for analysis.

Using Social Networking Sites to Find Information

There is a growing trend of investigators mining social media for evidence. *Social networking websites* use software to build online social networks for communities of people with shared interests.

With social networks, a user can create an account, provide specific details about his life—such as schools attended, past and present employers, hobbies, sports, and interests—and become networked to other individuals who share similar backgrounds or interests. And once users are connected, they can view the activity on each other's pages.

The popularity of social sites makes it easy for fraud examiners to find information about individuals who use such sites. Relevant social media evidence can include photographs, status updates, people's location at a certain time, and direct communications. For example, a person's online profile might provide valuable information, such as pictures of a new house that a subject cannot afford or postings detailing an aircraft previously unknown to the fraud examiner.

Fraud examiners might also find information about businesses on social networking sites. Relevant information on social media can include:

- Organization charts
- Price lists
- Hiring plans
- Expansion plans
- Customer names or lists
- Conflicts of interest
- Travel schedule and travel locations

In addition, fraud examiners can use social media to:

- Investigate complaints.
- Discover potential witnesses.
- Research the accused.
- Learn about the accusers.

While LinkedIn, Facebook, and Twitter are the current leaders of the social media pack, fraud examiners should look at the vast array of other types of networks on the Web, such as YouTube and Tumblr, and emerging social tools.

Social networking sites can be searched the same as traditional websites, and although much of the information available can be found using traditional search engines, there is an ever-growing number of resources specifically designed to search social networks.

Searching Social Media Sites

An entirely separate category of search engines has been designed specifically to find information within social networks. These search engines use social networks to order, prioritize, or refine search results. Some popular social networking search engines include Smashfuse, Social Mention, Spokeo, Topsy, Yoname, Icerocket, and FriendFeed. This section discusses these search engines along with how to search photo-sharing sites.

SMASHFUSE

Smashfuse aggregates publicly accessible data from many of the most significant social media sites, including Facebook, Twitter, Google+, and many others that are particular to regional areas around the world. Therefore, it can be useful for investigations involving parties who live in or have strong social ties with communities in other countries.

SOCIAL MENTION

Like many social media tools, Social Mention aggregates data from popular platforms. It also provides analytics tools that can help users discover what is being said about particular people, organizations, products, or other topics.

SPOKEO

Spokeo is a social network aggregator site that gathers information about people by searching for their email addresses on various social networking sites. Essentially, it is designed to locate and track online profiles within social networks. This site allows users to

search by a person's name, email address, or phone number. This can be helpful if a fraud examiner knows about the subject's profile in Facebook but is not aware that the subject is also a member of Hi5 and Xanga.

For investigators and researchers, this is an incredible tool that gathers subject information in a way that other research tools cannot. One of Spokeo's best features is its ability to track activity on members' profiles. If the subject posts something on one of the popular social networking sites, such as Facebook, the post will appear in Spokeo's search results and that person will be tracked for future updates.

Spokeo allows a user to search and track a limited number of email addresses or names for free, but requires a fee after a certain number of searches.

ICEROCKET

Icerocket is a search engine that offers a unique array of tools. It was designed to track what people were searching for, and it focuses primarily on blogs, using meta-tagging to categorize and index the content contained within blogs. As a result, a user can search by keyword, which captures any relevant matches found on a website and prioritizes matches marked as tagged searches.

Icerocket also allows users to narrow down blog searches with an advanced search link or by using search operators, such as title, author, and tag. For example, a search for [title:"public records"] would find pages with "public records" in their title. Similarly, a search for [title:"public records" author:"John Doe"] will return blog posts by John Doe that have "public records" in their title.

In addition to searching blogs, Icerocket searches through image directories, Twitter, and Facebook.

Privacy Issues When Collecting Evidence from Social Media

Social media sites might contain valuable information, and fraud examiners are free to search and extract information from a subject's page if it is open to the public. However, there are limitations to the information fraud examiners can access on a social networking site due to privacy settings and anonymity.

Individuals, for instance, might have privacy rights that protect the information stored on their social media accounts. Users of social network sites can select their own privacy settings, and when a user has a social media profile with tight privacy settings, gaining access to the information can be difficult. For example, Facebook users can adjust their account's privacy settings to restrict the sharing of their profile information.

Many users set their privacy settings in a way that prevents anyone besides their friends from seeing their profile information, and this creates several issues of legal access and privacy rights. Accessing information set to private could result in claims under privacy laws. Thus, information on social media sites that is restricted by privacy settings could result in liability for fraud examiners due to violation of users' privacy rights.

Privacy rights, however, vary between countries. Many European countries, for example, have laws that place limits on an employer's ability to regulate social media in the workplace. Spain, in particular, has some of the strictest legislation on personal data protection. Accordingly, fraud examiners must be careful about how they access information posted on a social media site.

Also, due to confidentiality, privacy, and security concerns, courts might not allow evidence obtained by someone who misrepresents himself to gain access to join a subject's private social network. For example, if a fraud examiner creates a Facebook account under an alias, "friends" the examination's target, and obtains information from the target's Facebook profile, the information might not be admitted as evidence.

Moreover, if a fraud examiner cannot access the information due to privacy restrictions, he might be able to petition the court to compel disclosure of the information. For example, courts can order parties to produce social networking sites as evidence. Similarly, a court may order parties to disclose their passwords, but this is an extreme approach. Also, a court might request a user to give information from his social media page to the opposing side. Absent some legal process, accessing information on a site with tight privacy settings is difficult.

Generally, to avoid violating privacy rights when searching social media, fraud examiners should:

- Observe any applicable privacy laws.

- Restrict searches to publicly available information (i.e., information that has lawfully been published or broadcast to the public for consumption).
- Refrain from using any pretexting, password-cracking tools, social engineering, or unethical means to gain access to private material on social networking sites.

Using Legal Orders to Obtain Information from Social Networking Sites

In some situations, it might be possible to obtain information from social networking sites via legal orders (i.e., subpoenas) to produce documents, witnesses, or other things. The ability to obtain evidence via legal orders varies among jurisdictions, however, and it might differ in criminal and civil matters.

Social Media Data Collection Best Practices

Evidence from social media is subject to the same rules of evidence as tangible evidence and other forms of electronic evidence, but because the information stored in social media sites changes constantly and users can easily update, alter, and delete relevant information, fraud examiners face additional challenges when collecting social media evidence.

Accordingly, the challenges facing the admissibility of social media evidence demand that fraud examiners consider admissibility and authenticity issues when they collect information from social media sites. This discussion provides some tips for preserving, reviewing, and collecting electronic information from social networking sites.

Generally, documentary evidence, including digital evidence, will not be admitted in a legal proceeding, or it will not be given much weight, unless it is established as authentic (i.e., the evidence is what it purports to be and is in the same condition as when it was seized).

There are a number of techniques used to authenticate information from social media. Often, authenticity can be established by the testimony of a witness who verifies that the exhibit at issue accurately reflects what he observed on the site, and typically, the witness is the party who collected the evidence. Consequently, fraud examiners who collect evidence from social media often become a form of eyewitness, and for this reason, fraud examiners must capture, download, and preserve any useful information as soon as they discover it, and they must memorialize each step of the collection process, creating a record of what they see at any point in the investigation.

There are various methods fraud examiners can use to capture information on social media sites and memorialize the collection process, including the following:

- Take screen captures of relevant information.
- Print the content.
- Use screen-recording software to create a digital recording of a screen's output.
- Convert Web pages into another format (e.g., PDF).
- Use a website capture tool that navigates to each link on a Web page and captures all the content on each link, including embedded files and source code, contained in those links.

Although these methods can capture information on social media sites, they do not maintain a significant amount of the underlying information, or metadata, that is used to authenticate digital evidence.

Due to the limitations of traditional methods of capturing website information, companies have created specialized programs that can capture social media information while preserving metadata, which is not possible through image capture or printouts. They can preserve social media information in a searchable, native format and establish a defensible chain of custody. For example, there are tools that allow users to capture key metadata unique to social media streams, preserving information not collected through image capture, printouts, or screen recording.

Using Online Sources to Conduct Specific Types of Searches

The following is a description of how online searches can be used to conduct certain types of searches, such as background checks, people searches, searches for hidden assets, legal records searches, and business filing searches.

Conducting Background Checks

Background checks generally involve two broad areas: performing due diligence to discover what public records reveal with respect to individuals and businesses with whom the investigating party might wish to do business and discovering information about prospective employees. In general, online public records databases are generally the best sources of background information.

Before conducting any background checks, consult with legal counsel.

DUE DILIGENCE

Management should ensure that it forms business relationships with reputable partners and agents. Such due diligence requires that the organization's leaders conduct public record inquiries into businesses or individuals with whom they intend to do business. This type of public record inquiry involves such issues as verifying application information, debt burden, adverse financial information, credit capacity or worthiness, business relationships (the so-called family tree), litigation history, and criminal background.

Some useful searches for due diligence are listed here:

- Corporate/business entity searches can verify information, identify principals, and develop other business relationships.
- Bankruptcy filings, tax liens, and judgments searches respond to issues of adverse financial information and credit capacity/worthiness.
- Searches of loans or leases with secured assets can answer questions of debt burden. Searches of such records can be helpful to identify hidden ownership or partnership interests, and they can be helpful to locate address information on debtors.
- Civil court records provide answers to questions concerning litigation history, past business relationships, and the potential for debt burden either as a function of an adverse judgment or as a function of financing expensive litigation.
- Criminal court records identify the possibility of a criminal background.
- The use of consumer credit reports and business credit reports helps resolve questions concerning credit capacity and creditworthiness. In addition, business credit reports are useful in verifying information, understanding business relationships, and developing basic financial information about an organization.
- Searches of occupational safety and health records might be useful in developing adverse information or verifying information given by a prospective vendor, client, or strategic partner.
- Aircraft mechanics, airmen, medical license, controlled substances, and other professional licenses might serve to verify that basic professional and occupational standards are met by a prospective vendor, client, or strategic partner.

EMPLOYMENT BACKGROUND

Organizations should implement appropriate due diligence for the retention of employees, and they must use due diligence to refrain from delegating considerable discretionary authority to any individuals who have a propensity to engage in illegal activities. Thus, for virtually all employee positions, employers should conduct a pre-employment background

check on the final candidates for the job. Every position carries with it the risk of the employee committing fraud or some other crime while in the scope of employment.

When performing background checks, it is important to keep in mind the different types of resources and the best ways to access them. Some of the most useful and widely used sources of information are available online.

Some of the searches useful in developing background information on employment are listed here (where permitted by law):

- Credit header searches are useful in confirming address and national identification number information.
- Civil court records can be searched to determine if candidates are or have been involved in legal actions.
- Criminal court records may be used to uncover past criminal problems.
- Fraud examiners can search tax court liens to determine if candidates have been sued by tax authorities.
- Aircraft mechanics, airmen, medical license, and other licenses are available to ensure that basic job requirements are met in the appropriate circumstance.
- Consumer credit reports may be used for employee selection, retention, and promotion.
- Bankruptcy filings, tax liens, and judgments may be used to identify adverse financial matters that can serve as potential motivators for fraud, defamation, and embezzlement.
- Where a prospective or current employee drives a personally owned vehicle or an employer-owned vehicle, such activity might expose the employer to liability for damages; therefore, driving records must be checked in such circumstances.
- A candidate's prior education and employment can be verified by conducting education and employment verification searches.

CRIMINAL BACKGROUND CHECKS

Criminal background searches involve checking criminal court records to see whether a person has a history of criminal misconduct. Criminal background checks are one of the most commonly used devices during employee screening and investigations. In employee screening, the purpose of these checks is to prevent the hiring of someone who, given a certain criminal history, would be unfit to serve the specific position applied for. In other investigations, criminal history can be useful in raising red flags and pointing out suspects.

The primary sources for criminal background records are court records and law enforcement agencies. Note that countries regulate access to each of these sources differently.

MANDATORY BACKGROUND CHECKS

In some situations, background checks are mandatory. When hiring for certain positions, employers must conduct background checks. Some of the professions that have mandatory criminal background check requirements include:

- Private investigators (in some jurisdictions)
- Securities brokers
- Financial industry personnel
- Security guards
- Insurance agents

Locating People Using Online Records

To locate people using online records, fraud examiners should adhere to three principles. First, when searching for an individual, the fraud examiner should obtain a past address of the subject, and search activities should begin with that information. Second, the fraud examiner should keep in mind the cost effectiveness of the search activity and avoid ordering online searches that yield unnecessary or impractical information. Third, the fraud examiner should know the most powerful and useful types of searches, which are discussed here.

CURRENT OCCUPANT/NEW ADDRESS SEARCHES

A current occupant/new address search can be used to identify the occupant of an address, to confirm occupancy, to uncover a forwarding address, or to develop a list of neighbors who might know the suspect's current whereabouts.

LAST NAME SEARCHES

Last name searches can be used if the subject's past address is unknown. This search produces better results if the subject's name is not common; however, if the subject's last name is common, differentiating information should be included in the search. Also, last name searches will return the identities of the subject's neighbors, who can be contacted for additional information about the suspect.

BANKRUPTCY FILINGS, TAX LIENS, AND COURT JUDGMENTS

Fraud examiners can use bankruptcy filings, tax liens, and court judgments to locate an individual because they might contain the national identification number of the person to whom they apply.

BUSINESS FILINGS SEARCHES

Fraud examiners can conduct business filings searches to locate individuals. Again, in many jurisdictions, individuals and corporations are required to file a doing business as (or an assumed or fictitious business name) statement with the jurisdiction where they conduct their business. By searching such records for an individual or business name, the fraud examiner can gather information from fictitious business name filings, including owner name, business name, file date, and file number. Some jurisdictions provide business address information, and in these jurisdictions, the fraud examiner can also conduct searches using the business address.

Locating Hidden Assets Using Online Records

When searching for hidden assets using the Internet, the fraud examiner must attempt to piece together the subject's lifestyle patterns. Online public records databases are useful in this capacity, and, to a lesser extent, new media sources can also assist in a search for assets.

Discovering whether assets exist, where they exist, and whether they are recoverable can be accomplished with a search of government and proprietary records. These records can be further divided into those identifying "hard" assets and those regarding the potential for assets, credit capacity, or credit worthiness.

Generally, a search for an individual's assets should include research into, among other things, the types of information (if legally accessible) discussed here.

REAL PROPERTY RECORDS

Real property records are records of land. These records can identify unknown assets or reveal property transfers to relatives, friends, or other legal entities. Accordingly, fraud examiners might examine real property records to identify the subject's main residence, land that adjoins the main residence, vacation homes, or other land.

TAX LIENS

A *tax lien* is a legal hold or claim that a government entity places on a taxpayer's property (both real property and personal property) to secure the payment of taxes. Governments file tax liens against the assets of an individual with unpaid taxes.

RECORDS OF SECURED TRANSACTIONS

Records of secured transactions in which the debtor(s) owes a stated value to a secured party or parties can provide valuable information. They can help identify personal property that an individual or business has financed. These records typically include the debtor's name and address, the name and address of the secured party, the filing date, the filing number, the filing type, and the type of collateral pledged as security. Moreover, these records might include documents such as tax liens, notices of secured interest in personal property, bank notes and drafts (including funds transfers between banks), letters of credit, securities exchanges, and so on.

VEHICLE REGISTRATION RECORDS

Vehicle registration records can lead to unknown assets, the locations of other assets, and lienholder data, which can offer insight into the subject's banking connections.

PROFESSIONAL LICENSE RECORDS

Many agencies or bodies maintain records identifying individuals holding professional licenses or memberships. Although some applications for professional licenses contain no more than a name and address, some contain lengthy personal information, such as previous residential addresses, previous employers, education and training, and financial statements.

BANKRUPTCY RECORDS

Fraud examiners should, if legally possible, also conduct a bankruptcy (insolvency) records search because such records can be used to gather background data on individuals and to determine a subject's assets, liabilities, and living expenses.

When checking bankruptcy records, the fraud examiner should check for the individual or business filing for bankruptcy, as well as for records involving any related businesses, principals, employees, or relatives.

CIVIL COURT RECORDS

Civil court records, especially those relating to a divorce, can be a noteworthy source of financial information. Divorce court records, for example, might contain information relating to bank accounts, employment, investment income, and other sources of income. Also, divorce records might contain a statement of assets that includes information on bank account holdings, retirement funds, artwork, coin collections, and so on. Moreover, divorce records might contain the filing date; the filing type; the locations, names, ages, and

birthdates of the divorced parties; the names (and ages) of any children the divorced parties have; and the properties owned. (Divorce records, however, are not available publicly in every jurisdiction).

Additionally, civil litigation records might contain valuable information. These records might identify a financial settlement a party was awarded as part of the litigation, and in some cases, civil litigation records might contain asset information of those involved in the litigation.

BUSINESS FILINGS AND DBA INFORMATION

Business filings, which refer to information an individual files to conduct business in a name other than his own, can provide valuable asset information. They might identify other businesses the subject owns or assets held by companies affiliated with the subject but not held directly in the subject's name. Business filings might also reveal a business's real property, vehicles, equipment, and intellectual property registered in the subject's name.

BUSINESS RECORDS

Business records can also be valuable. If, for example, the subject owns a business, the ownership might make it easier for the subject to hide his assets. In such cases, it might be necessary to investigate the subject's business records thoroughly for possible concealment. Also, if the subject owns a business, the fraud examiner should look for wages paid to family members or friends. It is possible that the subject paid wages to such individuals for work they did not perform with the understanding that the money belongs to the subject. Moreover, if a subject owns a business, he can write off investments as business expenses and inflate expenses to reduce income.

PHONE NUMBERS

Telephone records can provide valuable insight into asset investigations. For example, telephone records might provide contacts with real estate brokers or sellers, identify charge calls from vacation spots or contacts with co-conspirators, or provide other leads to assets and expenditures. Telephone records, however, might be private.

VOTER REGISTRATION INFORMATION

Fraud examiners can use the information contained in voter registration records to determine the identity of a person who resides at a particular address. Moreover, if a fraud examiner has the name and address of a suspect but no other identifying information, voter registration records are good sources of additional information.

BANKING RECORDS

Banking records might furnish evidence of fraud, and they might provide leads on sources of funds, expenditures, and personal affairs. Banking records can help the fraud examiner construct a paper trail to prove fraud.

Finding Business (Corporate) Filings Online

Again, in many jurisdictions, public companies, nonprofits, and some private companies must submit financial filings and forms to different government entities, and some of these records are available online.

For example, public companies in the United States must submit various filings (e.g., the annual report and the 10-K) to the Securities and Exchange Commission (SEC). These public filings provide a wealth of information about the filing company, including the nature of its business and its history, organizational structure, auditor, balance sheets, and income statements. SEC filings may be obtained from EDGAR (Electronic Data Gathering, Analysis, and Retrieval). EDGAR is a system that collects SEC filings, and it performs automated collection, validation, indexing, acceptance, and forwarding of SEC filings.

Using Newspaper/Media Databases to Find Information Online

Newspapers, periodicals, and journals can be excellent sources of information in a fraud investigation, particularly when searching for background information on an individual or a business. Many media outlets publish stories online for anyone to see, and such resources can be accessed through search engines or by going to the site directly.

Additionally, there are a number of commercial database vendors that offer wide access to newspapers and periodicals. These information database providers offer online access to the text of hundreds of newspapers worldwide, and although most providers are available for a fee, many can be accessed for free at most libraries.

Some popular news and media database vendors are described here.

Factiva

Factiva, from Dow Jones, is tailored for business and financial news searches. It maintains a catalog of thousands of the world's leading news and business sources from nearly 200 countries and in 28 languages. For more information, visit www.factiva.com.

LexisNexis

LexisNexis is a legal and business information database that provides its subscribers with access to daily newspapers for either a flat fee or a per-use fee. LexisNexis maintains a large database of U.S. and international media sources, including daily newspapers, magazines, and television transcripts. In addition, LexisNexis offers a service in which the user can request immediate information on difficult-to-find topics. LexisNexis will research the topic and give the user the information as quickly as possible. For more information, visit www.lexisnexis.com.

HighBeam Research

HighBeam has an extensive archive containing millions of documents from leading publications. HighBeam's archives are updated daily and go back as far as twenty years. Searchable sources include newspapers, magazines, journals, transcripts, books, dictionaries, and almanacs. For more information, visit www.highbeam.com.

ProQuest

ProQuest is a data service that offers access to thousands of online journals and magazines covering a wide array of subjects. ProQuest's vast content pools are available to researchers through libraries of all types and include the world's largest digital newspaper archive; periodical databases comprising the output of thousands of titles, with many in full-text, full-image format; an extensive dissertation collection; and various other scholarly collections. For more information, visit www.proquest.com.

Using Nontraditional Methods for Finding Information on the Internet

Moving beyond the use of Google and other traditional methods of searching the Internet is important for individuals conducting fraud examinations. This section will examine how to use the following websites to obtain information on the Internet:

- eBay
- Whois
- Craigslist
- Zoominfo
- GuideStar
- NOZA

The websites addressed in this discussion are tried and true resources that fraud examiners should be comfortable with using. But before using these sites, fraud examiners should

establish an undercover email account to use when searching. The email account should be set up through a Web-based service like Hotmail, Yahoo!, or Gmail. Fraud examiners should not use any of the following information when creating the email account:

- Personal names
- Geographical region
- Favorite sports teams
- Hobbies

In addition, a discreet email account should have certain characteristics, such as a gender-neutral name. The handle should be composed of numbers and letters that appear to be for a purpose, giving it added credibility and authenticity.

EXAMPLE

LS-194-2183@yahoo.com

eBay

The online auction website eBay.com can be a valuable resource for fraud examiners. It maintains lengthy, detailed logs for each transaction, but this high-level information should be obtained with a court order. A fraud examiner can search for eBay users and obtain information from their eBay profiles. A fraud examiner can gain insight by examining any items the subject bought or sold and by reviewing any comments the subject has made, as well as the subject's Feedback Profile. In addition, if the subject has a seller profile on eBay, the fraud examiner can make the suspect one of his "Favorite Sellers," to receive alerts when the subject places new items for sale on eBay.

The Whois Protocol

Whois is a query and response protocol that is used to search databases that store domain registration records, including domain name, server addresses, technical contacts, and addresses. These databases can be queried at the following sites:

- www.arin.net is a Whois server that searches for the registrant and IP address range of a particular IP address.
- www.whatismyipaddress.com provides a collection of tools for locating information about an IP address.
- www.traceroute.org—like whatismyipaddress.com—can be used to trace IP addresses.

Craigslist

Craigslist is a network of online communities featuring free classified advertisements with sections dedicated to jobs, housing, personals, items for sale, services, résumés, and so on.

The key to searching Craigslist is getting past the geographic restriction. For example, if the fraud examiner is looking for items in one location, he cannot search other areas at the same time. To expand the search, the fraud examiner must specify another area or use SearchTempest.com, a tool that allows users to search multiple Craigslist sites at once.

Zoominfo

Zoominfo collates information from websites, and then software bots—also known as *intelligent agents*—capture and match the information to particular individuals or companies. Zoominfo searches are conducted by company, person, or industry. Although Zoominfo searches can return a large amount of information, fraud examiners must understand that this information is generated from other websites and should be verified.Zoominfo search results look for résumés and include information like business experience, association connections, education credentials, and so on.

GuideStar

GuideStar is a great starting point to find data about nonprofits. GuideStar gathers and publicizes information about thousands of nonprofit organizations. It obtains information from a variety of sources.

Noza

Nozasearch.com is a Web-based database of charitable giving designed as a research tool for nonprofit organizations. It gathers data about private foundations' activities that might be of interest to grant-seekers, philanthropic organizations, and individual donors.

Additional Information Sources

A list of additional information sources is available in Appendix D. Additionally, for a list of websites that should prove useful to fraud examiners and other anti-fraud professionals, go to www.acfe.com/sample-documents.aspx.

DATA ANALYSIS AND REPORTING TOOLS

Understanding the Need for Data Analysis

Whether using the Internet in an investigation or using software to analyze data, fraud examiners rely heavily on technology to aid them in an investigation. More data is stored electronically than ever before—financial data, marketing data, customer data, vendor listings, sales transactions, email correspondence, and more—and evidence of fraud could be located within that data. Unfortunately, fraudulent data often looks like legitimate data when viewed in the raw. Taking a sample and testing it might not uncover fraudulent activity.

Fortunately, fraud examiners have the ability to sort through piles of information by using special software and data analysis techniques. These methods can identify future trends within a certain industry, and they can be configured to identify breaks in audit control programs and anomalies in accounting records.

In general, fraud examiners perform two primary functions to explore and analyze large amounts of data: data mining and data analysis. *Data mining* is the science of searching large volumes of data for patterns. *Data analysis* refers to any statistical process used to analyze data and draw conclusions from the findings. These terms are often used interchangeably.

If properly used, data analysis processes and techniques are powerful resources. They can systematically identify red flags and perform predictive modeling, detecting a fraudulent situation long before many traditional fraud investigation techniques would be able to do so.

Big Data

Big data is a buzzword in the worlds of business, audit, and fraud investigation today. According to the technology research firm Gartner, big data are "high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery, and process optimization." Simply put, big data is information of extreme size, diversity, and complexity.

In addition to thinking of big data as a single set of data, fraud investigators should think about the way data grow when different data sets are connected together that might not normally be connected. Big data represents the continuous expansion of data sets, the size, variety, and speed of generation of which makes it difficult to manage and analyze.

Big data can be instrumental to fact gathering during an investigation. Distilled down to its core, how do fraud examiners gather data in an investigation? They look at documents and financial or operational data, and they interview people. The challenge is that people often gravitate to the areas with which they are most comfortable. Attorneys will look at documents and email messages and then interview individuals. Forensic accounting professionals will look at the accounting and financial data (structured data). Some people are strong interviewers. The key is to consider all three data sources in unison. Big data helps to make it all work together to tell the complete picture.

With the ever-increasing size of data sets, data analytics has never been more important or useful. Big data requires the use of creative and well-planned analytics due to its size and complexity. One of the main advantages of using data analytics in a big data environment is that it allows the investigator to analyze an entire population of data rather than having to choose a sample and risk drawing conclusions in the event of a sampling error.

To conduct an effective data analysis, a fraud examiner must take a comprehensive approach. Any direction can (and should) be taken when applying analytical tests to available data. The more creative fraudsters get in hiding their schemes, the more creative the fraud examiner must become in analyzing data to detect these schemes. For this reason, it is essential that fraud investigators consider both structured and unstructured data when planning their engagements.

Structured Versus Unstructured Data

Data are either structured or unstructured. *Structured data* is the type of data found in a database, consisting of recognizable and predictable structures. Examples of structured data include sales records, payment or expense details, and financial reports.

Unstructured data, by contrast, is data not found in a traditional spreadsheet or database. Examples of unstructured data include vendor invoices, email and user documents, human resources files, social media activity, corporate document repositories, and news feeds.

When using data analysis to conduct a fraud examination, the fraud examiner might use structured data, unstructured data, or a combination of the two. For example, conducting an analysis on email correspondence (unstructured data) among employees might turn up suspicious activity in the purchasing department. Upon closer inspection of the inventory

records (structured data), the fraud examiner might uncover that an employee has been stealing inventory and covering his tracks in the records.

Data Mining

Data mining has roots in statistics, machine learning, data management and databases, pattern recognition, and artificial intelligence. All of these are concerned with certain aspects of data analysis, so they have much in common; yet they each have a distinct and individual flavor, emphasizing particular problems and types of solutions.

Data mining has great potential to help organizations shift their energy and focus to the most important information in their databases. Data mining tools search databases for unclear patterns, finding predictive information that even experts might not recognize. Using data mining technologies, companies can evaluate vast amounts of information, spotting patterns in their marketing and business procedures.

Although data mining technologies provide key advantages to marketing and business activities, they can also manipulate financial data that was previously hidden within a company's database, enabling fraud examiners to detect potential fraud.

Not so long ago, computer programmers were required to oversee any data mining processes; however, this is no longer necessary. Current methods use computers and computer software. Data mining software provides an easy to use process that gives the fraud examiner the ability to get to data at a required level of detail.

Data mining combines several different techniques essential to detecting fraud, including the streamlining of raw data into understandable patterns.

Data mining can also help prevent fraud before it happens. For example, IBM reports that some of its customers use data mining tools and applications to develop anti-fraud models that score transactions in real-time.[1]

[1] IBM Software, *Recognize the Many Faces of Fraud*, accessed February 2, 2012, www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=YTW03130USEN.

The scoring is customized for each business, involving factors such as locale and frequency of the order, and payment history, among others. Once a transaction is assigned a high-risk score, the merchant can decide whether to accept the transaction, deny it, or investigate further.

Data mining is an effective way for fraud examiners to develop fraud targets for further investigation. It can mine databases for various fraud indicators, such as (1) specific types of transactions; (2) patterns within the data; or (3) a relationship between two data fields that should not have a relationship (e.g., the same address or telephone number for companies with different names). Targets are then examined to develop an investigative strategy involving site visits and face-to-face interviews. Data mining can also be refined based on interviews of targets.

One of the most sophisticated uses of data mining is known as *computer matching*, also called *data matching*. This approach involves the comparison of two discrete data sets to identify questionable overlaps.

Before applying data mining processes, it is important to identify the sources from which the data will be collected. Data might be stored in any of the following locations:

- Mainframe software
- Laptop installed software
- Security system software
- Hand-held devices issued to the company's employees (e.g., smart phones, thumb drives, or inventory scanning equipment)
- Company vehicle GPS systems
- Telephone systems
- Time card systems
- Key card access

Often, companies use data warehouses to manage data for analysis. *Data warehouses* are repositories of a company's electronic data designed to facilitate reporting and analysis. By storing data in a data warehouse, data users can query and analyze relevant data stored in a single location. Thus, a company with a data warehouse can perform various types of analytic operations (e.g., identifying red flags, transaction trends, patterns, or anomalies) to assist management with its decision making responsibilities.

Although this section focuses on electronic data, fraud examiners should also identify manually generated data, such as:

- Visitor check-in logs
- Appointment logs or individual calendars
- Customer receipts for cash payments
- Return merchandise slips
- Any manually maintained lists

After the fraud examiner has identified the data sources, he should identify how the information is stored by reviewing the database schema and technical documentation. Fraud examiners must be ready to face a number of pitfalls when attempting to identify how information is stored, from weak or nonexistent documentation to limited collaboration from the IT department.

Moreover, once collected, it is critical to ensure that the data is complete and appropriate for the analysis to be performed. Depending on how the data was collected and processed, it could require some manual work to make it usable for analysis purposes; it might be necessary to modify certain field formats (e.g., date, time, or currency) to make the information usable.

The Data Analysis Process

Although the purpose of data analysis involves running targeted tests on data to identify anomalies, the ability of such tests to help detect fraud depends greatly on what the fraud examiner does before and after actually performing the data analysis techniques.

Consequently, to ensure the most accurate and meaningful results, a formal data analysis process should be applied that begins several steps before the tests are run and concludes with active and ongoing review of the data. While the specific process will vary based on the realities and needs of the organization, the following approach contains steps that should be considered and implemented, to the appropriate extent, in each data analysis engagement:

- Planning phase
  - Understand the data
  - Define examination objectives
  - Build a profile of potential frauds
  - Determine whether predication exists

- Preparation phase
  - Identify the relevant data
  - Obtain the data
  - Verify the data
  - Cleanse and normalize the data
- Testing and interpretation phase
  - Analyze the data
- Post-analysis phase
  - Respond to the analysis findings
  - Monitor the data

Planning Phase

As with most tasks, proper planning is essential in a data analysis engagement. Without sufficient time and attention devoted to planning early on, the fraud examiner risks analyzing the data inefficiently, lacking focus or direction for the engagement, running into avoidable technical difficulties, and possibly overlooking key areas for exploration.

Understand the Data

As a first step—long before determining which tests to run—the fraud examiner must know what data is available to be analyzed and how that data is structured. This might mean reviewing the database schema and technical documentation and consulting with the data administrator to learn what fields and records exist and in which tables the information is stored. The fraud examiner will also need to know how the tables are linked together.

Helpful tools in getting a full view of the organization's data include a data inventory and a data map. Such documents can be used to identify and record information about the data source, file formats, business process owners, and key systems used as they relate to specific projects. This documentation provides a good starting point for documenting the engagement history and for managing the data analytics process.

Understanding the structure of the existing data will not only help ensure that the fraud examiner builds workable tests to be run on the data, but might also help identify additional areas for exploration that might otherwise have been overlooked.

Define Examination Objectives and Scope

The amount of data housed by most organizations is extremely large; many companies process millions of transactions every day. Going through every piece of data would be impossible. And, although data analysis techniques can greatly increase investigative efficiency, performing every possible analysis of the data would be prohibitively time consuming. Consequently, at the outset, the fraud examiner must define the objectives and scope of the expected analysis. This includes considering:

- The purpose for the data analysis engagement
- The structure and size of the business
- The target area of examination, if restricted
- The resources (time, personnel, etc.) available for the engagement
- Whether any predication exists that a particular fraud is occurring
- Any existing thresholds or preferences for frauds to be considered material

Build a Profile of Potential Frauds

To maximize the potential success of detecting fraud through data analysis, the analysis performed should be based on an understanding of the entity's existing fraud risks. To do so, the fraud examiner must first build a profile of potential frauds by identifying the organization's risk areas, the types of frauds possible in those risk areas, and the resulting exposure to those frauds.

In organizations that have a formal fraud risk assessment process, this step should simply involve referring to the outcomes of that process and forming a fraud detection approach based on the risks identified. In organizations lacking such a process, however, this step can be quite time consuming, as it involves gaining a sufficient understanding of organizational operations to identify the full spectrum of fraud scenarios possible within the company.

Determine Whether Predication Exists

Data analytics is instrumental in helping a fraud examiner determine predication. *Predication* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, and/or will occur. Predication is the basis upon which a fraud investigation begins. Internal fraud investigations should not be conducted without proper predication.

Suppose someone has submitted a tip that gives the fraud examiner reason to believe a particular fraud has occurred. Before accusing someone of wrongdoing, the fraud examiner

must perform some preliminary work, such as data analysis, to determine predication; however, he must do this carefully to avoid defamation.

To illustrate, imagine a bull's-eye representing a particular fraud. The fraud examiner must stay on the outside of the bull's-eye during the predicate check. That means he should avoid conducting any interviews or making accusatory statements and instead use data analytics techniques that do not infringe upon anyone's rights. Because the investigation of fraud deals with the individual rights of others, an investigation must be conducted only with adequate cause or predication.

Preparation Phase

The results of a data analysis test will only be as good as the data used for the analysis. Thus, before running tests on the data, the fraud examiner must make certain the data being analyzed are relevant and reliable for the objective of the engagement. The phrase "garbage in, garbage out" is applicable in the preparation phase.

Identify the Relevant Data

Using the profile of potential frauds as a guide, the fraud examiner must identify the target data for analysis. Specifically, for each specific fraud scenario assessed to be a high risk to the organization, the fraud examiner should determine which data fields and records would be affected by such a scheme.

The fraud examiner must then identify the logistics involved with obtaining this information, including:

- What specific data (i.e., fields, records) is available
- Who generates and maintains the data
- Where the data is stored
- Timing of the data extraction (e.g., date range, cutoff dates/times)
- How the fraud examiner will receive and store the data
  - Data format
  - Storage/transfer mechanism
- Control totals needed for verification
- How to validate the sources of data

Obtain the Data

The fraud examiner should prepare and submit a formal request for the desired data, outlining the specifics determined in the previous step. Depending on the objectives of the engagement and the operations of the organization, the fraud examiner might be given a file containing the data to work with, or he might be provided read-only access to the data within the organization's information system.

This step in the process can be particularly challenging. In some cases, obtaining the data involves working with overloaded or uncooperative data managers, IT departments, or other parties. Other potential obstacles at this stage include data that is housed in different systems or on different platforms and data that is maintained manually.

Verify the Data

Once the data has been received by the fraud examiner, it must be verified. The first step is simply to ensure that the data analysis software that will be used is able to open and read the data as provided. The fraud examiner should then validate that the data received contains all requested fields and records.

Once the success of the transfer process has been confirmed, the fraud examiner should perform the following tests to verify the integrity of data:

- Confirm control totals.
- Confirm that the period covered by the data is appropriate and as requested.
- Sort the file in ascending or descending order to test for leading or lagging errors.
- Check for gaps in applicable fields, including system-assigned identifying record number, to identify missing records.
- Confirm the format of data in format-specific fields, such as date fields and numeric fields.
- Check for blank fields where information should be entered.
- Check for duplicate fields or records.

The fraud examiner can also use tests for reasonableness or logical relationships to verify data integrity. Examples of such tests include:

- If transactions average X per day, verify that a monthly file includes approximately X times the number of business days.
- Divide average transaction size by the number of transactions in the file.

- Compare fields such as items ordered to items shipped to confirm that the amount shipped is equal to or less than the amount ordered.

Cleanse and Normalize the Data

Depending on how the data was collected and processed, as well as the results of the data verification process, the fraud examiner might need to cleanse and convert the data to a format suitable for analysis before executing any data analysis tests. For example, certain field formats (e.g., date, time, or currency) might need to be modified to make the information consistent and ready for testing.

The data must also be normalized so that all data being imported for analysis can be analyzed consistently. Common data fields from multiple systems must be identified, and data must be standardized. In normalizing the data for analysis, table layout, fields/records, data length, data format, and table relationships are all important considerations.

Additionally, the following inconsistencies in the data must be addressed:

- Known errors
- Special/unreadable characters in the data
- Other unusable entries

When possible, such situations should be addressed by fixing, isolating, or eliminating them. Any issues that cannot be cleaned up will require special consideration during the testing and interpretation phase.

Testing and Interpretation Phase

If the planning and preparation stages have been conducted effectively, the testing and interpretation phase should yield results that are helpful in uncovering red flags of fraud in the data. Any known issues in the data that cannot be fixed or isolated might require further review. This data might lead fraud examiners to areas they did not think to focus their attention. It might actually prove to be useful information during the testing and interpretation phase.

Analyze the Data

When using data analysis to detect fraud, the fraud examiner should organize and analyze the data in a way designed to uncover patterns that are consistent with the specific fraud scenarios identified during the planning stage.

Grouping the data into homogenous groups can facilitate the fraud examiner's ability to spot outliers. The specific groupings should be based on the target fraud scenario and data being analyzed, but such categorization might include grouping data by:

- Geographical location
- Business division or unit
- Time period
- Dollar value
- Sales person

Another useful step involves running some high-level tests, such as summarization or statistical analysis, to get an overview of the data and provide some context for any outliers identified during later testing.

From here, the fraud examiner should run tests to uncover possible indicators of fraud, including unusual trends, anomalies, and control breakdowns. The data analysis techniques used should be chosen based on the high-risk fraud scenarios being considered. Tests designed to detect specific fraud schemes will be covered later in this chapter.

In analyzing the results of the tests run, the following issues merit special consideration:

- The role of concealment
- Addressing false positives

The Role of Concealment

The fraud examiner must remember that the goal of the data analysis engagement is to identify fraudulent transactions—transactions that, by their very nature, involve deception and attempted concealment. The fraud examiner is looking for data that has been intentionally manipulated, rather than just erroneously recorded. Consequently, he should focus his analysis on data that is strategically missing or altered, such as lacking contact information, or transactions that narrowly circumvent organizational policies. Additionally, because fraudsters can be creative in concealing their schemes, fraud examiners must be creative in their searches, often combining several data analysis techniques and tests.

Addressing False Positives

A false positive is a transaction identified by a data analysis test as an anomaly within the data set even though it is not actually a fraudulent transaction. Such results can occur for a number of reasons, including:

- Data validity/integrity issues
- Data merging difficulties
- Legitimate data that fall outside the field norm (e.g., letters in a numbers-only field, such as a phone number)

The goal in running data analysis tests is to identify anomalies without generating too many false positive results. Sorting through and analyzing false positives takes time and resources that could be spent further investigating other potentially fraudulent transactions. However, proper planning and preparation should help minimize the occurrence of false positives in the test results.

Post-Analysis Phase

The data analysis tests will likely reveal many potential areas of exploration. After executing the desired tests, the fraud examiner will need to determine how to respond to the findings and how to watch for future anomalies.

Respond to the Analysis Findings

The findings of the data analysis engagement will rarely be sufficient on their own to conclude that fraud is or is not occurring. Any anomalies identified will require follow-up and further examination to determine the reason for the discrepancy in the data. Often, this will include investigatory procedures such as document examination and interviews. The specific resultant actions should be based on the fraud scenarios in question and the particular red flags identified in the data.

Additionally, the terms and objectives of the engagement will dictate whether a formal report should be issued and, if so, the form and audience of the resulting report. Such a report should typically be easy to understand, summarize the analysis findings, and provide insightful and applicable information for the relevant readers.

Monitor the Data

Based on the results of the analysis and the needs of the organization, the fraud examiner should work with management to determine whether any of the tests performed should be repeated on a periodic or continuous basis. In areas deemed to be at heightened risk for fraud, continuous monitoring can provide increased assurance of early detection of any fraud schemes and can even serve as a deterrent to misconduct.

Spectrum of Analysis

The spectrum of application for data analysis includes:

- *Ad-hoc testing,* which involves a one-use, point-in-time analysis conducted for a specific project or exploration, such as a fraud investigation.
- *Repetitive testing,* which is composed of repeatable, predefined, automated procedures performed on similar data on a scheduled basis, and is most beneficially used on business processes where the risk and likelihood of fraud are high.
- *Continuous testing,* which involves constant automated data monitoring efforts, often embedded directly into the production system, focused on those transactions or areas that pose particularly strong risks or for which preventive controls are not possible or deemed ineffective.

Based on key risk indicators, ad-hoc testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered.

Using Data Analysis Software

Once data has been extracted, it must be analyzed. While data analysis is used mainly as an audit technique, it can be an important part of the fraud detection toolkit. Although the direct results from data analysis software cannot be used as trial evidence that a fraud was committed or that a specific individual was involved, they can serve to identify red flags associated with a wide variety of frauds. The results will thereby provide investigators with a trail to follow.

Advantages of Using Data Analysis Software

There are five significant advantages to using data analysis software. First, data analysis software allows the fraud examiner to centralize an investigation, relying less on others to gather data. Because of the amount of information data software is able to sort through, the fraud examiner no longer has to rely on different sources for information. In the past, when analyzing a company's books for possible discrepancies, the fraud examiner would have to ask for the assistance of several persons within the accounting department to locate the information. Now, however, software programs will do all the work, ensuring an above-the-board investigation without many variables.

Second, data analysis software allows the fraud examiner to ensure that an investigation is accurate and complete. In the past, an audit or fraud examination could only be complete to

the extent that the investigator was able to sift through information. When looking at one month's worth of a company's transactions, a fraud examiner might be forced to research more than one million transactions. Given the amount of time an auditor generally has to conduct a single examination, the depth of a manual audit can be suspect at best. By using a data analysis program, the fraud examiner can run several different analysis patterns in a matter of hours, enabling him to look at greater volumes of information from a number of different angles. These procedures lead to a more comprehensive examination.

Third, data analysis allows the fraud examiner to base predictions about the probability of a fraudulent situation on reliable statistical information. By using data analysis software, the fraud examiner can base any strong suspicions of fraudulent activities on hard numbers. Because the software will compare one month's expenditures with the same data for the rest of the months of the year, the fraud examiner can point conclusively to troubled areas. With hard data to support a fraud examiner's suspicions, a company is more likely to conduct further investigations into the wrongdoing.

Fourth, data analysis allows the fraud examiner to search entire data files for red flags of possible fraud. The number of checkpoints a fraud examiner can set up using a data analysis program is staggering. By cutting down the paperwork involved in an investigation, the fraud examiner is able to execute a number of different searches and analyses of the company's raw data.

Finally, data analysis can assist the fraud examiner in developing reference files for ongoing fraud detection and investigation work. By performing audits and examinations with data analysis software, the fraud examiner will begin to recognize trends and set up a list of precedents for individual accounting situations, such as a monthly statement reconciliation. In doing so, the fraud examiner can establish a "norm" with which to compare individual months or years. These precedents can also be used by the fraud examiner in general terms, and the knowledge can be applied to nearly any fraud investigation.

Core Data Analysis Software Functions

Computers can scan database information for several specific types of information, creating a red-flag system. To perform this, most software packages use a combination of different functions. These functions are:

- Sorting
- Record selection

- Joining files
- Multi-file processing
- Correlation analysis
- Verifying multiples of a number
- Compliance verification
- Duplicate searches
- Expressions and equations
- Filter and display criteria
- Fuzzy logic matching
- Gap tests
- Pivot tables
- Regression analysis
- Sort and index
- Statistical analysis
- Stratification
- Date functions
- Benford's Law analysis
- Graphing

Sorting

To sort means to arrange data in a meaningful order. Sorting is nothing new; most reports you read are sorted in some way. With sorted data, fraud examiners can quickly pick out what is important or identify blank fields where information should be entered. An investigator can ask a program to sort information using different methods, such as alphabetically or numerically. For instance, when searching for a suspected fraudster's name out of thousands in a check disbursement file, software can quickly sort a list of payee names.

Sample customer sales data

Date	Invoice	Customer	Amount
05/04/10	M3158001	J789889	$12,500.00
07/05/10	M5958256	Q189425	$14,580.00
08/09/10	M8897158	T681897	$38,889.00
07/25/09	M1569897	T888971	$87,569.56
12/20/10	M3158001	P123089	$12,500.00
01/08/10	M2098159	W555258	$56,347.23

Data sorted by invoice number

Date	Invoice	Customer	Amount
07/25/09	M1569897	T888971	$87,569.56
01/08/10	M2098159	W555258	$56,347.23
05/04/10	M3158001	J789889	$12,500.00
12/20/10	M3158001	P123089	$12,500.00
07/05/10	M5958256	Q189425	$14,580.00
08/09/10	M8897158	T681897	$38,889.00

Data sorted by amount

Date	Invoice	Customer	Amount
05/04/10	M3158001	J789889	$12,500.00
12/20/10	M3158001	P123089	$12,500.00
07/05/10	M5958256	Q189425	$14,580.00
08/09/10	M8897158	T681897	$38,889.00
01/08/10	M2098159	W555258	$56,347.23
07/25/09	M1569897	T888971	$87,569.56

Record Selection

Data analysis software can select specific records for analysis. Specific record selection is accomplished by making a request or query to find the occurrences of items or records in a field. This type of request will only return instances where the record did occur, effectively reducing large amounts of information into brief lists. Often, additional criteria placed on the record selection or query will reveal a more pertinent list of information. Most data analysis programs include simple macros to help locate specific records.

Joining Files

The Join function gathers the specified parts of different data files. Joining files combines fields from two sorted input files into a third file. Join is used to match data in a transaction file with records in a master file, such as matching invoice data in an accounts receivable file to a master cluster. For example, a fraud examiner might need to compare two different files to find differing records between files. The following is an example of how joining two files can easily provide that information.

File 1

Customer	Account	Balance	Last Invoice
Jerry's Cleaners	555221	$12,500	12/30/10
Quality Garments	555658	$9,283	11/15/10
Beverly's Tailoring	554891	$27,588	01/15/10

File 2

Customer	Account	Balance	Last Invoice
Quality Garments	555658	$9,283	11/15/10
McCloud's Fabrics	556897	$10,888	09/24/10
Beverly's Tailoring	554891	$27,588	01/15/10

The *JOINED* exception file

Customer	Account	Balance	Last Invoice
McCloud's Fabrics	556897	$10,888	09/24/09
Jerry's Cleaners	555221	$12,500	12/30/09

Multi-File Processing

Multi-file processing allows the user to relate several files by defining relationships between multiple files, without the use of the Join command. A common data relationship would be to relate an outstanding invoice master file to an accounts receivable file based on the customer number. The relationship can be further extended to include an invoice detail file based on invoice number. This relationship will allow the user to see which customers have outstanding invoices sorted by date.

Correlation Analysis

Fraud examiners can use a correlation analysis to determine the relationships among different variables in raw data. Fraud examiners can learn a lot about data files by learning the relationship between two variables. To illustrate, see the example that follows. In the example, there should be a strong correlation between the independent and dependent variables because there is a direct relationship between them. Hotel costs should increase as the number of days traveled increases. The gallons of paint used should increase as the number of houses painted increases. Any deviation from the expectation should be investigated more thoroughly.

Independent Variable	*Dependent Variable*
Number of days traveling	Hotel cost
Number of documents printed	Reams of paper used
Number of houses built	Paint used

To conduct a correlation analysis, there must be a pair-wise relationship between the two sets of data. In other words, each *x* variable has a corresponding and unique *y* variable. If the data are not intrinsically related (e.g., two fields on the same invoice), then there must be a strong logical relationship between the data (e.g., same general ledger account).

Correlation analysis allows a fraud examiner to evaluate the *strength* of the connection between two or more pieces of information on, for example, a balance sheet or an income statement. Suppose you find a strong correlation between consulting expenses and earnings over an adequate period of time. You then would use regression analysis to assess any fluctuations that had occurred in that relationship, compared to the historical norm for that organization or its industry. The goal is to find out whether (and if, so when and why) the relationship entered a new phase and to isolate any red flags that might warrant a fraud investigation.

The strength of the relationship between two variables is indicated by the correlation coefficient. The formula to calculate the correlation coefficient is the following:

$$r = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2 \sum (y - \bar{y})^2}}$$

In Excel, the CORREL(array1,array2) function returns the correlation coefficient.

The value of the *r* ranges between -1 and 1. A positive *r* means that the variables vary in the same direction together (positive slope). A negative *r* means that the variables have an inverse relationship and that the graph is negatively sloping.

The strength of the relationship between the two variables is indicated by the absolute value of *r*. An *r* of 0, for instance, means that there is no relationship between the two variables. A correlation coefficient ranging from 0.8 to 1 would indicate a strong relationship between the two variables. Note, however, that a strong correlation coefficient does not indicate there is a *causal* relation between the variables; it merely implies correlation. It also does not indicate fraud, but rather the potential for fraud, or at least suspicious data.

Once two variables have been graphed against each other, the result will be a scatterplot. If the two variables have a strong correlation, you will be able to calculate, or at least eyeball, a best-fit line. A best-fit line can be used to predict the *y* variable given any *x* variable. The least squares method is the most common way to calculate the equation of the line. It minimizes the squared distance of the data points from the line.

The equation of a line is $y = mx + b$, where m is the slope and b is the y-intercept (i.e., the value of y when $x = 0$). Linear regression and correlations are intimately related. The

importance of regression lies in the ability to predict the value of *y* based on known values of *x*. Remember, the stronger the correlation coefficient, the more accurately the best-fit line will predict *y* for any given *x*.

Values that fall far outside of the expected range (graphically, points that are far away from the best-fit line) are known as *outliers*. In some cases, there are reasonable explanations for outliers. Sometimes, however, an outlier is an indication of fraud.

Verifying Multiples of a Number

With this function, a fraud examiner can determine whether regularly disbursed checks, such as reimbursement for mileage, are consistent within the regular rate. For instance, if the mileage checks do not measure up to the standard units of currency-per-mile rate, a red flag should automatically be raised.

Compliance Verification

Compliance verification determines whether company policies are met by employee transactions. If a company limits the amount of its reimbursements, analysis software can check to see that this limit is being observed. Many times, fraud examiners can find early indications of fraud by testing detail data for values above or below specified amounts. For example, when employees are out of town, do they adhere to the company policy of not spending more than $30 a day for meals? For starters, the fraud examiner can look at the expense reports and select those with meal expenses exceeding $30. With the information returned from this simple query, the fraud examiner has a starting point for suspecting fraud. Even though these variances are small ($2 and $3), the time taken to research small variances can be well invested. The trail might lead to something big. After further investigation, the fraud examiner might learn that the employee did not have supporting documentation to submit because a vendor's sales representative paid for all the meals. If this is the case, you have two fraud suspects, the employee and the employee's boss who approved the report.

Duplicate Searches

Duplicate testing is used to identify transactions with duplicate values in specified fields. This technique can quickly review the file, or several files joined together, to highlight duplicate values of key fields. In many systems, the key fields should contain only unique values (no duplicate records).

For example, a fraud examiner would expect fields such as check numbers, invoice numbers, and government identification numbers (e.g., Social Security numbers) to contain only unique values within a data set; searching for duplicates within these fields can help the fraud examiner find anomalies that merit further examination.

Expressions and Equations

Fraud examiners can build expressions or equations based on their knowledge and expectations of what should be in the data (e.g., recomputing net payroll amounts based on gross pay, taxes, and other deductions; recalculating amounts charged on invoices based on unit price and quantity ordered). Comparing the actual data to these equations, then, can be used to verify actual amounts and test actual relationships.

Filter and Display Criteria

Fraud examiners can create filters or queries based on specific user-defined criteria that result in only those records that meet the criteria being displayed. Such filters can help identify transactions that are outside the expected norm for the data. Additionally, the results can be further filtered or analyzed using other data analysis techniques; such layered analysis can help the fraud examiner drill down to the most pertinent records for review.

Fuzzy Logic Matching

Employing fuzzy logic techniques can help identify records with similar or potentially duplicate—though not identical—values, such as First Street, First St., and 1st St. Using this approach is especially helpful in detecting fraudulent transactions where the perpetrator has taken some steps to manipulate values and conceal illegitimate data. However, it also typically produces an increased number of false positive results, so it should be used with appropriate caution and oversight.

Gap Tests

Gap testing is used to identify missing items in a sequence or series, such as missing check or invoice numbers. It can also be used to find sequences where none are expected to exist (e.g., employee government identification numbers).

Pivot Tables

A *pivot table* is an interactive data summarization tool found in Excel. It is used to sort, count, total, or give the average of specified data in a spreadsheet. It is a helpful way to see the "big

picture" of the data you are working with without having to enter in formulas. You can also perform the filter and sort functions within the pivot table.

Suppose you have a spreadsheet with sales data. A pivot table will allow you to determine how many sales occurred by month, by country, by product, by salesperson, and so on. The table will summarize this data in any way you like—for instance, in units or dollars sold. This allows the fraud examiner to make comparisons, detect patterns and relationships, discover trends, and possibly detect anomalies.

The following is an example of a pivot table made from sales data. Each row represents a salesperson, and the columns are broken out by country. The table results display the sales each salesperson made by country, and the final column is the total sales produced by each salesperson.

Sum of AMOUNT	Column Labels				
Row Labels	CAN	MEX	UK	USA	Grand Total
Carson		1,566.75		900.00	2,466.75
Grant		1,119.50	4,700.64		5,820.14
Hughes		287.19		456.64	743.83
Jamison			582.31	6,053.46	6,635.77
Miller	2,490.30			2,032.64	4,522.94
Parsons	2,380.71			889.76	3,270.47
Grand Total	**4,871.01**	**2,973.44**	**5,282.95**	**10,332.50**	**23,459.90**

Regression Analysis

Regression analysis is a sophisticated statistical technique that uses a series of records to create a model relationship between a dependent variable and one or more independent variables. For example, regression analysis could be used to model and predict the number of widgets manufactured based on amounts of materials and labor used. A period in which production output is significantly lower than predicted based on this model would merit further examination.

Sort and Index

Sorting or indexing arranges the data in ascending or descending order based on the specified field(s). Depending on the values in the selected field, the data might be sorted alphabetically (e.g., names), numerically (e.g., amounts), or chronologically (e.g., dates).

Statistical Analysis

Calculating statistics—such as averages, standard deviations, highest or lowest values, and absolute values—can be a valuable early step in analyzing volumes of data to enable quick identification of unusual relationships that need further review. Additionally, comparing statistical results to industry standards, past performance, or expected relationships can provide further direction for an investigation.

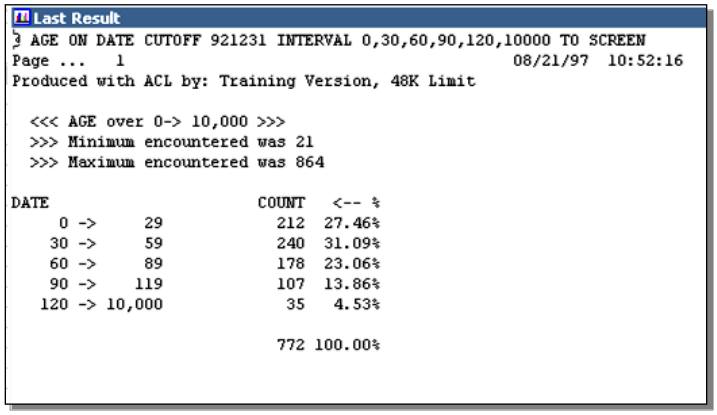
Stratification

Stratification breaks the data into specific intervals, or *strata*, based on a specific field and counts the results that fall into each group. The following is an example of the results of stratifying a sample of invoices by dollar amount:

Invoice amount	Count	Percent of total	Total amount
Less than $1,000	87	10.5%	$ 66,078.24
$1,001–$5,000	196	23.6%	$ 782,089.00
$5,001–$10,000	359	43.2%	$ 2,515,940.21
$10,001–$20,000	102	12.3%	$ 1,427,527.74
$20,001–$50,000	68	8.2%	$ 2,022,600.16
Over $50,000	19	2.3%	$ 1,298,874.96
Total:	831	100%	$ 8,113,110.31

Date Functions

Various software programs allow users to check for differences in dates, such as invoice dates. By verifying that check disbursements are consistent, fraud examiners can ensure that no suspicious payments were arranged by an employee. Analysis programs will also allow for aging of data. Aging techniques involve analyzing data based on date. For example, a fraud examiner might look at the age of different invoices by putting them into buckets of 30, 60, and 90 days and totaling the amounts for each bucket to look for patterns or outliers among the periods. The following is an example of accounts receivable aging.



Benford's Law Analysis

In the 1920s, General Electric Co. physicist Frank Benford made an interesting observation while examining his logarithm book. Logarithm books were used by scientists and mathematicians to multiply large numbers before computers or calculators were available. He noticed that the first few pages of his logarithm book were more worn than the other pages. Since the first few pages of a logarithm book list multi-digit logs beginning with the digits 1, 2, and 3, he theorized that scientists spend more time dealing with logs that begin with 1, 2, or 3. He also found that with each succeeding first digit, the amount of time it was used decreased.

This observation led to a remarkable mathematical discovery: In a population of naturally occurring multi-digit numbers, the multi-digit numbers beginning with 1, 2, or 3 must appear more frequently than multi-digit numbers beginning with the digits 4 through 9. Furthermore, the first digit of the numbers will be distributed in a predictable, but unexpected, way. Instead of the frequencies of the first digit being equal (a 1 out of 9 chance for each of the digits 1 through 9), the first digit of a multi-digit number typically follows a different pattern. Predictable patterns also occur in the second and third digits of multi-digit numbers.

Benford's Law distinguishes between natural and non-natural numbers, and it is important to understand the difference between the two types because Benford's Law cannot be applied to data sets with non-natural numbers. *Natural numbers* are those numbers that are not ordered in a particular numbering scheme and are not human-generated or generated from a random number system. For example, most accounts payable files will be populated by currency values that are natural numbers. Conversely, *non-natural numbers* (e.g., employee identification numbers and telephone numbers) are designed systematically to convey information that restricts the natural nature of the number. Any number that is arbitrarily determined, such as the price of inventory held for sale, is considered a non-natural number.

Benford's Law provides that the distribution of the digits in multi-digit natural numbers is not random; instead, it follows a predictable pattern. The following table shows the expected occurrence for the distribution of the first digit in natural numbers, according to this law:

First Digit	Probability
1	30.1%
2	17.6%
3	12.5%
4	9.7%
5	7.9%
6	6.7%
7	5.8%
8	5.1%
9	4.6%
Total	100.0%

Benford's Law maintains that certain digits show up more than others do when dealing with natural numbers. A "1" appears as the first non-zero digit roughly 30 percent of the time; "2" is the leading digit almost 18 percent of the time; and "9" leads off only 4.6 percent of the time. Moreover, "0" is most likely to be the second digit, appearing 12 percent of the time.

The goal of a Benford's Law analysis is to identify fictitious numbers. Many fraudsters fail to consider the Benford's Law pattern when creating false documentation or transactions to cover their tracks. Consequently, testing data sets for the occurrence or non-occurrence of the predictable digit distribution can help identify included numbers that are not legitimate.

To which data sets might Benford's Law be applied as a fraud detection tool? Mark J. Nigrini, Ph.D., is an expert on this topic. In his book, *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection,* Nigrini identifies the following criteria that a data set should possess in order for Benford's Law to be valid: [2]

- The data set should describe the sizes of similar phenomena (e.g., the monetary amount of purchase transactions).
- There should be no built-in minimum or maximum values in the data set.
- The data set should not consist of assigned numbers (e.g., account numbers, transaction numbers, purchase order numbers, or check numbers).
- The data set should have more small items than large ones (e.g., a business normally has a greater number of small transactions than larger ones).

[2] www.wiley.com/WileyCDA/WileyTitle/productCd-1118152859.html

The most common application of Benford's Law to fraud detection involves analyzing the dollar amounts of a data set consisting of business transactions. Note that Benford's Law is scale invariant under multiplication; that is, if a Benford set is multiplied by a nonzero constant (e.g., a foreign currency exchange rate), the new list of numbers will also be a Benford set.

In analyzing populations of financial transactions, Benford's Law can help uncover a wide variety of anomalies that might indicate asset misappropriations, such as:

- Shell company (fictitious vendor) schemes, in which the perpetrator makes up amounts to be used for the fraudulent invoices submitted by the supposed vendor
- Cashiers who ring fictitious refunds on cash registers
- Bid-splitting and other schemes involving limit circumvention, in which the fraudulent transactions often begin with a digit that is just below the threshold (e.g., if transactions above $10,000 are subject to increased scrutiny, one might observe a higher-than-usual number of transactions in which the first digit of the amount begins with a 9 or an 8)

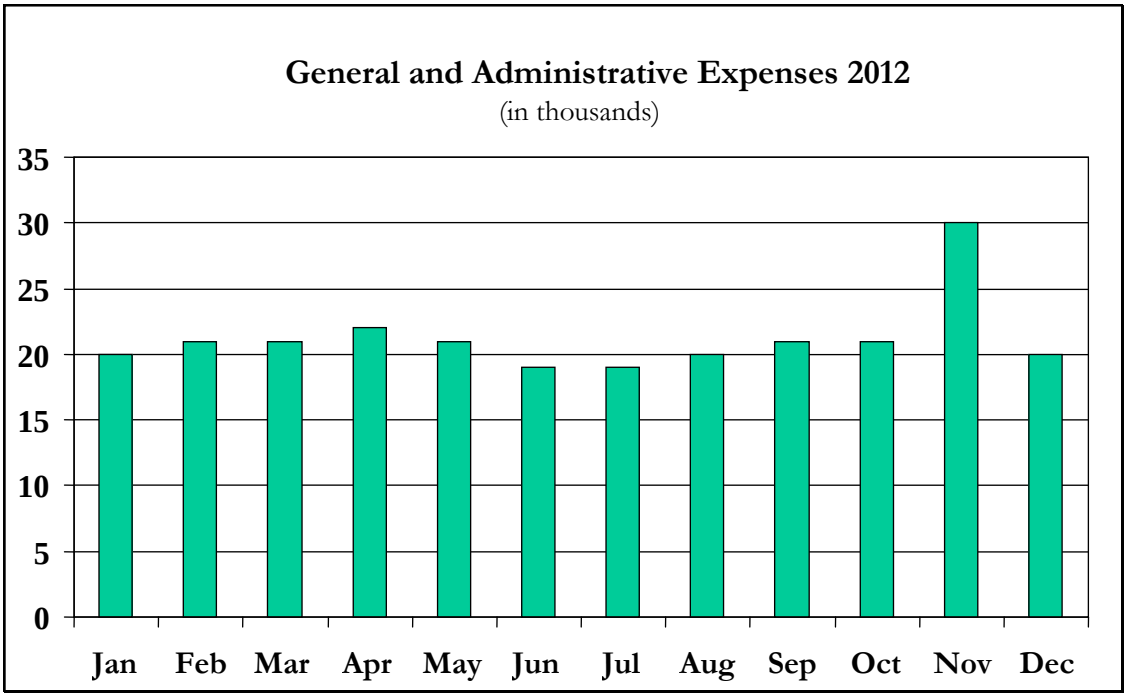
Benford's Law can also be useful in the detection of financial statement fraud. In their paper, "Data Mining Journal Entries for Fraud Detection: A Pilot Study," Roger Debreceny and Glen Gray studied the journal entries of 29 entities and found a high correlation between Benford's Law and the first digits of the amounts in journal entries.[3] Only a handful of anomalies were found, suggesting further investigation would be necessary to determine whether fraud was involved. (Note: Debreceny and Gray do not indicate what types of entities were included in their data, nor do they provide details of the anomalies that were identified, and these anomalies were not subject to further investigation.) Accordingly, Benford's Law may have useful applications in detecting financial statement fraud.

One possible application of Benford's Law to journal entries and financial statement fraud is the potential for discovery of multiple journal entries just below a limit threshold that would be subject to greater scrutiny, such as by the internal or external auditors. Similar to detecting limit circumvention associated with asset misappropriations, Benford's Law might also be used to detect numerous journal entries used to perpetrate financial statement fraud, such as recording many entries, each involving fictitious revenue.

[3] Debreceny, Roger S., and Glen L. Gray, "Data Mining Journal Entries for Fraud Detection: A Pilot Study," 2009.

Graphing

Graphs, like pictures, are worth a thousand words. Data analysis programs can provide numerous types of graphs to give fraud examiners a quick glimpse of the data. For example, the following graph demonstrates that an inquiry should be made as to why November expenses are $10,000 more than the monthly norm.



Examples of Data Analysis Queries

The following are typical examples of data analysis queries that can be performed by data analysis software.

General Ledger Analysis

The following are examples of data analysis queries that can be performed to detect fraud through examination of the general ledger:

- Select specific journal entries for analysis.
- Create actual-to-budget comparison reports.
- Analyze and confirm specific ledger accounts for legitimate transaction activity.
- Speed account reconciliation through specialized account queries.
- Calculate financial ratios.
- Calculate percentage comparison ratios between accounts.
- Prepare custom reports, cash flow, profit/loss, and asset and liability total reports.

- Compare summaries by major account in any order (low-high, high-low).
- Create reports in any format by account, division, department, etc.

Accounts Receivable

The following are typical examples of data analysis queries that can be performed to detect fraud by examining accounts receivable records:

- Create a list of customer limit increases and decreases.
- Age accounts receivable in various formats.
- Identify gaps in sequential forms such as invoices.
- Identify duplicate invoices or customer account numbers.
- Show specified reports on credits taken by customers.
- Report customer summaries by invoice, product, etc.
- Identify customer activity by age, product, etc.
- Compare customer credit limits and current or past balances.

Sales Analysis

The following are typical examples of data analysis queries that can be performed to detect fraud through examination of sales information:

- Create a report of all system overrides and sales exceptions.
- Analyze returns and allowances by store, department, or other areas.
- Summarize trends by customer type, products, salesperson, etc.
- Compare ratios of current sales to outstanding receivables or other variables.
- Generate reports on a correlation between product demand or supply and sales prices.

Accounts Payable

The following are examples of data analysis queries that can be performed to help detect fraud through examination of accounts payable:

- Audit paid invoices for manual comparison with actual invoices.
- Summarize large invoices by amount, vendor, etc.
- Identify debits to expense accounts outside of set default accounts.
- Reconcile check registers to disbursements by vendor invoice.
- Verify vendor tax forms (e.g., U.S. Form 1099 or Value Added Tax (VAT) forms).
- Create vendor detail and summary analysis reports.
- Review recurring monthly expenses and compare to posted/paid invoices.
- Generate a report on specified vouchers for manual audit or investigation.

Asset Management

The following are examples of data analysis queries that can be performed on asset accounts to help detect fraud:

- Generate depreciation to cost reports.
- Compare book and tax depreciation and indicate variances.
- Sort asset values by asset type or monetary amount.
- Select samples for asset existence verification.
- Recalculate expense and reserve/provision amounts using replacement costs.

Cash Disbursement

The following are typical examples of data analysis queries that can be performed to detect fraud through examination of cash disbursement records:

- Summarize cash disbursements by account, bank, department, vendor, etc.
- Verify audit trail for all disbursements by purchase order, vendor, department, etc.
- Generate vendor cash activity summary for analysis.
- Identify disbursements by department, supervisor approval, or amount limits.

Payroll

The following are examples of data analysis queries that can be performed to help detect fraud through examination of payroll records:

- Summarize payroll activity by specific criteria for review.
- Identify changes to payroll or employee files.
- Compare timecard and payroll rates for possible discrepancies.
- Prepare check amount reports for amounts over a certain limit.
- Check proper supervisory authorization on payroll disbursements.

Purchasing

The following are examples of data analysis queries that can be performed on purchasing records to help detect fraud:

- Track scheduled receipt dates versus actual receipt dates, in summary and detail.
- Compare vendor performance by summarizing item delivery times and amounts.
- Isolate purchase order types for analysis.

Data Analysis Checklist

The following are some key issues to address as one conducts a data analysis:

- *Ensure data validity and data integrity*. There are always concerns when the fraud examiner moves data from one place to another. One of the concerns is data validity. Is the data

valid and pertinent to the investigation? Another concern is data integrity. Is the valid data that was selected correct? A simple check or audit of the validity and integrity of the data should be the first step in the data analysis.

- *Consider data format and structure*. This consideration is important when the fraud examiner wishes to import or export data with his computer. A date can be formatted into a number of different styles, such as mm/dd/yyyy. The structure of the data will also be important, along with the extension. A text file will have a .txt extension associated with it. In what format is the current data? What format will the computer require? How does the fraud examiner get the data from here to there if the data formats and structures are different?
- *Compare the cost and benefit of potential analysis*. The fraud examiner should perform a preliminary analysis to ensure that the key strategic issue he is about to develop is worth the effort before initiating a fraud investigation.
- *Consider the spectrum of distinct levels of aggregation at which fraud monitoring is required*. Determine the lowest level (transaction level), the highest level (multiparty criminal conspiracies), and the intervening layers that might be present in your industry and respective data.
- *Begin with the end in mind*. In his book, *The Seven Habits of Highly Effective People*, Stephen Covey states that it is a good idea to begin with the end in mind. When the fraud examiner develops his fraud intelligence action plan, he must consider the end result. One question to ask might be, "Will this algorithm/consultant hold up under the intense scrutiny of a court of law?"

Scheme-Specific Data Analysis Tests

Data analysis tests are useful for many types of fraud investigations. Whether the suspected scheme is a case of asset misappropriation, corruption, or financial statement fraud, there are often ways that data analysis can detect or offer insight into the fraud. For more information on these schemes, refer to the Financial Transactions section of the *Fraud Examiners Manual.*

There are thousands of potential applications for data analysis in the anti-fraud profession. The following are a handful of examples to demonstrate how fraud examiners can use data analysis techniques to detect various types of schemes.

Asset Misappropriation

Asset misappropriation covers the largest percentage of occupational frauds committed. Data analysis can be helpful during these investigations, especially at organizations with

many employees, customers, or transactions. Any of these factors can lead to a large amount of data needing to be parsed through, and can make manual searches impractical.

One common asset misappropriation scheme is the ghost employee scheme. A ghost employee is someone who is on the payroll register but who does not actually work for the company. Finding ghost employees often coincides with an internal fraud scheme.

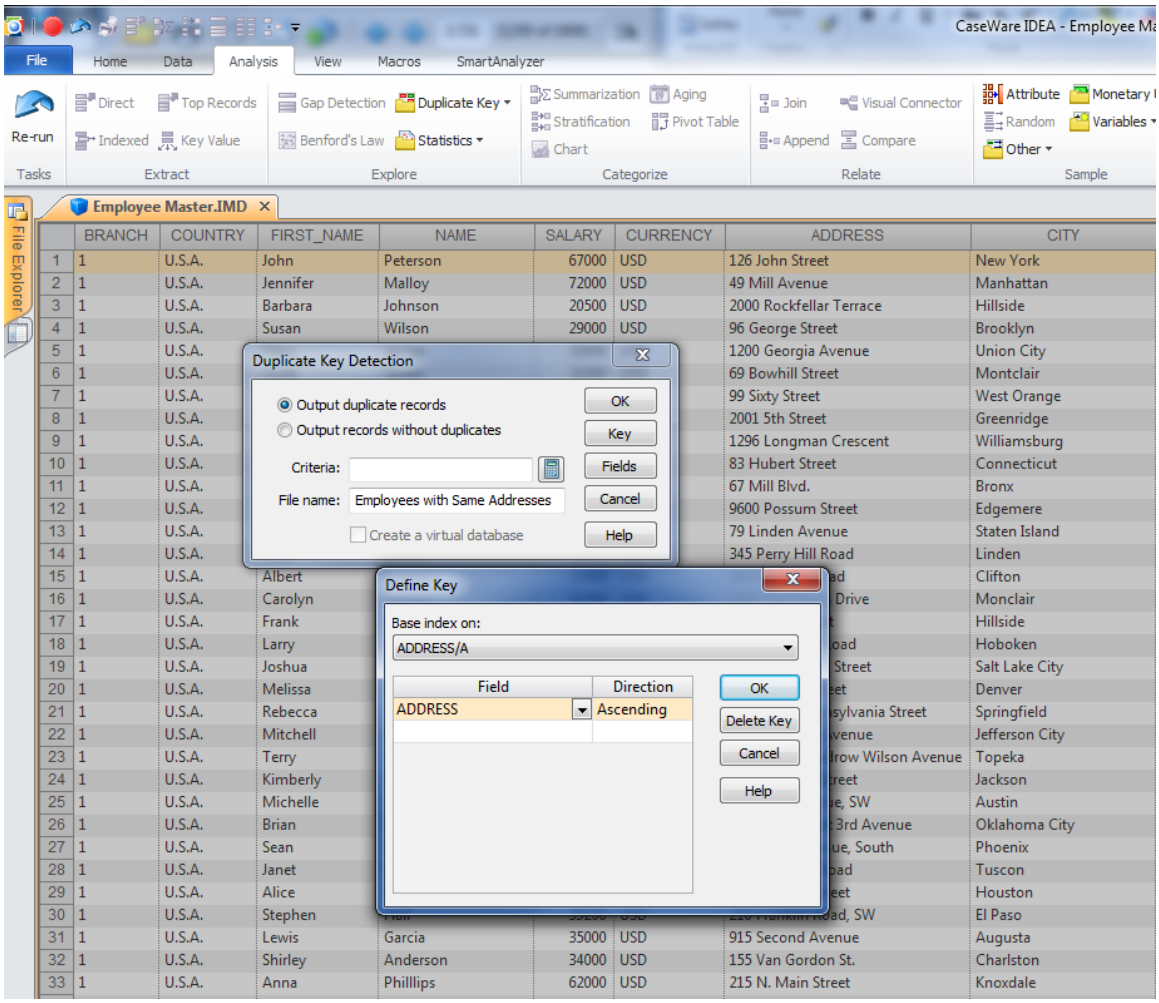
After gathering data, a fraud examiner would first need to determine what kind of tests to run if he suspected a ghost employee scheme. The following are some tests that can help to uncover ghost employee schemes.

- Multiple employees using the same bank account for direct deposit
- An employee using multiple bank accounts for direct deposit
- Invalid or blank tax/government identification numbers
- Multiple employees with the same tax/government identification number
- Multiple employees with the same home address
- Employees with PO Box addresses
- Employees with more than one address change within a year
- Employees on the payroll register prior to their start date or after their termination date
- Non-salaried employees on the payroll register but not in the timekeeping system
- Employees on the payroll register but not in the employee master file
- Manual payroll checks
- Multiple paychecks issued to an employee within a single pay period
- Employees with no deductions for taxes or benefits (where applicable)
- Bonuses paid during times when bonuses are not typically paid or to employees who are not normally eligible for bonuses
- Employees with no pay increases, or more than two pay increases, in the past year
- Employees with no paid time off, vacation time, or sick leave used

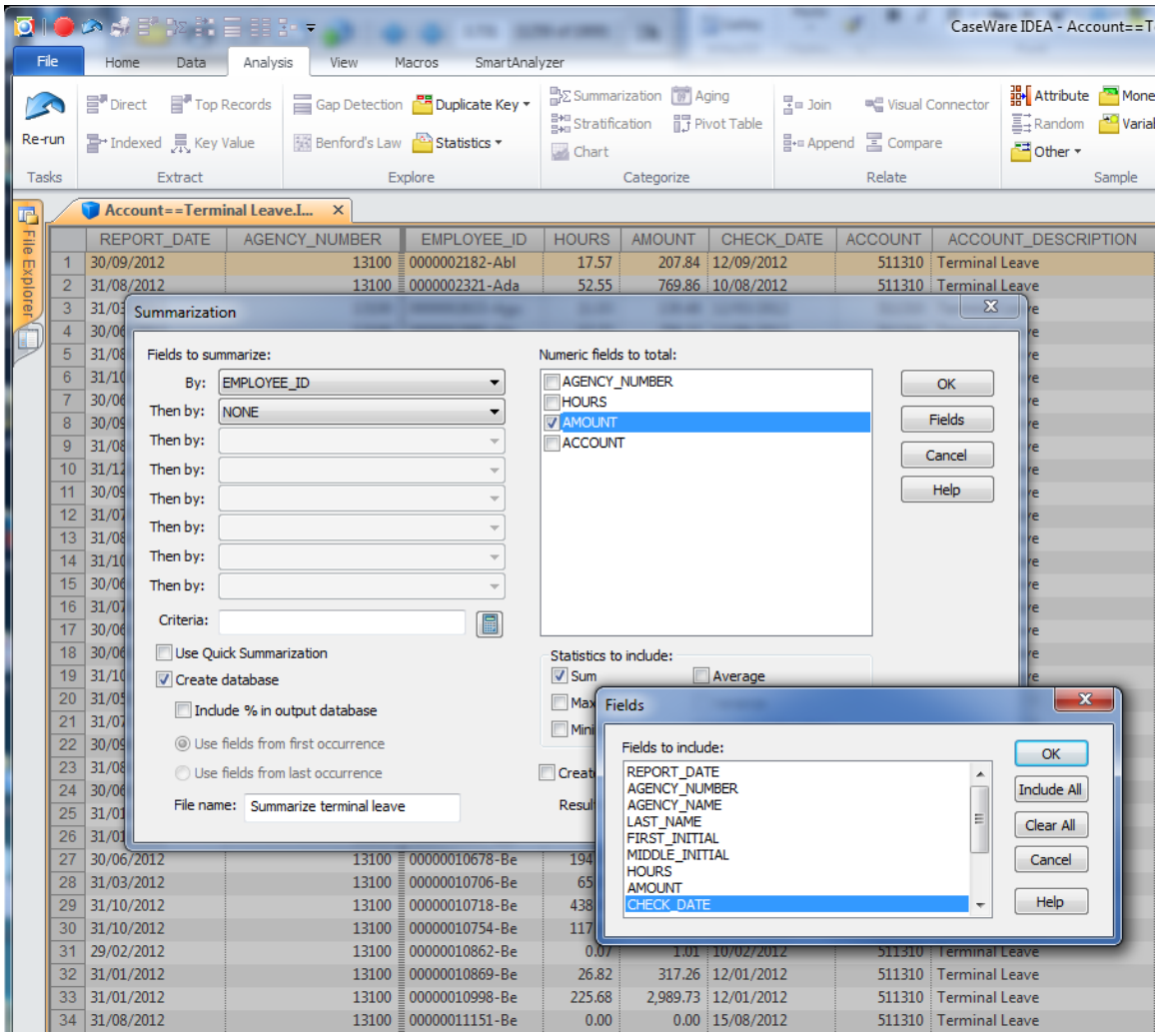
To get an idea of what a couple of these tests would look like using CaseWare IDEA Inc.'s IDEA Data Analysis software, look at the following examples. [4]

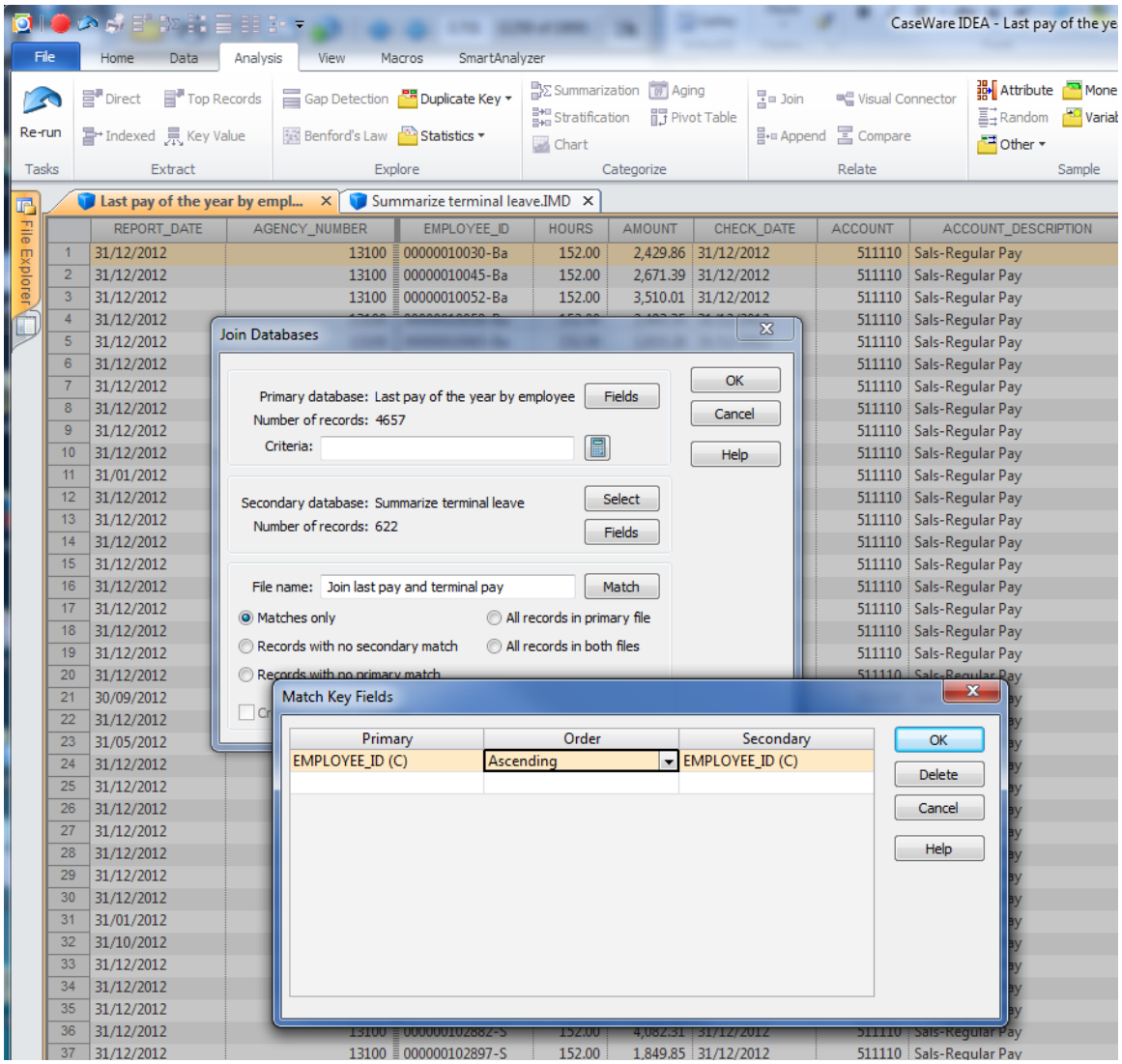
[4] The examples provided by software providers in this manual are for illustrative purposes only. The ACFE has no affiliation with any of these data analysis software providers.

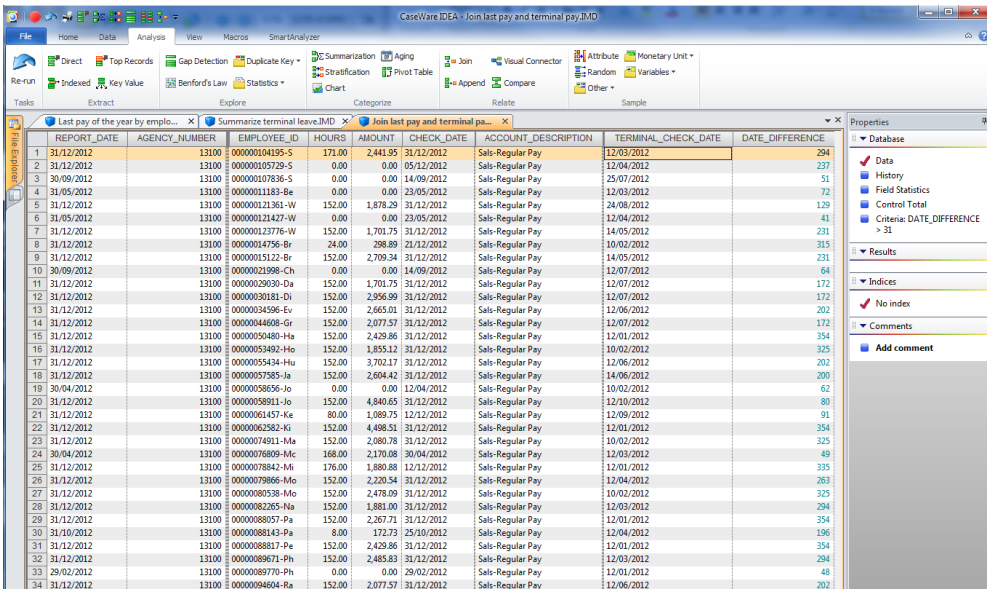
EXAMPLE: TEST FOR EMPLOYEES WITH THE SAME ADDRESS



EXAMPLE: TEST FOR PAYMENTS MADE AFTER TERMINATION DATES




CaseWare IDEA - Last pay of the ye
File
Home
Data
Analysis
View
Macros
SmartAnalyzer
Re-run
Direct
Top Records
Indexed
Key Value
Gap Detection
Duplicate Key
Benford's Law
Statistics
Summarization
Aging
Stratification
Pivot Table
Chart
Join
Visual Connector
Append
Compare
Attribute
Random
Other
Tasks
Extract
Explore
Categorize
Relate
Sample
Last pay of the year by empl...
Summarize terminal leave.IMD
File Explorer
REPORT_DATE
AGENCY_NUMBER
EMPLOYEE_ID
HOURS
AMOUNT
CHECK_DATE
ACCOUNT
ACCOUNT_DESCRIPTION
Join Databases
Primary database: Last pay of the year by employee
Fields
Number of records: 4657
Criteria:
OK
Cancel
Help
Secondary database: Summarize terminal leave
Select
Number of records: 622
Fields
File name: Join last pay and terminal pay
Match
Matches only
All records in primary file
Records with no secondary match
All records in both files
Records with no primary match
Match Key Fields
Primary
Order
Secondary
EMPLOYEE_ID (C)
Ascending
EMPLOYEE_ID (C)
OK
Delete
Cancel
Help


CaseWare IDEA - Join last pay and terminal pay.IMD
Properties
Database
Data
History
Field Statistics
Control Total
Criteria: DATE_DIFFERENCE > 31
Results
Indices
No index
Comments
Add comment

Corruption

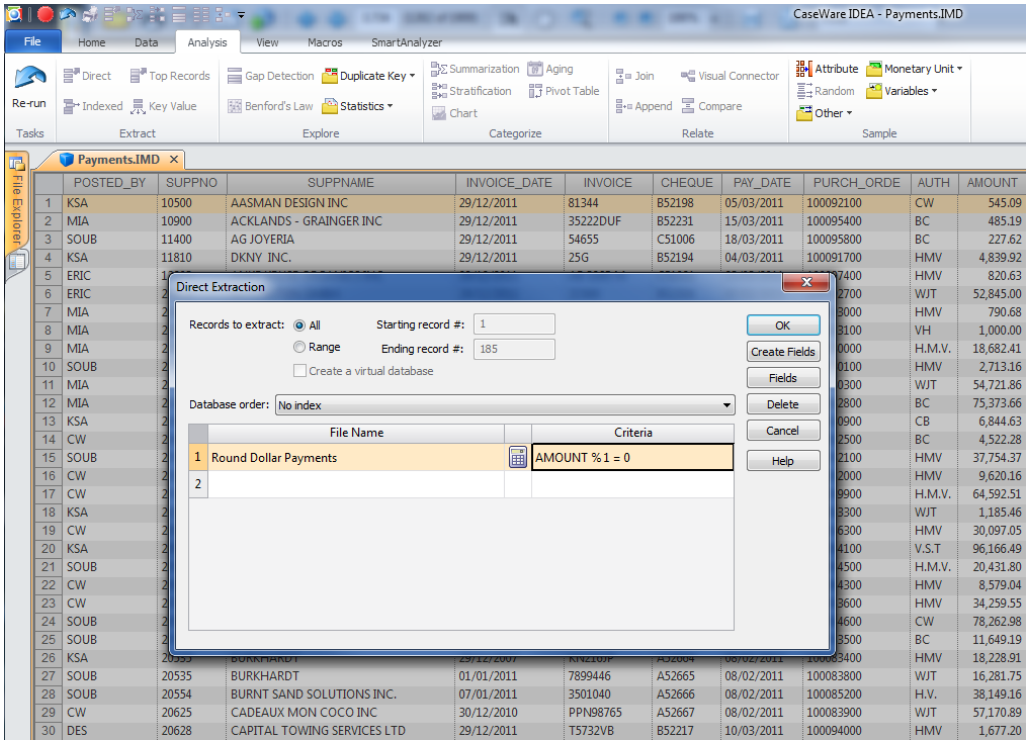
Data analysis can also help during examinations involving suspected corruption schemes. Corruption schemes involve the employee's use of his influence in a business transaction in a way that violates his duty to his employer for the purpose of obtaining a benefit for himself or someone else. Bribes, kickbacks, extortion, and other similar devices are common in corruption schemes.

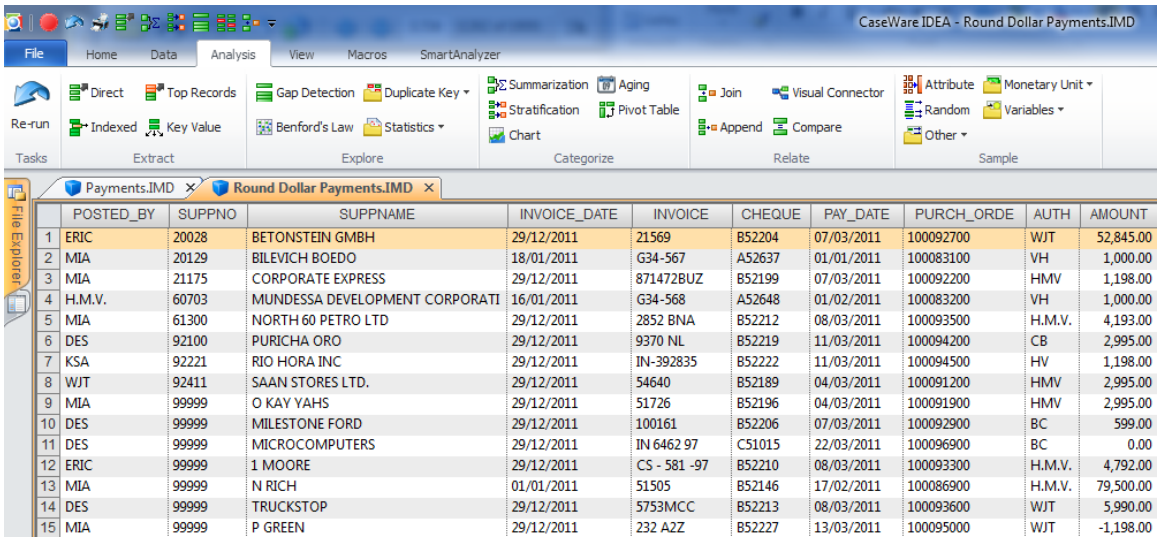
The fraud examiner should determine which types of tests apply to the case. Some examples of corruption-related tests include the following:

- Look for excessive quantities of inventory based on sales.
- Look for obsolete inventory based on quantity sold.
- Identify duplicate payments.
- Stratify vendor payments by approval limits, especially those directly below the approval limit.
- Calculate the ratio of the largest purchase to the next largest purchase by vendor.
- Summarize by vendor the number of inferior goods based on number of returns.
- Match the vendor master file to the employee master file on various key fields.
- Extract round-dollar payments and summarize by vendor.
- Identify payments with little or no sequence between invoice numbers.
- Summarize invoice payments by type of purchase and identify areas with fewer than three vendors.
- Calculate total purchases by ordering clerk and by vendor.
- Compute total business volume by agent and by vendor.
- Match contract price to invoice and report on variances.
- Stratify inventory actual price to standard price.
- Identify higher-than-average inventory costs.
- Compare order quantity to optimal reorder quantity.
- Identify delivery of inventory to employee address by joining employee address to shipment address file.
- Identify delivery of inventory to address not designated as a business address.
- Compare inventory levels and turnover rates.
- Match quantities ordered to quantities received.
- Calculate unit price by product.
- Identify cases in which inventory was written off and then a new purchase was made by comparing total write-off and purchase quantities by stock number.
- Calculate the total number and total value of contracts by contracting officer and by vendor.

- Calculate average value of contracts awarded by vendor.
- Calculate the percentage contract awards by vendor (contracts won divided by total number of bids).
- Calculate the percentage of sole-sourced contracts by vendor (contracts sole-sourced divided by total number of contracts).

EXAMPLE: ROUND-DOLLAR PAYMENTS





	POSTED_BY	SUPPNO	SUPPNAME	INVOICE_DATE	INVOICE	CHEQUE	PAY_DATE	PURCH_ORDE	AUTH	AMOUNT
1	ERIC	20028	BETONSTEIN GMBH	29/12/2011	21569	B52204	07/03/2011	100092700	WJT	52,845.00
2	MIA	20129	BILEVICH BOEDO	18/01/2011	G34-567	A52637	01/01/2011	100083100	VH	1,000.00
3	MIA	21175	CORPORATE EXPRESS	29/12/2011	871472BUZ	B52199	07/03/2011	100092200	HMV	1,198.00
4	H.M.V.	60703	MUNDESSA DEVELOPMENT CORPORATI	16/01/2011	G34-568	A52648	01/02/2011	100083200	VH	1,000.00
5	MIA	61300	NORTH 60 PETRO LTD	29/12/2011	2852 BNA	B52212	08/03/2011	100093500	H.M.V.	4,193.00
6	DES	92100	PURICHA ORO	29/12/2011	9370 NL	B52219	11/03/2011	100094200	CB	2,995.00
7	KSA	92221	RIO HORA INC	29/12/2011	IN-392835	B52222	11/03/2011	100094500	HV	1,198.00
8	WJT	92411	SAAN STORES LTD.	29/12/2011	54640	B52189	04/03/2011	100091200	HMV	2,995.00
9	MIA	99999	O KAY YAHS	29/12/2011	51726	B52196	04/03/2011	100091900	HMV	2,995.00
10	DES	99999	MILESTONE FORD	29/12/2011	100161	B52206	07/03/2011	100092900	BC	599.00
11	DES	99999	MICROCOMPUTERS	29/12/2011	IN 6462 97	C51015	22/03/2011	100096900	BC	0.00
12	ERIC	99999	1 MOORE	29/12/2011	CS - 581 -97	B52210	08/03/2011	100093300	H.M.V.	4,792.00
13	MIA	99999	N RICH	01/01/2011	51505	B52146	17/02/2011	100086900	H.M.V.	79,500.00
14	DES	99999	TRUCKSTOP	29/12/2011	5753MCC	B52213	08/03/2011	100093600	WJT	5,990.00
15	MIA	99999	P GREEN	29/12/2011	232 A2Z	B52227	13/03/2011	100095000	WJT	-1,198.00

Financial Reporting Schemes

If the fraud examiner suspects that someone intentionally misstated or omitted financial statements or disclosures to deceive the users of the financial statements, data analysis techniques can aid the examination.

In addition to traditional horizontal, vertical, and ratio analyses often performed on the financial statements by auditors, the following techniques can help identify anomalies in financial reporting activities:

- Track year-to-date activity for large operating accounts.
- Compare summaries by major account in any order (e.g., low-to-high, high-to-low).
- Identify employees who made a large number of adjustments or reversing entries.
- Calculate and sort percentage variances in accounts between periods.
- Recompute trial balances.
- Prepare account reconciliations.
- Identify large adjustment transactions.
- Review transactions posted at unusual times.
- Review transactions posted on unusual dates.
- Review suspense transactions activity for appropriate and timely clearing and offsets.
- Review transactions split among a large number of general ledger accounts.
- Review transactions with large even-dollar amounts.
- Review debit balances in accounts that have normal credit balances, and vice versa.
- Review manual postings to auto-posted accounts.

Textual Analytics

Data analysis in the traditional sense involves running rule-based queries on structured data, such as that contained in transactional databases or financial accounting systems. This type of analysis can yield valuable insight into potential frauds. But, a more complete analysis requires that fraud examiners also consider unstructured data.

Data are either structured or unstructured. *Structured data* is the type of data found in a database, consisting of recognizable and predictable structures. Examples of structured data include sales records, payment or expense details, and financial reports. *Unstructured data*, by contrast, is data that would not be found in a traditional spreadsheet or database. It is typically text based.

Unstructured Data Sources

The amount of unstructured data is exploding in most organizations. Employees are sending and receiving more email messages each year, retaining more electronic source documents, and using more social media tools. Unstructured data comes from numerous sources, such as:

- Social media posts
- Instant messages
- Videos
- Voice files
- User documents
- Mobile phone software applications
- News feeds
- Sales and marketing material
- Presentations

Textual analytics is a method of using software to extract usable information from unstructured text data. Through the application of linguistic technologies and statistical techniques—including weighted fraud indicators (e.g., fraud keywords) and scoring algorithms—textual analytics software can categorize data to reveal patterns, sentiments, and relationships indicative of fraud. For example, an analysis of email communications might help fraud examiners to gauge the pressures/incentives, opportunities, and rationalizations to commit fraud that exist in an organization.

Textual analytics provides the ability to uncover additional warning signs of potentially fraudulent employee behavior. The following are some examples of how to take unstructured data analytics to the next level:

- Emotive tone—happy, sad, angry, confused communications
- Unethical behavior—harassing, secretive, cursing
- Entity extraction
- Text link analysis
- Social network analysis
- Fraud triangle analytics

Fraud Keywords

Depending on the type of fraud risk present in a fraud examiner's investigation, he will want to come up with a list of fraud keywords that are likely to point to suspicious activity. This list will depend on the industry, fraud schemes, and the data set the fraud examiner has

available. In other words, if he is running a search through journal entry detail, he will likely search for different fraud keywords than if he were running a search of emails. It might be helpful to look at the fraud triangle when coming up with a keyword list.

The factors identified in the fraud triangle are helpful when coming up with a fraud keyword list. Consider how someone in the entity under investigation might have the opportunity to commit fraud, be under pressure to commit fraud, or be able to rationalize committing fraud.

Pressure

Many people commit fraud because of something that has happened in their life that motivates them to steal. Maybe they find themselves in debt, or perhaps they must meet a certain goal to qualify for a performance-based bonus. Keywords that might indicate pressure include *deadline*, *quota, trouble, short*, *problem*, and *concern*.

Opportunity

Think of words that would indicate someone has the opportunity or ability to commit fraud. Examples include *override*, *write off*, *recognize revenue*, *adjust*, *discount*, and *reserve/provision*.

Rationalization

Most fraudsters do not have a criminal background. Therefore, justifying their actions is a key part of committing fraud. Some keywords that might indicate a fraudster is rationalizing his actions include *reasonable*, *deserve*, and *temporary*.

The fraud triangle is a good place to start when developing a keyword list, but also consider the nature of the entity's industry and the types of payments made or suspected of being made. Think about the fraud schemes that are likely to have occurred. Does the entity do a significant amount of work overseas or have many contractors? If so, there might be a high risk of bribery. Focus on the payment text descriptions, since no one calls it "bribe expense." Some examples of words in payment descriptions that should get special attention include:

- *Goodwill payment*
- *Consulting fee*
- *Processing fee*
- *Incentive payment*
- *Donation*
- *Special commission*

- *One-time payment*
- *Special payment*
- *Friend fee*
- *Volume contract incentive*

Any payment descriptions bearing these or other similar terms warrant extra attention to check for reasonableness. Also, be wary of large cash disbursements that have a blank payment description.

Emotional Tone Analysis

Another way to discover fraud clues hidden in text is to consider the emotional tone of employee correspondence. In emails and instant messages, for instance, a fraud examiner should identify derogatory, surprised, secretive, or worried communications. In one example, former Enron CEO Ken Lay's emails were analyzed, revealing that as the company came closer to filing bankruptcy, his email correspondence grew increasingly derogatory, confused, and angry. This type of analysis provided powerful evidence that he knew something was wrong at the company.

While textual analytics can be extremely revealing and can provide clues for potential frauds that might otherwise go unnoticed, it requires the use of sophisticated software, as well as a thorough understanding of the legal environment of employee rights and workplace searches. Consequently, fraud examiners who are considering adding textual analytics to their fraud detection arsenal should consult with technological and legal experts before undertaking such techniques.

Visual Analytics

Even with the sophisticated data analysis techniques previously discussed, some data are so vast or complex that they remain difficult to analyze using traditional means. Visually representing data via graphs, heat maps, link diagrams, time-series charts, and other illustrative representations can bring clarity to a fraud examination.

The utility of visual representations is enhanced as data grow in volume and complexity. Visual analytics build on humans' natural ability to absorb a greater volume of information in visual rather than numeric form and to perceive certain patterns, shapes, and shades more

easily than others. By using mathematical techniques to evaluate patterns and outliers, effective visuals can translate multidimensional data such as frequency, time, and relationships into an intuitive picture.

Fortunately for fraud examiners, many data analytics software programs—including those for conflict checking, link analysis, and timeline analysis—feature visual analytic tools to help uncover relationships, patterns, and other important insights into data.

Tree Maps

A heat map is a graphical representation of data where the individual values contained in a matrix are represented as plots or colors. While not typically used in the detection of fraud, heat maps are an effective visual tool for internal auditors and risk management teams when conducting a fraud risk assessment. The vulnerability an organization faces to different fraud schemes is determined by plotting their likelihood and significance on a heat map.

However, one type of heat map that uses data analysis to detect fraud is the tree map. A *tree map* is a type of heat map in which rectangular space is divided into regions and then each region is divided again for each level in the hierarchy. The size and shading of the rectangles represent two additional data points, allowing the viewer to identify patterns in complex data.

Tree maps are especially effective in showing data represented by several dimensions (e.g., region, department, line of business, product, account, and time period). The hierarchical structure provided by tree maps can reveal multi-faceted information more quickly than spreadsheets, bar charts, or line graphs.

Link Analysis

Link analysis software is used by fraud examiners to create visual representations (e.g., charts with lines showing connections) of data from multiple data sources to track the movement of money; demonstrate complex networks; and discover communications, patterns, trends, and relationships.

Link analysis is very effective for identifying indirect relationships and relationships with several degrees of separation. For this reason, link analysis is particularly useful when conducting a money laundering investigation because it can track the placement, layering,

and integration of money as it moves around unexpected sources. It could also be used to detect a fictitious vendor (shell company) scheme. For instance, the investigator could map visual connections between a variety of entities that share an address and bank account number to reveal a fictitious vendor created to embezzle funds from a company.

The following are some other examples of the analyses and actions fraud examiners can perform using link analysis software:

- Associate communications—such as email, instant messages, and internal phone records—with events and individuals to reveal connections.
- Uncover indirect relationships, including those that are connected through several intermediaries.
- Show connections between entities that share an address, bank account number, government identification number (e.g., Social Security number), or other characteristics.
- Demonstrate complex networks (including social networks).

Geospatial Analysis

Imagine a listing of vendors, customers, employees, or financial transactions of a global company. Most of the time, these records will contain a reference to a location, including country, state, city, and possibly specific street address. By visually analyzing the size or frequency of events in different geographical areas, a fraud investigator has yet another variable with which he can make inferences.

It is important for a fraud examiner to understand the relevance of the location in which events occur to determine and discover patterns in suspicious behavior. In a geospatial analysis, visual analytics depict intersections between various types of data and its corresponding geographical location, helping to uncover a hidden relationship or unknown trend, such as those present in a bribery or corruption scheme.

Geospatial analysis is also especially useful in uncovering fraudulent insurance claims; an insurance fraud ring might be far more obvious when an analyst plots claims data on a map rather than listing it on a spreadsheet. Additionally, analyzing accounts payable and travel and expense risk scoring and overlaying them by the vendor payment or expense location on a geospatial map can help identify high-risk regions.

Timeline Analysis

Timeline analysis software aids fraud examiners in transforming their data into visual timelines. These visual timelines enable fraud examiners to:

- Highlight key times, dates, and facts.
- More readily determine a sequence of events.
- Analyze multiple or concurrent sequences of events.
- Track unaccounted for time.
- Identify inconsistencies or impossibilities in data.

Evaluating Data Analysis Software

Although there are no silver bullets, any data analysis software should possess the following minimum requirements:

- *Data import/export capabilities*: Considering your data format and structure, how easily is data imported/exported?
- *Data visualization*: How easy is it to move your data from a spreadsheet into a graphic for analysis and interpretation?
- *Look for a suite of tools*: There is no single software program for the fraud examiner's fraud intelligence efforts. Therefore, he should choose the most appropriate set of tools according to his available data and then select the software that best fits his current and future needs.

Develop two methods of using the computer to acquire fraud intelligence: Use commercial software currently on the market and begin collaborative activities with the academics at your local university. There are numerous software packages in various stages of development in academia that are in need of data to be tested. This can prove to be a win-win for both parties. The fraud examiner has the data and the academics have the prototype software.

Tailoring Data Analytics Software for Your Organization

Because no single software tool can satisfy all user purposes, fraud examiners must consider the applications with respect to their client's or organization's particular needs. Ken Collier—an expert in data warehousing, business intelligence, software engineering, and agile methods—and his colleagues established a framework for evaluating data mining software.[5]

[5] Ken Collier, Bernard Carey, Donald Sautter, and Curt Marjaniemi, "A Methodology for Evaluating and Selecting Data Mining Software," (IEEE, Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999).

The framework divided the criteria into the following four areas:

- *Performance*: Performance refers to the ability to handle a variety of data sources.
- *Functionality*: Functionality refers to the variety of capabilities, technical methods, and methodology for data mining included in the program.
- *Usability*: Usability refers to the conformation of different levels and types of users without losing usefulness or functionality.
- *Support of additional activities*: Additional task support permits the user to perform the variety of tasks that support data mining.

When creating or updating data analysis techniques, organizations choose a *platform*—the combination of hardware, software, and labor necessary to run the program. Some small organizations create in-house programs. While these can work, they can also be problematic, even if they function properly. Regulators might want to review the organization's controls at some point and might find an in-house program difficult to navigate compared to standard commercial options. Moreover, labor turnover might cause significant disruption, depending on how hard the program is to learn.

Commercial options also have pitfalls to avoid. There are many types available, and some representatives selling the platform will be more interested in maximizing the sale rather than suiting the needs of the organization. Beyond unnecessary costs, a platform that does not suit the organization will either not detect the transactions it needs to, or will return too many false positives (i.e., target suspicious items that turn out to be legitimate), making it hard for analysts to filter the transactions for review.

Because every organization has different needs, there is no all-in-one solution. Organizations should look to the best practices in their industry to see what platforms are effective. Additionally, shopping around with commercial software product representatives helps to develop a picture of which measures are necessary and which are cumbersome. A person with experience in developing platforms for similarly situated organizations should give input into the process.

Evaluating Data Mining Consultants

If an entity intends to use a data mining consultant, the following qualities should be assessed:

- *Innovation*: How does the individual stay current? Look for professional associations, publications, and training in your area of investigation.

- *Creativity*: Can the individual work in a creative environment, such as fraud intelligence? Can the individual work unsupervised and be expected to produce results? Because fraud is a moving target, how has a past client's platform altered from the original investigation? Why/how did that occur? What were the results?
- *Experience*: Does the individual have experience in the type of investigation you are planning? Does the individual have experience in the type of software/tools you are planning to use? Does the individual have experience in the type of data you have?

This expertise might take one, two, three, or more people. It is necessary to have people who understand what it is they are looking for—and what they can do with it once they find it.

Types of Data Mining and Analysis Software

There are many types of data mining and data analysis software on the market these days, and every year, new products and new versions of old products emerge. Because every fraud examination involving data analysis is different, it would be impossible to recommend one software product to serve every purpose. Choosing a data analysis tool is something that the fraud examiner must evaluate on each individual case. A fraud examiner should research applications intensively to decide which package is most appropriate for the current investigation. The most prominent commercial applications include:

- ACL (www.acl.com)
- Caseware IDEA (www.casewareanalytics.com)
- Excel (www.products.office.com)
- ActiveData for Excel (www.informationactive.com)
- Thomson Reuters (risk.thomsonreuters.com)
- DataWatch (www.datawatch.com)
- Arbutus (www.arbutussoftware.com)
- Oversight (www.oversightsystems.com)
- SAS (www.sas.com)

Reporting and Case Management Software

There are a number of reporting and case management programs that can assist the fraud examiner in managing the data and information he gathers during an examination. These programs can also be used to create reports, graphs, and charts of a particular case. Some of the most useful programs for fraud investigations include:

- IBM's i2 Analysis Product Line (www-03ibm.com)
- CaseMap by LexisNexis (www.lexisnexis.com)

- Actimize Enterprise Risk Case Manager (www.niceactimize.com)
- Xanalys Suite (www.xanalys.com)
- Infoglide Software (www.infoglide.com)
- Regulatory DataCorp (www.rdc.com)
- World-Check (risk.thomsonreuters.com)
- Safe Banking Systems (www.safe-banking.com)
- GlobalVision Systems (www.gv-systems.com)
- Detica NetReveal Enterprise Investigation Management (www.bobsguide.com)
- i-Sight Investigation Software for Case Management (i-sight.com)
- NAVEX Global (www.navexglobal.com)

DIGITAL FORENSICS

Conducting an Investigation Involving Computers

The presence of the Internet and other technology in all aspects of life has created new opportunities for technology to be used in perpetrating almost every type of fraud, and in most fraud cases, investigators gather some type of digital evidence.

Fraud examiners must, therefore, be prepared to address the myriad issues related to examinations involving digital evidence.

Digital Investigations Versus Digital Forensics

While the term *digital investigation* might at first appear synonymous with *digital forensics*, there is an important distinction between the two. *Digital investigations* are investigations that involve relevant digital data processed or stored by *digital devices*—devices that process data in the form of numbers (digits). Digital devices can be used to communicate with others, create documents, access data online, enter data online, store information, and so on. An investigator leading an investigation into a crime that involves a digital device is not necessarily—and, in most cases, should not be—the forensic examiner.

Conversely, *digital forensics* encompasses the recovery and investigation of material found in digital devices.

It is important to keep digital investigations and digital forensics separate. Combining the two, especially in cases in which the suspect is already named, will invite questions about the forensic examination's objectivity. Also, combining the two could subject investigators to unwelcome scrutiny regarding whether they suppressed exculpatory evidence that might have been found during an examination by a more objective investigator.

Hiring Digital Forensic Experts

When conducting an examination involving computers, fraud examiners should determine whether a digital forensic expert is needed. *Digital forensic experts* are individuals who specialize in identifying, recovering, collecting, preserving, processing, and producing digital data for use in investigations and litigation. Some organizations have their own in-house personnel whom they have trained and outfitted with the proper equipment and software tools to conduct the examination and analyze digital evidence, while others might prefer the use of

an outside examiner who will be able to conduct a thorough examination, prepare a proper report, and deliver expert testimony if needed in legal proceedings.

Sometimes retrieving digital data is as easy as searching the target computer's hard drive, but other times retrieval requires a thorough knowledge of computers. For example, many fraudsters delete or hide incriminating files, and in these instances, efforts must be made to recover or find such data. There are, in fact, a variety of ways of recovering deleted or hidden data from a target computer, and digital forensic experts are specially trained for such tasks.

Specifically, digital forensic experts are capable of analyzing digital media at the hexadecimal level, which means that such experts can view every sector, and all the bytes in those sectors, on a system. Thus, digital forensic experts can recover data from deleted files, both those that have been purposefully deleted and those that were accidentally deleted. Deleted files are recoverable until they are overwritten because data is not erased from a computer's hard drive until it is overwritten. A deleted file will remain present on a hard drive until the operating system overwrites all or some of the file. So, deleted files that have been overwritten generally are not recoverable. Digital forensic experts can also recover temporary auto-save files, print-spool files, deleted emails, and deleted link (shortcut) files, and they can work with data at the hexadecimal level. The hexadecimal level contains various items found in restore points and registry files that define hardware, such as external drives and websites visited, in addition to the document revisions and files created and maintained by the user.

Computer forensics specialists can recover, among other things, the following types of information from computer systems:

- Deleted files and other data that has not been overwritten (e.g., deleted documents, images, link or shortcut files, and email messages)
- Files deleted through computer-automated processes
- Temporary auto-save files
- Print-spool files
- Websites visited, even where the browser history and cache have been deleted
- Communications sent via chat or instant messenger
- Financial-based Internet transactions
- Documents, letters, and images created, modified, or accessed, even if the data was not saved on the computer in some situations
- Data that has been copied, corrupted, or moved

- The time and date information about files (e.g., when files were created, accessed, modified, installed, deleted, or downloaded)
- Data from a drive that has been defragmented or reformatted

The increased sophistication of hardware and operating systems allows computer systems to store more information about how people use their computers, and therefore, the digital forensic examiners are able to uncover a large amount of data that relates to the use of a computer, what is or has been stored on it, and the details about the computer's user.

Moreover, digital forensic examiners have special tools and software designed to facilitate a thorough and legally sufficient analysis of items that contain digital evidence. It is important to allow a trained digital forensic expert to conduct a proper seizure and examination on a piece of evidence so the investigator will have the best chance of using that evidence in a legal proceeding.

Furthermore, whether technical specialists are needed to assist with an investigation will depend on the complexity of the examination required. The more technical the nature of the crime, the more technical and specialized the analytical skills required. Some computer investigations do not require sophisticated technical skills. For example, in cases where the computer is the instrument used to commit the crime (e.g., scams involving payroll applications, accounting irregularities, fraudulent electronic funds transfers, or insider trading), the fraud examiner need only know how to search a database and analyze the results.

Additionally, the determination as to whether a specialist is needed will depend on the fraud examiner's skill level. Therefore, a fraud examiner conducting an examination involving computers must have a basic understanding of his skill level and must be aware of his limitations in the field of computer technology because, in many instances, one or more technical specialists are needed to assist with an investigation.

Within the computer forensics field, there are several different types of special experts:

- *Operating and file system experts*: These experts are proficient in certain operating systems (e.g., Windows Vista, Windows 7, Windows 10, Linux, and OS X) and the various file systems they employ (e.g., Joliet, NTFS, FAT, VFS, Ext2), and they have the ability to convey operational characteristics and observe artifacts.

- *Data recovery experts*: These experts operate clean rooms designed to magnetically extract information from a damaged media source. Using special tools and equipment, these experts can disassemble a hard disk, separate the platters, and extract and reassemble the information for subsequent examination.
- *Forensic accounting experts*: Forensic accounting is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation, and a forensic accountant can provide various services, including audits, accountant performance reviews, and examinations of financial documents for fraud, misconduct, or industry standard violations.
- *Recording and archival extraction experts*: These are experts in extracting information from tapes, digital media, or other system backups. Typically, backup solutions archive data in proprietary formats, making extraction very cumbersome.
- *Intrusion and malicious code experts*: These experts specialize in investigating computer network intrusions. Specialists can determine attack vectors, the tools employed, what occurred during access, and what, if anything, was taken.

Given the diversity of computer-related fraud, no person can be an expert in all aspects of computer technology.

If a fraud examiner decides to hire a forensic expert, he must be diligent when hiring the expert. The best way to hire an expert is to follow a few simple guidelines:

- Ask colleagues for referrals.
- Make sure the expert is properly licensed (if required) and insured.
- Ask the experts if they have worked on the type of case that is at issue, and if so, what they were retained for and the outcome.
- Set up a budget for the investigation.
- Make sure there is a comfortable relationship and good communication between the client and the expert.
- Listen to the expert because he might have new, unique ideas and suggestions that were not previously considered.

Determine the Need for Law Enforcement Assistance

Once an organization has received evidence that misconduct involving digital devices has occurred, it should determine the need for law enforcement assistance. If it is determined that the victim organization will make a formal referral to law enforcement or a prosecuting

agency, then the organization should notify the authorities before conducting an investigation to determine whether law enforcement personnel should participate in the examination.

Digital Evidence

Digital evidence is information stored or transmitted in binary form (i.e., ones and zeroes) that can be used to prove something. And again, the proliferation of digital technologies has created new opportunities for technology to be used in perpetrating almost every type of fraud. Consequently, fraud examiners will gather some type of digital evidence in almost all fraud examinations.

Generally, when digital data is collected in an investigation, the facts at issue involved a computer, either as (1) a target of a criminal act, (2) an instrument of crime, or (3) a repository of evidence associated with the crime.

Computers themselves can be the targets of crime. Crimes committed against computers include computer and computer-component theft, system intrusions, software piracy, and software theft.

Computers can also be used to facilitate criminal conduct. When this occurs, the computer is known as the *tool* or *instrument* of crime.

Additionally, computers can be repositories of evidence associated with a crime. Generally, in an examination involving computers, the fraud examiner attempts to locate the storage of potential digital evidence, in one form or another, on the computer system. The computer system involved in the investigation is a potential repository of evidence whether the user intended to store an item or not. Therefore, in such situations, the fraud examiner is interested in incriminating evidence that the user intentionally or unintentionally stored on the computer system.

Volatility of Digital Evidence

Digital evidence is more volatile than tangible information because data can be altered or destroyed more easily than tangible information. Digital data is, by design, fragile and short-lived in nature. It is easily manipulated, substituted, modified, and deleted.

Generally, if a computer system is on, its files will be changing. Operating systems and programs frequently alter, delete, and modify digital data, and this might happen automatically. Moreover, if a user interacts with a system, its files will change. In fact, digital information can be altered by seemingly harmless actions, such as shutting down a running system, starting up a system, or looking through files on a running computer. Also, if a computer system is connected to a network, its files will be changed.

The following is a list of some actions that can alter, delete, or modify data that is potentially relevant to an investigation:

- Using or interacting with a computer system
- Clicking on files or folders on a computer, which will result in information being written to the system's hard drive and could potentially overwrite valuable evidence
- Turning systems on or off
- Visiting websites
- Using software applications
- Downloading or transferring files

And because digital evidence can be easily altered or destroyed, the integrity of digital evidence must be preserved. Data that has been altered or destroyed are considered violations of data integrity. What is more, the alteration or destruction of digital evidence is irreversible. So, once the integrity of digital evidence has been violated, it usually cannot be restored.

The failure to preserve the integrity of digital evidence could result in several adverse consequences. For one thing, the failure to preserve the integrity of digital evidence could result in the government's questioning of the integrity of any evidence collected in a fraud investigation.

For another thing, digital evidence that is destroyed when litigation is expected, or in progress, might give rise to claims of spoliation of evidence, which, if proven, could lead to monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defenses. *Spoliation* is broadly defined as the act of intentionally or negligently destroying documents relevant to litigation.

Additionally, the failure to preserve the integrity of digital evidence could result in evidence being deemed inadmissible in a legal proceeding, or, even if admitted, it might not be given much weight because evidence of questionable authenticity does not provide reliable proof.

Generally, evidence will not be admitted (or it might not constitute reliable proof of what it is offered to prove) unless it is authenticated. Evidence is authenticated when the party offering the item produces some evidence (e.g., testimony from a person with direct knowledge) to show it is, in fact, what the party says it is and to show it is in the same condition from the moment it was seized until it is used in court. Thus, if it is determined that a piece of digital evidence cannot be authenticated, it might not be admitted even if it is plainly relevant, or it might be rejected because it is deemed unsuitable to prove the facts in question.

Although digital evidence is different from tangible evidence, the rules regarding the admissibility of digital evidence in court are really no different from the rules regarding the admissibility of any other type of evidence.

The rules of admissibility, however, differ in civil law and common law systems. Because civil law systems do not rely on juries like common law systems, there is a relative lack of restrictions on the admissibility of evidence in civil law systems. Thus, there are far fewer limitations on the admissibility of evidence in civil law trials than in common law ones.

Generally, in civil law systems, evidence is admitted if the presiding judge determines it is relevant, even if the authenticity of an item of evidence is in question. But even though any relevant evidence is admissible, the court will evaluate how much weight is to be given to an item of evidence, and courts consider authenticity when determining what weight is appropriate for evidence. Authentic evidence is reliable proof of what it purports to show, but evidence that lacks authenticity is not reliable proof of what it purports to show. So, even if an item of evidence of questionable authenticity is admitted, it will not be given much weight because it will not be helpful to a fact finder due to the fact that such evidence is not reliable proof of what it purports to show.

In contrast, the common law contains several rules that restrict admission of evidence. But generally, to be admitted into evidence in common law systems, evidence must, in addition to being established as authentic, be:

- *Relevant to an issue that is in dispute in the case*: Relevant evidence is evidence that tends to make some fact in issue more or less likely than it would be without the evidence.
- *Material*: Material evidence is evidence that has important value to a case or that can be used to prove a point. Repetitive or additive evidence is nonmaterial evidence.

Therefore, if a fraud examiner collects digital evidence, he should be able to state unequivocally that the evidence was not changed in any way by his actions. This requires that strict forensic methodologies be followed to satisfy the stringent evidentiary standards necessary to ensure the integrity of the evidence beyond a reasonable doubt for presentation in court. That is, digital evidence must be properly preserved in a forensically sound manner so that it will be admissible.

Locating Digital Evidence

To conduct a successful examination, fraud examiners must know what to look for and where to look for it, but this can be difficult because digital data can be stored in large volumes and in a number of different locations. For example, the fraud examiner should know where to look for information on any suspect computer systems, information on a suspect's workstation, including any peripherals or other portable media devices that contain data, information stored on any network from which the suspect's traffic flows, and information stored in cloud storage services.

This discussion examines where digital evidence might be located on computer systems, workstations and peripheral devices, networks, smartphones, and cloud environments.

COMPUTER SYSTEMS

A wealth of information can be recovered and analyzed on seized computer systems. Common files containing evidence stored in computer systems include user-created files, user-protected files, and computer-created files.

USER-CREATED FILES

User-created files are digital files created under the user's direction, and these files include text-based documents, spreadsheets, databases, emails, address books, presentation slides, audio/video files, image files, Internet bookmarks, and so on.

USER-PROTECTED FILES

Often, users hide files to prevent them from being found. There are a variety of techniques to hide files, but some of the most common methods include camouflaging, steganography, and encryption.

A user might camouflage certain files under an innocent name or different file extension to prevent others from discovering them. For example, a suspect might change a file name from "evidence.doc" to "install.exe" and place the file in a directory that stores program files. Therefore, fraud examiners should analyze a target's hard drive to determine whether any file types have been camouflaged. This is done by analyzing the file header—the first bits of data in a file—which contains data identifying the file format.

A user might also seek to protect files using steganography. *Steganography* is the process of hiding one piece of information within an apparently innocent file. For example, a user can use the least significant bits of a bitmap image to hide a message. By hiding the message in the least significant bits of an image, there is almost no perceivable change in the bitmap image itself. And without directly comparing the altered image to the original, it is practically impossible to tell that the image was altered.

EXAMPLE

After a French defense contractor suspected that some of his critical designs were being compromised, the government conducted an investigation. The investigation revealed that an employee had obtained his position at the company to steal the contractor's trade secrets. To transmit the trade secrets out of the company, the employee imbedded them into graphic images used on the company's public access website using steganography. Another party then copied the image files from the website and extracted the proprietary designs.

Digitized audio files are another type of file that can be used to hide messages. For example, by encoding a message in the least significant bits of a WAV file, a user can make the message almost impossible to detect.

There are a number of tools that investigators can use to detect steganography, and these tools use different methods to detect the use of steganography. Some common methods of detecting the use of steganography are:

- Visual detection by looking for visual anomalies in jpeg, bmp, gif, and other image files
- Audible detection by looking for audible anomalies in wav, mp3, mpeg, and other media files

- Statistical detection by determining whether the statistical properties of files deviate from the expected norm
- Structural detection by looking for structural oddities that suggest manipulation (e.g., size differences, date differences, time differences, or content modification)

A user might also protect files by encrypting them. *Encryption* refers to procedures used to convert information using an algorithm (called a *cipher*) that makes the information unreadable to anyone without the encryption key. There are two primary ways to access encrypted information without a key. First, numerous utility programs can decrypt documents encrypted by many of the more common software applications. In addition, some encryption programs have a secret "key" for emergencies that may be used to decrypt encrypted data. There are also several companies that specialize in decryption.

Second, there is precedent for forcing a suspect (or employee) to divulge the decryption key. The computer is only a container and encryption is an additional lock prohibiting the investigator from reviewing the files for potential evidence. A fraud examiner with a legal right to examine encrypted data might be able to force a suspect to divulge the decryption key because doing so is no different than ordering a suspect or employee to unlock a file cabinet to inspect its contents.

COMPUTER-CREATED FILES

Evidence might also be found in information generated by a computer's operating system. This type of information is important because it can identify that a certain activity has taken place, and in most cases, the user is not aware that this information is being written. Some common examples of computer-generated data available for examination include:

- *Metadata*: Metadata is data about data, and these file tidbits contain a tremendous amount of information. Metadata information can help determine who wrote a document; who received, opened, copied, edited, moved, or printed the document; and when these events occurred.
- *Registry*: The registry, which is a central database that stores settings and configurations for the operating system and most applications installed on the system, is an important source of potential evidence because it contains information on user accounts, typed URLs, networks shared, the run command history, and so on.
- *Event logs*: Every operating system generates event logs, files that record events or transactions on a computer. In fact, a log entry is created for each event or transaction that takes place on any computer, and consequently, there are numerous types of event

logs. Some common types of logs include system logs, application logs, and security logs. *System logs* record events executed on an operating system, including miscellaneous events and those generated during system startup, like hardware and controller failures. Other common types of system events include starting up and shutting down, configuration updates, and system crashes. *Application logs* record the events regarding access to application data. Such events would include data files being opened or closed; specific actions such as reading, editing, deleting, or printing of application files; or the modification of records in an application file. *Security logs* track security-related events like logon and logoff times and changes to access rights.

- *Internet activity*: Internet browsers create temporary files that store information about websites that a user has visited. These files can show websites that were recently visited and usually include time and date information relevant to the visit; they can also show images previously viewed online. This information allows the fraud examiner to recover websites and images previously viewed by the system's users.
- *Temporary files*: Applications will create temporary files like those created by Internet browsers. For example, certain communication software like instant messaging (IM) and chat software will keep a history of the user's conversations in a proprietary and sometimes encrypted format.
- *Deleted data:* Deletion is a widely misunderstood function in computing because deleting data is not the same as destroying data. Choosing the delete option erases the file's reference from the table of contents, but it does not erase the file. In fact, data is not erased from a computer's hard drive until it is overwritten. Therefore, deleted files might be recoverable.

WORKSTATIONS

In addition to investigating any computer systems at issue, evidence might be stored on any form of technology that can be used to transmit or store data. Therefore, it is also important to investigate any suspect workstations, including any peripherals or other portable media devices that can be used to transmit or store data. A *peripheral device* is an auxiliary device that is connected to, but not part of, a host computer.

As data moves to and from peripheral devices, it leaves evidence of its presence and sometimes leaves full copies of its contents. Therefore, fraud examiners should consider the many different types of peripherals that might contain evidence. Items to be seized might include any or all of the following items, depending upon the nature of the fraud case.

PRINTERS

Fraud examiners must be aware that it might be possible to recover previously printed documents. Although the odds of recovery can be low depending on a variety of factors, understanding how retrieval can be achieved can be of great value to the investigator.

Printers might contain valuable evidence. Many printers have internal hard drives that could contain information relevant to a fraud examination. In general, any information sent to and stored by a printer is recoverable unless the printer has overwritten the data. So, when seizing a computer for forensic analysis, it is generally necessary to seize any printers connected to it.

In addition, when a printer is connected directly to a computer (when a printer is connected in this way, it is referred to as a local printer), it might be possible to recover print data from print-spool files, which are stored on a system's hard drive. When computers running Windows operating systems print files, a print-spooling process occurs. The process involves writing the print job to files, allowing users to keep working while the print job runs in the background. After the user creates a print job, it is not immediately sent to the printer; instead, it is stored in a local file that is sent to the printer when the printer becomes available to perform the job. Once printing is complete, the operating system deletes the files; but again, deleted files can be recovered.

Furthermore, some printers have *memory buffer*—temporary storage area of jobs waiting to be printed—which might also contain important information. Information contained in memory buffer, however, is generally limited to recently created and stored data.

COPIERS, SCANNERS, AND MULTIFUNCTION DEVICES

Copiers, scanners, and other multifunction devices—machines that provide printing, copying, scanning, and faxing functionalities in one device—might have internal storage devices that store relevant data. In fact, almost every copier built since 2002 has a hard drive that stores images of documents the machines have copied, scanned, or emailed. Some copiers store user access records and a history of copies made. And, as with most file systems, it might be possible to retrieve information from a copier's hard drive that has been deleted. As a result, a copier might be brimming with important information. So, when seizing a computer for forensic analysis, it is generally necessary to seize any copiers and scanners connected to it.

FAX MACHINES

Although some kinds of stand-alone fax machines simply scan and send data without storing it, like many printers and copiers, some fax machines store faxing data on their own internal hard drive. This data might remain in the machine's memory until overwritten.

BACKUP STORAGE DEVICES

Backup storage devices store data, and some of them can be easily removed from a computer system. Most computer users archive their activities on backup devices, and most companies use them to store old data, including archived emails, that was once stored on their servers.

REMOVABLE STORAGE DEVICES

In addition to backup devices, any relevant removable storage devices should be examined. Removable storage devices such as CDs, DVDs, USB flash drives, mp3 players, and various other devices provide users with the ability to store large amounts of data. Such devices can be used to facilitate a variety of frauds. They provide users with the ability to store files that go undetected by anyone accessing the computer. Removable media can also be used to store copies of files containing sensitive information to facilitate unapproved use.

NETWORKS

In addition to searching for evidence on the suspect's workstation, it is also important to examine information stored on any network from which the suspect's traffic flows. A wealth of information that is separate from a user's workstation might be stored on company servers. Data stored on networks might include documents posted to a suspect's own home directory on the network; collaborative work saved to a shared folder or directory; email messages that have been sent, received, deleted, or archived; calendars; contact lists; and so on.

SMARTPHONES

The proliferation of smartphones has made them an extremely valuable source of information. Smartphones (e.g., Androids and iPhones) are mobile phones that also have the ability to store personal data, search the Internet, check email, instant message (IM), make video calls, download/upload content to and from the Internet, take pictures, and record video. The information that can be stored on these small devices can be very important in many cases. For more information on recovering evidence from smartphones, see the subsequent discussion on mobile forensic investigations.

CLOUD ENVIRONMENTS

Organizations and individuals are increasingly storing data and applications on the cloud. The cloud is a metaphor for the storage and utilization of data online rather than locally. *Cloud storage* refers to information stored by a third-party host that is accessible online.

Cloud computing offers numerous benefits. For one thing, the cloud can provide savings on hardware, software, or licensing fees, and cloud services offer a cost-effective alternative to building out IT infrastructure. For another thing, the cloud improves accessibility because users can access the cloud anytime and anywhere. And finally, with cloud computing, organizations can easily scale information technology resources up or down to suit their business needs.

Virtually anything that can be stored on a hard drive can be uploaded to the cloud (available space is normally the primary limitation). Accordingly, information relevant to a fraud examination might be stored in the cloud. Fraudsters might save records or other key evidence to cloud storage to avoid possessing a copy on their own storage devices, so fraud examiners should search these places, if possible.

Determining whether a subject uses cloud storage can be done by searching for payments made to cloud services, browser history (for types of cloud storage accessed via browsers), smartphone applications linked to cloud services, or making a request through discovery in litigation.

Computer Investigations and Computer Forensics

The following discussion provides a process for conducting investigations involving computer forensics. Although there are several definitions and different schools of thought for investigations involving computers, most practitioners in the field will agree that investigations typically involve the following phases:

1. Planning
2. Seizing
3. Imaging
4. Processing
5. Analyzing
6. Reporting and testifying

Each phase is dependent on the phases that come before it. For instance, if the seizure phase is handled incorrectly, then each of the following phases can suffer and ultimately render the reporting and testifying phase moot.

Planning

Before the fraud examiner can seize evidence, he must take certain steps to help ensure that the evidence will be admissible: He must determine whether there are any privacy interests in the item(s) to be searched; he must take certain steps to prepare for an investigation that involves the use of a legal order; and he must take steps to ensure that his equipment is sound (e.g., only use licensed software applications, independently validate all forensic equipment, and maintain the validation on file).

Privacy Issues

Before searching and seizing an item, the fraud examiner must determine whether the individual who is the subject of the search has a privacy interest in the item(s) to be searched. In every case where it becomes necessary to seize a computer or other device capable of storing digital evidence, the investigator should consult with legal counsel. It is imperative that legal counsel be involved in the seizure process, and the fraud examiner must be knowledgeable of the law pertaining to workplace seizures.

Likewise, when conducting an examination in the workplace context, fraud examiners must determine whether the employee who is the subject of the search has a privacy interest in the item(s) to be searched.

Generally, if an individual has a reasonable expectation of privacy in an area being searched or items being seized, privacy rights provide protection against unreasonable searches and seizures.

Employers, however, can lower employees' expectation of privacy in the workplace. To lower employees' expectations of privacy, employers should adopt written privacy policies that put employees on notice that their workplace is not private and should require employees to sign it. Such policies should provide that, to maintain the security of its operations, management may gain access to and search all work areas and personal belongings, including desks, file drawers, lockers, briefcases, handbags, pockets, and personal effects.

Such privacy policies should also notify employees that all computer systems (e.g., the Internet, email communications, hardware, and files) are solely for business use and that the company reserves the absolute right to review, audit, and disclose all matters sent over the system or placed in storage.

Moreover, employees often carry personal electronic devices into the workplace, and because such devices can be used to facilitate fraud or other types of misconduct, employers should include the right to search such devices in their privacy policies. Personal electronic devices such as smartphones, USB flash drives, MP3 players, and laptops are capable of a multitude of functions that can be used to facilitate fraud or other misconduct, but because they are personal devices, employees can have privacy rights with respect to the contents stored in them. Employers, however, can retain the right to search employees' personal electronic devices by adopting written privacy policies stating that any personal electronic devices brought onto the organizations' premises are subject to search. This type of policy serves to lower employees' expectations of privacy in personal electronic devices by putting employees on notice that such devices are not private and are subject to search.

For more information, see the "Individual Rights During Examinations" chapter in the Law section of the *Fraud Examiners Manual*.

Seizing

Perhaps the most critical step in the forensics process is how data is collected or acquired. Acquisition of digital evidence must be completed in such a way as to ensure that all relevant evidence is seized and secured in a forensically sound manner so that the evidence is not tainted or destroyed.

In fact, there are a number of practical considerations and procedures to employ when the decision is made to go forward with a computer seizure. For example, fraud examiners often fail to debrief the subject, which should be a primary consideration for any examination involving computers. Debriefing the subject involves asking the subject for passwords and whether any encrypted data exists on the target computer.

The Scientific Working Group on Digital Evidence (SWGDE) from the Organization of American States has published a document, titled *Best Practices for Computer Forensics*, which provides a good foundation for digital forensics examiners.[1]

Although a complete review of the entire document is beyond the scope of this manual, several guidelines deserve review. According to the SWGDE, examiners should adhere to the following guidelines:

- Before obtaining evidence, ensure that there is legal authority to seize evidence and review the data associated with the evidence. This might require obtaining a warrant in a criminal matter or ensuring that internal policies authorize seizure for an internal investigation.
- If removing evidence from the scene is impractical, copy or image the items of evidence according to established procedures.
- Remove all suspects, witnesses, and bystanders from the proximity of the digital evidence. Keep in mind that remote access to computers can put potential evidence at risk even if no person has physical access to the computer. Also, consider the wide range of mobile data storage devices today (e.g., USB flash drives) that can be hidden.
- Ensure that no suspects, witnesses, and bystanders possess any items containing potential evidence.
- Thoroughly and systematically search the scene for potential evidence. Once again, consider the wide range of data storage media and devices.

Generally, data should not be analyzed on the machine from which it was collected. Instead, the examiner should make forensically sound copies of all data storage devices—primarily hard drives—and analyze the data on these copies.

Moreover, when seizing a computer that is running, the party seizing the system should not, in most situations, use the computer or search it for evidence. Any such use of a computer could damage and taint any evidence that it might contain.

To ensure that a machine can be fully analyzed, the fraud examiner should adhere to the following practices:

1. Examine and document the machine's surroundings.
2. Inspect for traps.

[1] Scientific Working Group on Digital Evidence of the National Center for Forensic Science. *Best Practices for Computer Forensics* V2, 2006. www.oas.org/juridico/spanish/cyb_best_pract.pdf. In June 2014, the SWGE posted a draft of version 3.1 of its *Best Practices for Computer Forensics* for public review and comment.

3. If the computer is off, leave it off.
4. Consider collecting volatile data "live."
5. Secure the evidence.
6. Image the system hard drives.
7. Document the collection process.
8. Implement a system to manage the evidence.

Examine and Document the Machine's Surroundings

The first step in the evidence-collection process is to examine and document the machine's surroundings. The party seizing the computer should collect all printouts, disks, notes, and other physical evidence for further analysis, and he should document the scene with photographs or a diagram, depending on the complexity of the setup. Documenting the machine's surroundings is important because the party seizing the computer might have to testify about what the area looked like on the day of the seizure, and it might be a year or longer before such testimony occurs.

The party seizing the computer should also document the condition of the machine and any relevant evidence. When doing this, the examiner should consider:

- Documenting what is on the screen, if the system is on
- Documenting any processes that are currently running
- Taking photographs of the various views of the equipment and media to document any damage or defects
- Taking photographs of the equipment's physical connections
- Making a drawing of the location to document the layout and relative locations from which evidence was seized

Additionally, because many people write down or record their passwords near their computers, fraud examiners should look around for notes that might appear to be passwords. This might aid in discovering passwords needed to access encrypted or password-protected data if the individual who knows the password is uncooperative and will not divulge it. Although there are ways to access encrypted information without an encryption key—decryption, emergency keys, forcing cooperation—having the passwords for protected files will save time and reduce efforts.

Fraud examiners should take good notes on the machine's state at the time of the seizure, and record the time and date that the system was seized and the personnel involved in the

seizure. The status of the system should also be noted. Was it on, off, or on standby? Was there anything unusual attached to the system? Was there any obvious damage? Did any files have to be saved? Also, if the computer was active, the fraud examiner should record any open applications. Furthermore, he should make sure to start a chain of custody document and note each person and storage location through which each piece of evidence passes.

In addition to documenting the machine's state at the time of seizure, the fraud examiner should document any serial numbers and other potential identifying markings (e.g., manufacturer, model number, asset tracking number), and he should photograph and diagram the system's entire configuration.

Inspect for Traps

Fraud examiners should also inspect the computer for traps, intrusion detection software, and self-destruct mechanisms.

If the Computer Is Off, Leave It Off

When seizing a computer system that is switched off, it should not be turned on. Turning a system on might damage and taint any evidence that it contains. For example, the booting up process in a Windows operating system will access and change the contents of the system's hard drive. In fact, each time a Windows operating system is booted up, some change, however small, is made to the system's hard drive. In particular, when a user boots up a Windows system, the computer's last access dates and times will be modified.

Collect Volatile Data "Live," as Required

If a formally trained computer investigator is present, he should consider engaging in collecting volatile data "live," which refers to the collection of evidence performed during the seizure phase when a digital device is not shut and is up and running. It involves the retrieval of data from a digital device directly via the device's normal interface.

When collecting digital evidence, fraud examiners should not do anything that will alter digital data. And because evidence on a running computer system can be altered by seemingly harmless actions (e.g., looking through files on a running computer system), historically, it was recommended that those seizing digital evidence adhere to a strict, traditional methodology to ensure that data is not changed in any way. The traditional methodology stated that when seizing running systems, those responsible should simply unplug the systems from their power sources and secure them for future examination by

trained digital evidence examiners. In short, the traditional methodology provided that when an individual is seizing a running computer system, he should unplug it from its power source, he should not use the computer, and he should not search it for evidence.

Although the traditional methodology has been a central premise in recommendations for dealing with digital evidence, and even though it is appropriate in many circumstances, there are situations where the traditional methodology is not appropriate.

Accordingly, the forensic industry has begun adopting methodologies that include *live evidence collection*—evidence collection performed during the seizure phase when a suspect system is not shut and is up and running—and it has been shying away from stating that "pulling the plug" should be the first step in the collection process in every situation. This trend has occurred because often, the most important evidence exists only in the form of volatile data (e.g., RAM) stored within a system. *Volatile data* refers to forensic artifacts in a state of flux that can be lost when power (or network connections, in some cases) has been removed from a computing device. So, if volatile data is not collected live from a suspect computer, it might be altered or lost when the system is shut down or disconnected from its network.

Because a computer system's volatile data simply disappears and is irretrievable when the system is off, fraud examiners seizing a system should consider live evidence collection when volatile data could be of interest to an investigation. So, for example, if the evidence that a formally trained computer investigator needs to collect exists only in the form of volatile data stored in volatile computer memory such as RAM, and the data is expected to disappear when the computer is shut down, he should collect the data live from the suspect computer.

Here is a list of reasons for performing live digital evidence collection to obtain volatile data:

- Volatile data might help identify evidence of misconduct on a system that can be lost if the system loses its power.
- Volatile data might contain encryption keys.
- Volatile data might show the existence of memory-resident malware.
- Live data collection can provide information before a full-blown forensics investigation can be performed.
- Some systems are critical and cannot be shut down.
- Shutting down a system might damage equipment or result in unintentional loss of data.
- Live digital evidence collection is less intrusive than traditional methods.

In addition to situations in which there is volatile data that could be of value in an investigation, other circumstances in which live data collection should be seriously considered include:

- The suspect is using the machine at the time of seizure.
- An attack is in progress at the time of seizure.
- Shutting down the computer might cause data to be unusable by drive encryption, running processes, network connections, and so on.

Common sources of volatile data include:

- *Random access memory* (*RAM*): Volatile data in RAM includes recently accessed data, such as data files, recent commands, and password hashes, and residual data in slack space and free space.
- *Operating system*: Volatile data that might exist in an operating system includes currently running programs, login sessions, open files, network configuration settings, incoming and outgoing network connections, and the operating system time.
- *Network device logs*: Volatile data in network device logs includes the logs created by networking gear, such as routers and switches.

Moreover, when collecting data for a computer forensic investigation, the examiner should collect the most volatile data first, as it will be lost the quickest, and live digital evidence collection organizes the collection of digital evidence based on the life expectancy of the evidence at issue. The following is a list of volatile digital information, from the most volatile to the least:

- Central processing unit (CPU) registers, cache, and peripheral memory
- Contents of main/physical memory
- Virtual memory (e.g., swap files also known as paging files)
- Network connections
- Running processes
- Data stored on local disk drives
- Data stored on backup media, etc.
- Data stored on archive media (e.g., CD-ROMs, USB flash drives)

Registers, cache, and peripheral memory; main/physical memory; virtual memory; network state; and running processes will all be lost when a system is shut down.

Despite the benefits of live data collection, it has its challenges, including:

- Untrained individuals using live data collection methods can compromise the data.
- A number of live data collection toolkits are untested.
- There is a lack of established processes and procedures for live data collection.

In *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community*, the authors recommend that investigators employ the following basic steps when collecting volatile evidence:[2]

1. Maintain a log of all actions conducted on a running machine.
2. Photograph the screen of the running system to document its state.
3. Identify the operating system running on the suspect machine.
4. Note date and time, if shown on screen, and record with the current actual time.
5. Dump the system RAM to a removable storage device or a remote system.
6. Check the system for the use of whole disk or file encryption.
7. Collect other volatile operating system data and save to a removable storage device or a remote system.
8. Determine evidence seizure method (of hardware and any additional artifacts on the hard drive that might be determined to be of evidentiary value).
9. Complete a full report documenting all steps and actions taken.

Secure the Evidence

When collecting evidence from a computer system, fraud examiners should also secure the evidence.

The primary concern when collecting and analyzing digital evidence is to maintain its integrity; therefore, forensic examiners must take steps to avoid and counter allegations that the methodology used to collect or analyze data was improper and could have damaged or altered the evidence. So, for example, if a system is off, do not turn it on.

In short, the examiner must secure computers in such a way that will allow him to testify, if need be, that no unauthorized access to the suspect system occurred. Thus, in most situations involving the seizure of a running system, fraud examiners should not peek through the files on the system. If a system is running, the fraud examiner might be tempted to explore the system's files and folder for evidence or to copy the computer's files to an

[2] Shipley, Todd G., and Henry R. Reeve. "Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community." The National Consortium for Justice Information and Statistics. http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RunningComputer.pdf.

external storage device. Generally, this should not be done because the fraud examiner's actions will alter data on the system. For example, if a fraud examiner explores a system's files and folders, each file he touches will have its original time stamps changed, and once the time stamps are changed, the original time stamps cannot be recovered.

But generally, proper seizure should include:

- Disconnecting all cords and devices
- Prohibiting access
- Maintaining a chain of custody
- Using write-blocking devices, if necessary
- Using appropriate packaging materials
- Using encryption technologies, if necessary

DISCONNECT ALL CORDS AND DEVICES

Also, proper seizure requires that when seizing a system, the fraud examiner should disconnect all cords, including the power supply, and devices and secure it for future examination by trained digital evidence examiners. If the fraud examiner is seizing a running system, disconnection should occur once the collection of volatile data is complete, but otherwise, disconnection should occur after documenting the machine's surroundings and inspecting for traps.

Accordingly, when seizing a running system, those responsible should not turn the system off using normal shutdown routines. There are two methods for shutting down a running system: a hard shutdown and a graceful shutdown. A *hard shutdown* occurs from power failure. Thus, a hard shutdown is performed by unplugging all power from the computer including power cables. A *graceful shutdown* occurs when the user relies on the set of built-in processes that prepare a computer for shutdown. If the fraud examiner uses the normal shutdown routines, a number of temporary files will be deleted and possibly overwritten during the shutdown process, and such files might be important to the investigation. The following is a list of data that is lost when a system is turned off using a graceful shutdown:

- Open files are closed.
- Temporary files are deleted.
- In Windows, the swap file is erased.
- Malicious material (e.g., memory-resident rootkits, Trojan horses, rootkits, or malware) might disappear or be removed.

Hard shutdowns, in contrast, will preserve swap files, temporary files, and other information that might be altered or deleted during a graceful shutdown. Therefore, disconnecting a running system from its power sources seeks to preserve the state of the system at the time of seizure.

Although hard shutdowns can preserve the state of the system at the time of seizure, they are not without risks. For example, hard shutdowns might cause:

- The disappearance or removal of malicious material (e.g., memory-resident rootkits, Trojan horses, rootkits, or malware)
- The corruption of operating system data

Nevertheless, in most cases, if a computer identified for seizure is running, the investigator should simply unplug it (i.e., he should perform a hard shutdown) and secure it for future examination by trained digital evidence examiners.

In some situations, however, there might be extenuating circumstances where a graceful shutdown would be best. Accordingly, it is important to evaluate the best shutdown option based on the type of data being preserved and the possible ramifications of a hard shutdown based on the type of operating system installed.

Moreover, laptop computers require additional considerations. When seizing a laptop, it is important to disconnect the laptop's power sources when performing a hard shutdown. This can be done by removing laptop's battery. But if the laptop is also plugged into an electrical source, remove the battery first and then unplug the power supply from the laptop and the wall outlet. If, however, the battery cannot be removed, unplug the laptop's power supply from the laptop and the wall outlet, and then press the power button for about 30 seconds to perform a hard shutdown. Additionally, when seizing a laptop, it is essential to recover all of the components that belong to the laptop, such as flash drives, CD- and DVD-ROMs, and power supply chords and related components. Often, laptop computers must be imaged with their drives installed, and because of the proprietary nature of the laptops themselves, they will only function with their own components. Many times these components can be located in the laptop carrying case.

Like laptops, networked computers present unique considerations. Shutting down or disconnecting a networked system might alter evidence. Also, it is important to use extreme

caution when removing power from a networked system without using proper shutdown methods because this can damage the system and expose the fraud examiner to liability.

PROHIBIT ACCESS

Moreover, once a computer system is seized, it is necessary to secure it in such a way that will allow the investigator to testify, if need be, that no unauthorized access to the suspect system occurred. Thus, once the investigator takes possession of the computer, he should prohibit access to it, with the exception of a trained forensic examiner.

MAINTAIN A CHAIN OF CUSTODY

Another method to help ensure the integrity of digital evidence is to maintain a chain of custody for all evidence gathered and analyzed. Again, the *chain of custody* is a recordkeeping procedure that documents who had possession of an item and what that party did with it. The chain of custody is a means of establishing that there has not been a material change or alteration to a piece of evidence. Therefore, from the moment evidence is collected, its chain of custody must be maintained.

In general, to establish the chain of custody, the fraud examiner must make a record when he receives an item or when it leaves his care, custody, or control. This is best handled by a record document when the evidence is received and turned over to someone else. At a minimum, the memorandum should:

- Identify each item that contains relevant information.
- Document each item that was received, who it was received from, who authorized its removal, the location of the item, and the date and time the item was received.
- Maintain a continuous record of the item's custody as it changes hands.

Gaps in the chain of custody (e.g., when it is not clear what occurred with a set of records) or outright mishandling (e.g., a group of questioned documents was not properly sealed) can harm a case.

WRITE-BLOCKING DEVICES

Also, investigators should consider using a hardware or software write-blocking device to protect the integrity of digital evidence. These devices allow the user to acquire information on a drive without damaging the drive contents by allowing read commands to pass and blocking write commands.

A *hardware write-blocking* device stops any automated processes or incidental processes that an operating system or fraud examiner might use to interact with a piece of digital media. That is, these devices trick the operating system into believing that the interaction occurred so that it will not generate an error and thwart the acquisition process. What actually happens is that the write commands are intercepted and cached by the write-blocking device instead of reaching the target; therefore, no writes to the media occur. The device allows only read permissions to the media.

A *software write-blocking device*, however, denies access to media by prohibiting certain requests to the media by filtering out those requests. When a software write-blocking device is in place, only read requests are accepted and all write requests are denied. Software write blockers must operate at a separate level than a standard graphical user's interface (GUI), such as in DOS mode.

APPROPRIATE PACKAGING MATERIALS

Moreover, fraud examiners should use appropriate packaging materials for evidentiary items. They should consider using tamper-proof evidence tape to document any future access to the evidence. Also, devices with volatile memory, such as mobile phones, should be packaged separately so that power to the device can be maintained.

ENCRYPTION

Furthermore, because digital forensics examiners frequently acquire data that contains sensitive or confidential information, they should consider using encryption techniques to protect sensitive data.

Imaging

Once a computer system is seized and before any analysis occurs, it should be imaged for analysis. Forensic analysis should not be performed on suspect devices directly because doing so can alter or damage digital evidence, and imaging the data from suspect devices allows a fraud examiner to view and analyze a computer's contents without altering the original data in any way.

Imaging refers to the process whereby a forensic image of a hard drive or other digital media is made and imaged to another hard disk drive or other media for forensic analysis. A *forensic*

image (also called a forensic copy, mirror image, or ghost image) is an image or exact, sector by sector, copy of a hard drive or other digital media.

The acquisition of a forensic image involves using a standalone hard drive duplicator or similar device to make a duplicate or exact copy of a hard drive or other digital media. The process can be divided into the following three steps:

- Acquire the original storage media.
- Create the forensic image of the original storage media.
- Verify the image of the original storage media.

Once a forensic image of the data on digital media has been made, it can be analyzed for potential probative data.

Generally, to avoid contaminating evidence, a system should not be imaged using subject machines.

Also, the image must be created and preserved in a manner that will withstand a legal challenge; therefore, before imaging a hard drive, the best method for acquiring the image and the proper procedures for facilitating the image capture must be determined.

Furthermore, during the imaging process, those responsible should use some type of write-blocking device or application to ensure no information is written onto the original drive, and after the hard drive is duplicated, they must move the original drive to a secure location to prevent tampering.

Document the Collection Process

When conducting an investigation of a digital device, the fraud examiner should document the investigation throughout the process by making notes regarding what he did during the investigation. Generally, such notes should include information such as:

- Date and time the examination began
- Photographs of the device and its components
- The status of the system when seized (on or off)
- The identification information of the device (e.g., make, model)
- Tools used in the examination
- Data documented during the examination

Implement a System to Manage the Evidence

Fraud examiners should have a system to track and manage physical and digital evidence. There are a number of software products that facilitate evidence management, and these products contain various tools to help fraud examiners and investigators meet digital evidence handling needs. For instance, users can use such programs to search, categorize, and distribute digital evidence while helping to maintain chain of custody controls and restricting access.

Processing

Once the collection process is complete, fraud examiners are left with large volumes of digital data that might contain relevant or irrelevant information. At this point, the fraud examiner must process and filter the digital information to reduce the amount of data (commonly known as *data culling*) that has been collected by identifying relevant information and by setting aside duplicates and other information that is not relevant due to its type, origin, or date. While doing this, the fraud examiner must preserve the integrity of the data.

There are several methods that fraud examiners can use to filter large amounts of data, but the techniques the team employs to process information will vary depending on the investigation's goals. Some common methods include:

- Keyword searches
- Deduplication filtering
- Date-range filtering
- File-type filtering

Keyword Searches

Keyword searches involve identifying relevant evidence by searching for words that are material to a case (e.g., names, dates, account numbers). This type of search will minimize the amount of time used to complete an analysis, and it will help protect the fraud examiner from allegations that his search was overly broad.

To conduct a keyword search, the fraud examiner should establish a list of relevant keywords that are based on the information known about the case. Because enormous amounts of data will need to be searched in most fraud examinations, fraud examiners should take care in keeping the list as short and relevant as possible, and they should avoid common words or

words that can be part of other words. As a case progresses, there is a strong likelihood that more keywords will be identified.

Furthermore, search terms can be devised to look for patterns in data.

Deduplication Filtering

An issue faced in most examinations is that multiple copies of various files will be collected as part of the investigative process. Because reviewing such duplicative materials is expensive and time consuming, the fraud examiner should identify and eliminate duplicates in the collected data. This process is referred to *deduplication filtering*, and it is critical to help reduce the vast amounts of information collected during a fraud examination.

Date-Range Filtering

If an analysis involves activities within a certain period, it might be useful to limit the search to data that falls within a specific period. For computer files, filtering can be based on the operating system's metadata (e.g., based on the files created, modified, or last accessed dates). Similarly, email messages can be filtered by their sent date.

File-Type Filtering

There might be cases where only certain types of information are required, and in such cases, *file-type filtering* (i.e., filtering data based on file type) will be useful.

Analyzing

The analysis phase involves the use of specialized software designed to give the fraud examiner the means to identify, extract, collect, examine, and store digital artifacts that will be used as evidence in the investigation.

There are a number of analytical review products that can assist in analyzing volumes of data for relevant evidence. But generally, these products employ various ways to search and analyze data for relevant materials. Unfortunately, due to the vast array of digital devices available, there is no single perfect tool or platform. No single analytical review tool can recover everything; each tool has its own strengths and weaknesses. Therefore, it is best to use a combination of the various tools during the analysis phase, allowing for the identification and recovery of more information.

Also, when analyzing data for evidence, the fraud examiner should look for inculpatory evidence (i.e., evidence that serves to incriminate the subject of the investigation) and exculpatory evidence (i.e., evidence that service to disprove the subject's involvement in the misconduct).

The primary concern when analyzing digital evidence is to maintain the integrity of the data at all times. Fraud examiners must be careful with computer equipment because a careless investigator might inadvertently alter important evidence. Therefore, it is helpful to develop procedures to prevent the opposing party from raising allegations that the methodology used to collect or analyze data was improper and could have damaged or altered the evidence. Again, it might be helpful to use a hardware-based write-blocking device to protect the integrity of digital evidence.

Reporting and Testifying

The reporting and testifying phase is where the hours of analysis are reported fairly and objectively. In this phase, a qualified expert might be asked to render an opinion about the use or misuse of a computer system. This is where experience and training are tested and where fraud examiners must know with certainty that their opinion is based on their research, knowledge, and experience and that an opposing expert will not find fault with their conclusions.

Additionally, the fraud examiner might provide witness testimony at a deposition, trial, or other legal proceeding.

Investigating in the Cloud

Although information relevant to a fraud examination might be stored in the *cloud*—a metaphor for the storage and utilization of data online—conducting digital forensic investigations in the cloud environment (i.e., *cloud forensics*) presents challenges not faced in traditional forensic practices. This discussion explores some of those challenges.

Challenges of Cloud Forensics

Some of the important challenges of cloud forensics are:

- Lack of frameworks and specialist tools
- Lack of information accessibility

- Lack of data control
- Jurisdiction of storage
- Electronic discovery
- Preserving chain of custody
- Resource sharing
- Lack of knowledge

Lack of Frameworks and Specialist Tools

Unlike traditional forensics, which have clear, step-by-step frameworks and specialist tools for the collection of evidence suitable for presentation in court, there are no such frameworks or tools for collecting evidence in the cloud. In fact, many digital forensics tools are not designed to operate within the cloud environment, and tools and procedures for locating, isolating, and preserving data in the cloud are in their infancy.

Lack of Information Accessibility

Cloud computing complicates the collection of data because cloud storage systems are not local, and therefore, there is a lack of access to forensic data stored on the cloud.

Cloud customers do not typically have physical access to data stored on the cloud, and they generally have limited to no access to their cloud data's log files and metadata.

Accordingly, investigators generally do not have physical access to evidence stored on the cloud—something that investigators typically have when examining traditional privately owned and locally hosted systems. For instance, if a suspect's files relevant to an investigation are on the cloud, investigators cannot simply confiscate the suspect's computer and get access to the relevant files.

Lack of information accessibility also means that often, cloud customers do not have much information about the physical locations of their data. So, due to the nature of the cloud, it might not be clear what data are available. Moreover, if an entity uses more than one cloud provider, it might not be clear which provider has stored the data.

Also, a cloud customer's accessibility to data stored on a cloud provider's servers might depend on the contracts between the provider and the customer. Therefore, in some cases, it might be necessary to review such contracts to determine the contractual obligations of the providers, the access the customer might have to the data stored on the provider's servers,

and ownership rights to data. Thus, companies that use cloud-computing providers should include clauses in their service-level agreements that address investigative and data preservation responsibility and liability.

Likewise, many cloud providers do not provide for the facilitation of forensic readiness in the cloud. Many cloud providers do not furnish services or interfaces for the collection of forensic data. In fact, many customers of cloud service providers have limited access to their cloud data's log files and metadata.

Lack of Data Control

Moreover, with cloud computing, clients of cloud service providers do not have physical control of the media or the network on which their data resides, which can complicate efforts to collect data stored on the cloud.

Additionally, there are many providers of cloud services, and each service has proprietary implementations that might influence the data available, how that data is collected, and who has access to the data.

Furthermore, cloud providers might not maintain detailed logs of transactions on their systems, which can minimize the amount of useful information available in an investigation.

Likewise, relevant data stored in the cloud must be preserved until it can be lawfully acquired, but a provider's practices can inhibit preservation.

Jurisdiction of Storage

Cloud providers commonly store data in servers in different locations around the world. Consequently, it is possible that evidence related to individuals within the same organization could be segregated in different physical locations, thus complicating an investigator's ability to determine jurisdiction. Furthermore, because all jurisdictions impose different laws and regulations regarding the storage, use, and access of data, the collection of relevant data might be complicated by the distribution of servers around the world.

Electronic Discovery

Even if information on the cloud can be obtained through *discovery*—the phase where parties to litigation obtain information or evidence that might be used during trial—collecting information through discovery mechanisms has its own challenges. Information stored in

the cloud is different than other forms of evidence because cloud customers do not typically "possess" the evidence, which is often an element required to successfully demand discovery of evidence. However, the trend is for courts to require parties to turn over evidence that they can access or control, even if it is not in their possession.[3]

Preserving Chain of Custody

Maintaining the integrity of evidence stored in the cloud is difficult because the following information typically is missing from such data:

- How the data was processed and by whom
- Who had access to the data and when it was accessed
- Whether the data was commingled with the data of the provider's other clients
- Who acquired the data submitted for analysis (e.g., a trained digital forensics examiner or an employee of the cloud-computing provider)
- How the data was preserved and by whom

Resource Sharing

Under the traditional computing model, resources tend to be used exclusively by a single entity, but in the cloud environment, providers allocate resources for multiple customers on the same physical infrastructure. This difference exists because cloud-computing providers use server virtualization, which involves the partitioning of an existing server in such a way that it effectively becomes multiple servers. Server virtualization allows individual virtual servers to be used without affecting the server as a whole. As a result, computing resources are made more efficient and data resources become more flexible.

But under this type of infrastructure, a cloud customer's data gets stored on the same physical infrastructure used to store data belonging to other customers. That is, each cloud server contains files of multiple customers.

Server virtualization affects the privacy of cloud users. Because each cloud server contains files of multiple customers, investigators cannot seize servers from a provider's data center without violating the privacy of many other cloud customers. For example, if a cloud user's data is stored on a physical system that also contains another user's data that is needed in a fraud investigation, the first user's data might be inadvertently gathered during the fraud

[3] See *Gordon Partners, et al. v. Blumenthal, et al.*, 244 F.R.D. 179, 195 (2007).

investigation. And in some jurisdictions, the inadvertent access of data not relevant to an investigation can infringe upon privacy legislation.

Also, if a cloud provider stores the data of multiple cloud customers on the same physical computer, the provider will likely prohibit any effort to create a forensic image of its physical storage media if the forensic image would likely contain the data of other customers.

And even if investigators can seize or image servers from a provider's data center, they must separate the data of the different users, which is a difficult feat.

Lack of Knowledge

Even if an investigator has complete access to a cloud provider's storage media, it would be difficult to interpret relevant data from the system. Generally, to extract useful information from storage media, the investigator needs to have knowledge about the system from which the image was obtained, including information about its operating system, its application(s), and the operations of its user logging system.

Conclusion

The growing complexities of the IT cloud-computing infrastructure can impede fraud examinations, and it follows that overhead costs will rise as companies have to hire highly specialized digital forensics examiners to identify and forensically preserve relevant data in cloud-computing environments.

For more information on cloud forensics, visit the Cloud Security Alliance (CSA) website at www.cloudsecurityalliance.org. The CSA is a not-for-profit organization tasked with promoting the use of best practices for providing security within cloud computing environments. In 2013, the CSA published a whitepaper titled *Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing*, and the paper details some of the key digital forensics challenges posed by cloud computing. Also, in 2013, the CSA announced the formation of the Incident Management and Forensics Working Group, a Working Group created to focus on forensics in cloud environments.

Mobile Forensic Investigations

As a result of the proliferation of smartphones, mobile phone forensics have become an essential element of most civil and criminal investigations. *Mobile phone forensics* refers to techniques used to gather data from smartphones so that the data will be admissible in court. Organizations use mobile phone forensics to determine whether a company device has been used in violation of its use policies.

There are many companies that provide mobile phone forensic services, and there are numerous readily available tools available that can extract information from the hardware, microchips, and software of mobile phones. Generally, these forensic tools employ various ways to extract data from mobile devices, and in many investigations, it is best to use a combination of methods when gathering evidence. The main areas for recovering data on mobile devices are as follows:

- *Logical*: This includes the logical storage objects that reside on a logical store (e.g., a file system partition). The actual data that can be retrieved using a logical examination will vary, depending on the type of device, but the retrievable information could include text messages, multi-media messages, call registers, contacts, tasks, images, audio, videos, calendar entries, and so on.
- *File system*: This includes information in the logical extraction and hidden information such as deleted information and operating system files.
- *Physical*: This includes information on a physical store (e.g., flash memory or memory chip).

But unfortunately, due to the vast array of mobile devices available, there is no single forensic tool that will cover the wide range of today's devices.

To complicate things further, mobile device forensics use methods different from traditional computer forensics because, among other things, mobile devices store data in various unique formats that prevent mobile devices from being copied in the same ways that computer hard drives can be imaged. But regardless of the differences, it is essential that mobile forensic procedures maintain the integrity of any data collected. The Association of Chief Police Officers (ACPO) *Good Practice Guide for Computer based Electronic Evidence* provides four principles that investigators should adhere to when dealing with digital evidence. Those four principles are summarized as follows:

- Investigators should not perform any action that will change data contained on digital devices or storage media that might subsequently be relied upon in court.

- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- When examining a mobile device, an audit trail or other record of applied processes, suitable for replication of the results by an independent third party, must be created and preserved to accurately document each investigative step.
- The person in charge of the investigation should have overall responsibility for ensuring the aforementioned procedures are followed and in compliance with governing laws.

The following discussion provides a methodology for conducting mobile device investigations. Typically, such investigations will involve the following phases:

- Plan
- Seize
- Extract
- Process
- Analyze
- Document
- Report and testify

The following discussion, however, is not an exhaustive discussion on mobile forensics. Rather, the discussion is a brief description of the routine processes involved in mobile forensics. For more information on mobile forensics, see the National Institute of Standards and Technology's (NIST) *Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology*. NIST created the *Guidelines* to help organizations establish policies and procedures for dealing with cell phones.

Plan

Just as when conducting a traditional computer forensic investigation, a fraud examiner conducting a mobile forensic investigation must prepare for the investigation. Among other things, the planning phase should address the following:

- The legal authority to examine the device
- The goals of the investigation
- The make, model, and identifying information of the device to be seized
- Any other sources of potential evidence

Once the fraud examiner has identified the make and model of the device to be seized, he can conduct research to determine what forensic tools are capable of extracting data from the target device.

Seize

Next, the fraud examiner must seize and collect the devices, isolate the device, and document the phone at the time of seizure. When seizing mobile devices, the fraud examiner should seize any supporting devices and information, including:

- Removable storage media
- Cables for transmitting data
- Power chargers
- Documentation relating to the devices purchase

Also, when seizing a mobile device, the fraud examiner should isolate the device to prevent unnecessary changes to the device's data because the data on mobile devices is volatile and always changing. The procedures, however, will vary for devices that are powered on and those that are powered off.

If a device is powered off, the fraud examiner should leave it off to prevent any changes to its data.

If, however, the device is powered on, the fraud examiner must consider several things. The fraud examiner should not unnecessarily scroll through the device because doing so will likely change the device's data. Additionally, if a device is powered on, the fraud examiner should not turn it off in most cases. If a device is password protected or encrypted, powering it off might prevent subsequent access to it. But because a device that is turned on might communicate with the network—which will cause data changes—the fraud examiner should isolate such devices from the network. Isolating a device from the network will also prevent:

- The device's user from remotely accessing the device to destroy data
- Cross contamination
- New data from overwriting old data
- New data from contaminating the existing data

There are three basic options for isolating mobile devices in a manner to prevent unnecessary data changes. The first option is to use a Faraday container—a container that

shields devices from electromagnetic signals—to prevent the device from communicating. One disadvantage of this method is that when the device is placed in a Faraday container, it will constantly scan for a network to connect to, causing its battery to deplete quickly. Wrapping a device in several layers of aluminum foil will approximate a Faraday container. If placing a device in a Faraday container, it should not be connected to an outside power supply; instead, investigators might consider using a portable power supply that can be connected to the device while leaving it secured inside of the Faraday container.

Second, the fraud examiner can set the device into flight mode. This will isolate the device's transceiver but will allow its other functions to continue running normally. However, putting a device in flight mode requires user input.

Third, the fraud examiner can turn the device off by removing its battery instead of using the device's normal shutdown routines. A fraud examiner should turn the phone off if the device cannot be processed immediately. The benefits of turning a phone off include:

- Preserving the call log
- Preserving the information of the last cell tower location
- Preventing the overwriting of deleted data
- Preventing communications from reaching the device and changing data
- Preventing the device from being handled improperly

Once the device is isolated from the network and ready for forensic analysis, the analyst should document the device at the time of seizure by:

- Recording all the details of active applications on the device
- Conducting a photographic survey to show the state of the device when it was found or received
- Identifying the device's model and type and searching for the device's user manuals and technical characteristics

Extract

Once a device is seized, a professional analyst should extract and examine the device with professional forensic tools. But due to the vast array of mobile devices available, there is no single tool that can be used to extract all potential evidence from mobile devices. Instead, fraud examiners likely will have to use a combination of various techniques and available mobile forensic tools to extract the best data from most devices.

The following discussion provides a brief summary of the basic extraction processes using widely available forensic tools. As these forensic tools do not work for all devices, such cases will require that advanced extraction techniques must be used.

Typically, when using off-the-shelf mobile forensic tools, the analyst must decide on the base forensic application to use for collecting data from the device. Once he has made this decision, he should connect the device to the forensics tool. There are three basic connection methods to extract data from mobile devices—cable, infrared, and Bluetooth—but because each method has its benefits and drawbacks, it might be necessary to use a combination of each connection method when extracting data from a mobile device.

Once a connection has been established, the analyst should extract information from the device's hardware, removable storage media, and the SIM card if working with a GSM device.

Next, the analyst should record the device's make, model, and International Mobile Station Equipment Identity (IMEI) number. Usually, this information is found printed inside the device's battery compartment.

After recording the device's identification information, the analyst should remove the device's SIM card and any removable media. He should then extract data from them using forensic tools.

Once the analyst has extracted data from any removable media, he should manually examine the device to verify the accuracy of the extracted information, create a working copy of the extracted data for analysis purposes, and secure the data from the original extraction for storage. Extracted data can be verified in various ways, including:

- Checking to ensure that the extracted data matches the data displayed by the device
- Using more than one forensic tool to extract the data from the device and cross verifying the results by comparing the extracted data from each tool
- Checking the hash values of the extracted data against the originals to verify individual files

Finally, once the analyst has successfully extracted the data from the device, he should conduct a photographic survey to show the state of the device after the extraction.

Analyze

Like the analysis phase in traditional computer investigations, the analysis phase in mobile forensic investigations involves efforts to identify inculpatory and exculpatory evidence. The potential evidence on mobile devices includes the following items:

- Subscriber and equipment identifiers
- Settings (date/time, language, etc.)
- Contacts
- Calendar information
- Call history (e.g., dialed, incoming, and missed calls)
- Text and multimedia messages
- Email
- Photos
- Audio and video files
- Internet history
- Downloaded applications
- Electronic documents
- Location information

Document

When conducting an investigation of a mobile device, the fraud examiner should document the investigation throughout the process by making notes regarding what he did during the investigation. Generally, such notes should include information such as:

- Date and time the examination began
- The condition of the device
- Photographs of the device and its components
- The status of the phone when received (on or off)
- The identification information of the device (e.g., make, model, IMEI number)
- Tools used in the examination
- Data documented during the examination

Report and Testify

The reporting and testifying phase in mobile forensic investigations is similar to the last phase in traditional computer forensic investigations. In this phase, the fraud examiner makes a fair and objective report of his analysis and, if necessary, testifies about the investigation at a deposition, trial, or other legal proceeding.

Digital Forensics Software

There are a number of products that can assist in identifying, extracting, collecting, and storing digital evidence. Although these tools range in complexity, features, and price, they employ various methodologies to extract and analyze data from computer systems. And again, because these tools employ different methodologies, it is best to use a combination of them when gathering evidence.

Also, when using such tools, it is extremely important to understand and be able to articulate how the tools work. This means that a forensic examiner who uses an automated tool should be able to explain how to conduct the same process manually.

The following is a general listing of the most frequently used products on the market today. This list, however, is sure to change. (Please note that the product descriptions are adapted from materials provided by the manufacturer, and the ACFE does not endorse any particular product.)

EnCase Forensic

EnCase Forensic is a computer forensics software program by Guidance Software. It gives investigators the ability to image a drive and preserve it in a forensic manner using the EnCase evidence file format (LEF or E01), a digital evidence container vetted by courts worldwide.

For more information about EnCase Forensic, visit www.guidancesoftware.com.

Forensic ToolKit

Created by AccessData, the Forensic Toolkit (FTK) offers law enforcement and corporate security professionals the ability to perform complete and thorough computer forensics examinations. The FTK features file filtering and search functionality. FTK's customizable filters allow investigators to sort through thousands of files to locate evidence. FTK is also a forensic tool to perform email analysis.

For more information on AccessData, visit www.accessdata.com.

Password Recovery Toolkit

The Password Recovery Toolkit (PRTK) from AccessData is geared toward law enforcement and corporate security professionals. It allows users to find and identify encrypted files on handheld, desktop, and server computer systems. PRTK recovers lost, forgotten, or unavailable passwords. If users need access to locked files or if they have simply locked themselves out of their files, the PRTK can get them back in.

For more information on AccessData, visit www.accessdata.com.

ProDiscover Forensics

Distributed by the ARC Group of New York, ProDiscover Forensics is a computer security tool that enables computer professionals to find all the data on a computer disk while protecting evidence and creating evidentiary quality reports for use in legal proceedings.

ProDiscover Forensics is a tool for computer forensics analysis. It reads disk data at the sector level, making it impossible to hide the data. By employing this approach, ProDiscover Forensics allows the investigator to examine files without altering any valuable metadata. ProDiscover Forensics will not alter any data on the disk.

For more information, visit www.arcgroupny.com.

Stego Suite

The Stego Suite by WetStone is a software bundle available for the investigation, detection, analysis, and recovery of digital steganography. It identifies the presence of steganography without prior knowledge of the steganography algorithm that might have been used against the target file.

WetStone's Stego Suite is composed of four products: Stego Watch, a steganography detection tool; Stego Analyst, an imaging and analysis tool; Stego Break, a password cracker; and Stego Hunter, a steganography application identifier.

For more information about the Stego Suite and other products by WetStone, visit www.wetstonetech.com.

Mobile Device Forensic Tools

Again, mobile device forensic tools allow for the acquisition and examination of mobile devices.

Cellebrite UFED

Cellebrite manufactures various data extraction, transfer, and analysis devices for cellular phones and mobile devices. Cellebrite's UFED systems are standalone, handheld devices that extract mobile device data directly onto an SD card or USB flash drives (although it does not store data within its own memory). Because Cellebrite's UFED products are standalone devices, they can be used for in-field data extraction and analysis under adverse conditions.

For more information about the Cellebrite UFED systems, visit www.cellebrite.com.

Logicube CellDEK

CellDEK by Logicube is a self-enclosed extraction device that can be used to extract data from CDMA, GSM, and BlackBerry devices. The CellDEK software performs forensic extraction of the following data: handset time and date, serial numbers (IMEI, IMSI), dialed calls, received calls, phonebook (both handset and SIM), SMS (both handset and SIM), MMS messages (not available from all handsets), deleted SMS from SIM, calendar, memos, to-do lists, pictures, video, and audio.

For more information on CellDEK, visit www.logicube.com.

XRY/XACT

Micro Systemation's XRY/XACT system can be used to perform logical data acquisitions and physical dumps in one platform.

XRY is a software application that can be used to acquire data from GSM, CDMA, and SIM/USIM cards. The XRY tool connects to the device and the software stores data in a proprietary format that cannot be altered, but data remains exportable. The XRY software allows for examination and reporting on the content of the device and its SIM card, in the case of a GSM device.

XACT is a separate hex viewer software application that complements XRY, allowing investigators to view the raw hexadecimal data extracted during a physical dump of a mobile

device. Thus, XACT allows forensics specialists to perform physical data acquisitions that recover deleted information from confiscated mobile phones without compromising the quality of the information and their legal standing in court.

For more information about Micro Systemation's XRY/XACT system, visit www.msab.com.

Paraben Device Seizure

Developed by Paraben, Device Seizure is an acquisition and analysis tool for examining mobile devices. It supports mobile phones operating under GSM, CDMA, and TDMA, as well as BlackBerry, Windows Mobile, iPhone, and other smartphones through the use of a variety of plug-ins.

For more information about Device Seizure, visit www.paraben.com.

EnCase Forensic v7

EnCase Forensic v7 includes the capability to, among other things, review and forensically collect data from smartphone and tablet devices that use Apple iOS, Windows Mobile OS, Google Android OS, and RIM BlackBerry OS.

For more information about EnCase Forensic v7, visit www.guidancesoftware.com.

TRACING ILLICIT TRANSACTIONS

Tracing refers to the search for evidence for the purpose of showing what has happened to property, identifying the proceeds of property, and identifying those who have handled or received property or the proceeds of property. Accordingly, fraud examiners are often tasked with tracing illicit transactions and the underlying assets. For example, a fraud examiner might be engaged to assist:

- A victim of fraud who wants a tracing search to facilitate the recovery of criminal proceeds
- A potential plaintiff who wants a tracing search to determine if the potential defendant can pay a court-ordered sum if a judgment is ordered
- A judgment creditor who needs to identify the judgment debtor's assets

This section seeks to demystify the process of tracing illicit transactions and provide tools for success in this complex work. This section is organized into the following sections:

- General process for tracing illicit transactions
- Direct methods of tracing financial transactions
- Indirect methods of tracing financial transactions
- Locating hidden assets

General Process for Tracing Illicit Transactions

Although the procedures performed during a tracing investigation vary depending on the circumstances, an actual investigation to trace transactions generally should involve the following elements:

- Collect information.
- Profile the subject.
- Review information for leads and prioritize leads.
- Trace the illicit transactions.

Collect Information

To trace transactions, fraud examiners must collect information about the parties and transactions involved. Because not all of the parties or transactions involved are known from the outset of an investigation and might only become known in the course of an investigation, the collecting of information is an ongoing process.

Generally, fraud examiners should begin tracing investigations by compiling everything known about the subject, and once this is done, they should search public record sources, collect nonpublic records (if available), and conduct interviews.

Compile Information About the Subject

To begin a tracing search, the fraud examiner should compile everything known about the subject. If the subject is an individual, the subject's legal name and current address are essential to any tracing investigation. In addition, other relevant items of information include:

- The subject's place of employment
- The subject's date of birth and place of birth
- The names and birthdates of the subject's close relatives (e.g., spouses, children, parents, siblings, spouses of siblings, grandparents, grandchildren, uncles, aunts, or cousins)
- The identities of the subject's close friends
- The subject's national identification number (e.g., Social Security number, personal identification number, social insurance number, or Personal Public Service Number)
- The subject's last known address
- Relevant telephone numbers
- Relevant email addresses
- Contact details of any Internet communication by the subject
- Criminal record search results
- Results of public-information searches
- Results of private-records searches
- Records of any relevant real estate
- Financial account information

Much of the basic information about a subject can be found in audit documents, business records, personnel records, the Internet, and conversations with people who know the subject.

Search Public Record Sources

Once the fraud examiner has basic information about the subject, he can use it to search public records and gain intelligence to trace the transactions. He can gather relevant information from online sources, government agency databases, public databases, and through the use of other special investigative techniques. Some techniques might require legal authorization (e.g., electronic surveillance, search and seizure orders, legal orders to

produce information, or account monitoring orders), while others might not (e.g., physical surveillance or witness interviews).

Collect Nonpublic Records

The fraud examiner should also obtain nonpublic records, if available by legal means. Nonpublic records, however, are difficult to obtain unless the subject of the information voluntarily turns the records over, the person to whom the records pertain consents to their release, or the disclosure of such records are required by some type of legal process.

Conduct Interviews

Also, the fraud examiner should conduct *interviews*—question-and-answer sessions designed to elicit information—of relevant parties who might have information concerning the matters at issue.

Information obtained during an interview can corroborate or illuminate information obtained from documentary evidence, identify new financial documents, fill in the information gaps that remain, or expose new leads.

Fraud examiners should conduct interviews with the subject and those who are close to the subject. Often, when tracing illicit transactions, fraud examiners will not have access to the subject, but they might have access to individuals close to the subject (e.g., friends, family, associates, or coworkers). Typical interviewees include complainants; employees of financial institutions involved; the suspect's business associates, ex-spouses, friends, relatives, neighbors, employees, business rivals, or other associates; other individuals who have been in contact with the target; and people who have a stake in an asset or transaction at issue.

Often, the interviews conducted in tracing examinations are of a financial nature. Although financial interviews are similar to other interviews, in financial interviews, evidence often develops incrementally and, when viewed separately, might appear to lead nowhere. Consequently, frustration is common in financial interviews.

When seeking information about illicit transaction, the fraud examiner should ask interviewees for records, documents, and other types of information that might identify, trace, and locate assets. Questions might seek to obtain information about the subject's:

- Employment and sources of income
- Real and personal property

- Financial needs (e.g., medical, educational, or other ongoing expenses)
- Investments
- Business or financial dealings
- Debts and other financial obligations
- Lifestyle habits
- Family

Also, when interviewing the subject, fraud examiners should ask the subject to discuss:

- Sources of funds he received during the relevant period
- The amounts of current liquid assets
- Any significant transactions and the reasons behind such transactions
- His accounts at financial institutions
- His principle assets, their purchase dates and costs, and how he paid for them
- His principal liabilities
- His average total monthly expenditures and how he pays living expenses
- His estimated current net worth
- Litigation in which he has been involved during the relevant period
- The professionals (e.g., accountant, lawyer, or travel agent) he uses

Checklist of General Information for Tracing Investigations

The following is a checklist of general information that should be sought in tracing investigations.

IDENTIFICATION INFORMATION ABOUT THE SUBJECT

- Full name
- Alias
- Reason for alias

THE SUBJECT'S BIRTH INFORMATION

- Date and place of birth
- Citizenship
- Father's name; living? (If deceased, when?)
- Mother's name; living? (If deceased, when?)

THE SUBJECT'S ADDRESS(ES) DURING PERTINENT YEARS

- Resident address; phone number
- Business address; phone number

- Other present or prior address(es)
- Marital status; if married, date and place of marriage
- If divorced, when and where
- Spouse's maiden name
- Spouse's parents; living? (If deceased, when?)
- Children's names and ages; other dependents

THE SUBJECT'S OCCUPATION INFORMATION

- Present occupation
- Company name and address
- Present salary
- Length of time employed
- Additional employment
- Prior occupations
- Spouse's occupation

GENERAL BACKGROUND INFORMATION ABOUT THE SUBJECT

- Physical health
- Mental health
- Education
- Professional qualifications
- Military service
- Passport, Social Security, and/or social insurance numbers (for identification purposes)
- Criminal history
- Arrest history
- Bankruptcy history; who acted as receiver/trustee?
- Hobbies and interests

INFORMATION ABOUT THE SUBJECT'S FINANCIAL INSTITUTIONS (BUSINESS AND PERSONAL)

- Financial institution accounts
- Safe deposit boxes (request inventory); in whose name; contents; does anyone else have access?
- Credit cards
- Trusts; beneficiary, donor, or trustee
- Mutual funds or other securities owned
- Brokers; currency exchanges used
- Life insurance

- Indirect dealings (e.g., through lawyers or accountants)
- Cashier's checks
- Money orders, bank drafts, traveler's checks

THE SUBJECT'S SOURCES OF INCOME

- Salaries, wages, business receipts
- Interest and dividends
- Sale of securities
- Rents and royalties
- Pensions, trusts, annuities, etc.
- Gifts (money, property, etc.)
- Inheritances
- Loans
- Mortgages
- Sales of assets
- Municipal bond interest
- Insurance settlements
- Damages from legal actions
- Any other source of funds, ever

THE SUBJECT'S NET INCOME AND EXPENDITURES

- Current cash on hand, including cash in safe deposit boxes, but not cash in bank accounts
- Location of current cash
- Largest amount of cash ever on hand; location
- End-of-year cash
- Notes receivable
- Mortgages receivable
- Life insurance policies
- Automobiles
- Real estate
- Stocks, bonds, and other securities
- Luxury items (e.g., jewelry, furs, exotic vehicles)
- Airplanes, boats
- Any other assets valued

THE SUBJECT'S LIABILITIES

- Payables
- Loans
- Assets purchased by financing
- Mortgages
- Bonds

THE SUBJECT'S EXPENDITURES

- Debt reduction
- Insurance premiums
- Interest expense
- Contributions
- Medical
- Travel
- Real estate and other taxes
- Household wages (e.g., babysitter, housekeeper, gardener)
- Casualty losses

THE SUBJECT'S BUSINESS OPERATIONS

- Name and address
- Date organized and nature (corporation, partnership)
- Company or business registration numbers
- Tax identification numbers
- Title and duties
- Reporting arrangements—to and from whom?
- Banking and cash handling arrangements
- Investment; where and when
- Subsidiaries and associates
- Key people

THE SUBJECT'S BOOKS AND RECORDS

- Nature of accounting system (e.g., cash, accrual)
- Period covered
- Location
- Name of person maintaining and controlling
- Types (journal, ledgers, minute books, canceled checks, bank statements, invoices, cash)
- External auditors

THE SUBJECT'S BUSINESS RECEIPTS

- Form (electronic, check, or cash)
- Are all receipts deposited? Where?
- Are business receipts segregated from personal ones?
- Are expenses ever paid with undeposited receipts?
- Arrangements for foreign currency payments
- Trade finance arrangements, letters of credit, etc.

Profile the Subject

Once the fraud examiner has begun collecting information, he should then begin creating a personal profile of the subject. The personal profile, which is comprised of the financial and behavioral profile, will contain information on the subject's financial condition.

The financial profile is essentially a financial statement with some modifications and additions. It shows what the subject earns, owns, owes, and spends at any given point, or over a period of time; it reflects the subject's income, expenses, assets, and liabilities. That is, it shows the subject's financial condition.

The behavioral profile is comprised of outside pieces of information that can support estimates and fill information gaps. The behavioral profile contains information about the suspect's personal characteristics (e.g., carries large amounts of cash, wears expensive clothes, or has club memberships), home and furnishings, automobiles, and leisure activities.

Review Information for Leads and Prioritize the Leads

Early on, as the fraud examiner begins collecting information, he should review it for leads and subsequently prioritize those leads.

The leads, however, will vary depending on the facts of each case. Potential leads might include information on accounts, assets, persons, entities, technology, and so on. More specifically, the leads might include information about:

- The subject's educational background
- The subject's employer
- The subject's occupation
- The subject's marital status
- The names of the subject's family members, friends, or business associates
- The subject's address

- The subject's interests or hobbies
- The subject's property
- Any membership organizations to which the subject belongs

When reviewing data for leads, the fraud examiner should note the names of any attorneys, corporate officers, lending officers, and notaries found on any uncovered records. When doing so, he should look for connections between these individuals and the subject.

Also, once the fraud examiner has identified potential leads, he should prioritize them and select which ones might result in the development of the most significant evidence in a timely manner.

Trace the Illicit Transactions

After the fraud examiner has identified, compiled, and reviewed documents indicating ownership, he should begin analyzing financial records and begin tracing. Again, *tracing* refers to the search for evidence showing what has happened to property, identifying the proceeds of property, and identifying those who have handled or received property or the proceeds of property. That is, tracing involves documenting the movement of assets in and out of accounts.

Tracing will involve identifying those persons, organizations, and assets at issue and the connections between them, and it should include an analysis of the assets and financial flows. For example, once the fraud examiner has established the financial profile, he can compare and contrast the information in the financial profile with known information about suspicious transactions (e.g., dates, origins, destinations, account holders, banks) to group and reconcile the transactions and identify any gaps in data. This will help the fraud examiner understand the flow of assets and identify leads.

Also, the tracing analysis should look for unexplained changes in the subject's income, expenses, lifestyle, travel patterns, and behavior to determine whether the subject has hidden assets. Such analysis might indicate activities designed to conceal income or income-producing property.

Here are three key questions to consider when conducting a tracing analysis:

- What are the sources of the subject's income, assets, and liabilities?
- Is there any missing or inconsistent information?
- Does the subject live a lifestyle that is in excess of the reported income?

Generally, fraud examiners can trace illicit transactions using a direct method or an indirect method. A *direct method* identifies the receipt or disposition of funds or assets through the analysis of specific financial transactions, whereas an *indirect method* employs circumstantial evidence to analyze the relationship between a suspect's receipt and subsequent disposition of funds or assets.

More specifically, a direct method employs direct evidence of the subject's books and records (or financial transaction records belonging to third parties) to analyze the relationship between a suspect's receipt and subsequent disposition of funds or assets.

But in many situations, direct evidence of a subject's books and records is not available; in such cases, the fraud examiner must use an indirect method, employing circumstantial evidence to analyze the relationship between a suspect's receipt and subsequent disposition of funds or assets.

Direct Methods of Tracing Financial Transactions

Direct methods of tracing financial transactions require access to the subject's financial records and involve the use of *direct evidence* (i.e., evidence that tends to prove or disprove a fact in issue directly), such as eyewitness testimony or a confession. Direct evidence is conclusive—the fact is established if the evidence is believed. For example, when a corrupt official is caught in the act of soliciting a bribe payment, witnesses' observations and video of the official's act are direct evidence against him. These items of evidence are conclusive to prove that the official attempted to receive an illicit payment.

Under a direct method, the fraud examiner uses the information in the individual's financial records to establish the subject's financial profile, which is then used to identify the subject's accounts, assets, and expenditures. Once these items are identified, the fraud examiner can use them to trace back the source of funds in each. In other words, under the direct process, the fraud examiner traces funds the subject used to purchase assets or make deposits back to his source.

There are several sources the fraud examiner can use to demonstrate a subject's financial standing and profile under the direct approach, but some common sources include:

- Documents from financial service providers (e.g., accountants or bankers)
- Tax records
- Accounting reports
- Financial statements
- Bank account records
- Payroll records
- Credit reports
- Court records
- Mortgage and loan files
- Credit card records

If the fraud examiner has access to the subject's financial records, he should analyze them to:

- Identify money deposited into the accounts.
- Discover money transferred out of an account by cash withdrawal, check, debit memo, or wire transfer.
- Identify increases and decreases in account balances.
- Create a summary of deposits and withdrawals.
- Develop a summary of checks written on the account.
- Establish a summary of wire transfers into or out of the account.

Also, when analyzing such records, the fraud examiner must be sure to record the dates, amounts, check numbers, names of payees, and the name of the endorsing bank for any relevant transaction.

Moreover, records obtained from financial institutions are perhaps the single most important financial source available to a fraud examiner for asset-tracing purposes. They can be used as evidence for fraud, as well as to:

- Identify witnesses and other evidence.
- Uncover criminal profits.
- Identify criminal assets.
- Locate assets that can be used to satisfy a judgment.
- Identify localities where assets are stored.
- Determine the lifestyle of an account holder.
- Determine the financial health of an organization.

- Determine the source of funds placed into the account.
- Determine the use of the funds from the account.

Although financial records are one of the most important sources available to fraud examinations, they are not available to the public and, therefore, might be difficult to obtain. In fact, financial records are private in almost all countries, including the United States. For example, in the United States, the Right to Financial Privacy Act prohibits financial institutions from disclosing financial information about individual customers to governmental agencies without following certain procedures specified in the law.

This discussion will examine how to use financial records to locate hidden assets, and it covers the following topics:

- Gaining access to financial records
- Establishing a database
- Types of financial records to examine
- Types of financial records to request
- Tracing financial transactions

Gaining Access to Records Held by Financial Institutions

Again, financial records are not available to the public and, therefore, might be difficult to obtain.

Often, fraud examiners use informants, witnesses, and surveillance operations to obtain information about financial records. But typically, these sources only help identify people or businesses with whom the subject is conducting financial transactions; they do not provide access to financial records.

Suspects generally will not willingly give their records to a fraud examiner, and financial institutions' authority to disclose bank records is restricted by federal and state law. In general, banks will not provide financial records to anyone, including law enforcement, unless the customer has consented or the institution is legally compelled to do so.

Generally, bank records can be obtained in most jurisdictions by using one of the following methods:

- A discovery request in a civil trial
- A legal order to produce documents, witnesses, or other things (e.g., a subpoena) or a summons issued by a government agency

- Civil summons
- Customer consents to disclosure by signing a release indicating that the information could be shared with a particular entity, usually in relation to a stated purpose (e.g., compliance with a financial disclosure requirement for employment or compliance with some court order)
- A court order that grants government authorities the right to search a premises or property for information pertinent to a case (e.g., a search warrant)

Furthermore, the cost of obtaining bank records can be high. Banks generally charge both public and private entities to search and retrieve records, and they might charge additional costs for the reproduction of records.

Yet, despite the limitations on obtaining financial records, fraud examiners might be able to, depending on their circumstances, obtain bank records from other sources. For example, the fraud examiner might seek to obtain access to financial records by contacting the subject's former spouse. Former spouses might have banking records useful to the fraud examination. Similarly, a suspect's banking records might be available as part of a divorce settlement or a lawsuit.

Establishing a Database

To aid in the analysis of financial records, fraud examiners should establish a database to sort and analyze the financial data for patterns of activity, as well as to code all records. By placing the records into a spreadsheet, database, or other type of data analysis software, the fraud examiner can compare records, uncover patterns, and execute a number of different searches and analyses of the data collected during the investigation.

Although a standard spreadsheet program might be fine for this purpose, databases are more effective than spreadsheets when dealing with large sets of raw data records.

When creating a database for financial data, the fraud examiner should create a profile for each bank account at issue and, as data is collected, the account profile information for each bank account can be combined with other collected data.

Bank profiles should include the following information:

- Bank name
- Bank address

- Account number
- Type of account
- Name of account holder
- Date of account opening and closing, if applicable
- Currency
- Current balance
- Annual credit turnover
- Annual debit turnover

Once the account profile is established, the fraud examiner can enter additional data about each account, such as credit and debit activity that occurs during the relevant period, date, amount, and, if available, the source or beneficiary of the funds.

The financial information available for each record varies, meaning the data entered in a spreadsheet or database will vary. But a basic list of elements that can be obtained from financial records can be obtained by considering the types of information contained in check records.

As illustrated in the following list, there are 17 primary elements that can be pulled from check records, including an element for general comments, and these elements can be used for almost all bank records.

1. Check number
2. Entity from
3. Bank from
4. Date written
5. Payee
6. Amount written
7. Amount deposited
8. Memo written
9. Signatory
10. Account number from
11. Transaction type
12. First endorser
13. Transaction bank
14. Deposited to account
15. Date of transaction
16. Location
17. Comments

Details on what goes into each of these fields are provided below:

1. *Check number*: This field should contain the number of the financial instrument written on or deposited to the account. The following items, however, will not contain a check number: wire transaction, automated teller machine transaction, point-of-sale transaction, and debit memo. A deposited amount would include a check number unless the deposit was cash, an incoming wire, or a credit memo.

2. *Entity from*: This field should contain the name of the company or person the check is from—the owner of the account on which the check is written.
3. *Bank from*: This field should contain the name of the bank from which the check, debit memo, or wire transfer was issued. If desired, the fraud examiner can enter the bank identification number to identify the bank's source of the funds.
4. *Date written*: This field should contain the date the check was written, the transaction (e.g., wire transfer or debit memo) was generated, or the withdrawal was made. This is not the date shown on the bank statement; bank statements show the clearing dates—the dates that checks clear the bank. The clearing date can be used if no other dates are present (e.g., if there is no check copy provided by the bank, but the check is listed on the statement).
5. *Payee*: This field should contain the name of the payee—the person or entity to whom the check was written.
6. *Amount written*: This field should contain the amount written on the face of the check. If there is a discrepancy between the numerical and written amounts, the bank will usually honor the written amount. Check the amount the bank has imprinted on the bottom right-hand side of the check in magnetic ink character recognition (MICR) to determine which amount the bank used.
7. *Deposited amount*: This field should contain the amount of money credited to the bank account by a cash or check deposit, wire transfer, or credit memo. This amount is put into a field separate from the amount written for ease of separating, sorting, and adding the amounts.
8. *Memo*: This field should contain any notation written on the "Memo" line or box on the check.
9. *Signatory*: This field should contain the name of the person (or persons) who signed the check as the authorized signatory. When entering the data into this field, initials are sufficient if the person referenced is clear.
10. *Account number from*: This field should contain the account number on which the check, debit memo, or wire transfer was written.
11. *Transaction type*: This field should contain the type of transaction (e.g., check, transfer, wire, debit memo, credit memo, deposit, ATM deposit or withdrawal, or ATM purchase).
12. *First endorser*: This field should contain the name of the first endorser. The *first endorser* is the person or persons who endorsed the check (i.e., signed the check on the back as the endorser). On checks made out to a company, the back of the check might be stamped with the company name, bank, and account number and no endorsing signature should be shown.

13. *Transaction bank*: This field should contain the name of the bank the item was deposited to (or where the check was cashed). This could be the bank from which records have been subpoenaed, the bank stamped on the back of the check, or the bank at which the check was cashed. If the check was negotiated at a non-bank financial institution (e.g., check-cashing agency, money transmitter, or casino), the name of that company can be placed here with other specifics entered in the "comments" field.
14. *Deposited to account*: This field should contain the account number to which the check was deposited. It should be noted that some banks write the account number on the back of checks when cashed; this serves as an identifier for the check casher. Therefore, a bank account number located on the back of a check might not mean that the check was deposited into that account. Remember to check the front of the check for a "cashed" stamp.
15. *Date of transaction*: This field should contain the date the check was deposited or negotiated.
16. *Location*: This field should be used for transactions made at an automated teller machine or a point-of-sale if the location is important.
17. *Comments*: The comments field is used for other comments about the transaction. NSF could be entered into the comments field to signify that there were non-sufficient funds to cover the check. Additional information about the endorser (e.g., driver's license or alien registration number), the name of a secondary endorser, or notes written on the back of the check by the teller could also be placed in the comments field.

Here are some basic rules to follow when entering records into a spreadsheet or database:

- Enter data as fully as possible.
- Assign unique names to identify each person, place, or thing in the case.
- Be consistent when assigning names and avoid giving multiple names for the same person, organization, or document.
- Have all records reviewed for accuracy.

Also, to foster uniformity in style and formatting, follow a set of standards for entering content. For example, when entering names, adhere to the following guidelines:

- Enter names in normal sequence (e.g., first, middle, and last).
- Use only capitals for initials.
- Omit titles, such as "Ph.D.," "M.D.," "B.A.," "M.A.," "D.D.S.," "Sr.," "Jr.," or "III."
- Eliminate periods after abbreviations and middle initials.

- If the given name or the surname is missing, use five underscore lines as a substitute for the unknown name (e.g., _____Brandt, John H _____).
- If a person is known primarily by his middle name, enter the name in all capital letters (e.g., Randy THOMAS Smith).

Types of Financial Records to Examine

While investigating financial records, the fraud examiner should review the following types:

- Account-opening documents
- Negotiated (canceled) checks
- Deposit tickets
- Wire transfer records
- Intrabank transfer records
- Electronic payment records
- Savings account records
- Certificates of deposit
- Account statements (e.g., bank statements)
- Exchange instruments
- Loan records
- Credit card records
- Prepaid access card records
- Bank collection department records
- Safe deposit box records
- Financial intelligence unit (FIU) documents and reports
- Stock brokerage records
- Tax returns and related documents
- Accounting records
- Purchase and sale documents

Account-Opening Documents

Account-opening documents include the records required to create a bank account, but the types of files required might vary depending on the type of account. This discussion will focus on two types of bank accounts: personal accounts and business accounts.

PERSONAL ACCOUNTS

To open a personal account, the individual opening the account must provide a signature card, or similar document, evidencing a contract between the customer and bank. When a depositor opens an account, the bank requires that a signature card, or equivalent record, be

signed (by hand or electronically). By signing the card or similar document provided by the bank, the depositor becomes a party to a contract with the bank under which he accepts all rules and regulations of the bank and authorizes the bank to honor his orders for withdrawing funds.

The signature card is a source of valuable information. Although the form of these cards varies, the card usually contains the person's name, address, telephone number, identification number (e.g., national number, uniform civil number, national identification number, national identity number, national insurance number, personal identification number, Social Insurance Number, or government identification number), amount of opening deposit (and possibly the source of opening deposit), and security data (e.g., mother's maiden name). The person's identification information might be significant, especially if the depositor used an alias. Also, a fraud examiner might be able to trace the opening deposit through the bank's records to disclose a source of income.

In addition to containing a signature card, the account-opening file for a personal account might contain a copy of the account holder's driver's license or other identification provided to the bank.

Many banks investigate the references given by a new customer. They might also make inquiries of various credit reporting agencies. This information is contained in a correspondence file or a credit file that can contain comments of the person who opened the account and might show information given by the depositor when opening the account.

In tracing information about a subject's transactions with the bank, the signature card and account number should be used. The signature card might contain the customer's taxpayer identification number (e.g., Social Security number) and account number, but if the account number does not appear on the signature card, it can be located in other places. Assigned account numbers can be located in the bank's customer information file, and they are encoded on customers' checks and deposit slips.

When requesting the signature card, the fraud examiner should determine whether the bank maintains any type of central file. Most large banks have a central file that lists all departments with which a customer has had dealings. If the bank has such a file, the fraud examiner does not need to check with each department to obtain information. The subject might at one time have had a bank account that later was closed. Requests for information

from a bank about a subject should always include a reference to both active and closed accounts. Records of closed accounts are usually maintained in a separate file.

BUSINESS ACCOUNTS

To open a business account, the party opening the account must provide documentation in addition to the documentation required for opening a personal account.

To open a business account for a corporation, the opening party must provide a signature card, or similar document, and copies of corporate resolutions of the board of directors authorizing the opening of the bank account and naming the person authorized to draw checks on the accounts. Also, the bank might require a copy of the company's organizational or business filings (such as articles of incorporation). These documents should indicate who the company's corporate officers are and its date of incorporation.

To open a business account for a partnership, the opening party must provide a signature card, or equivalent record, and a partnership agreement authorizing the opening of the bank account and naming the person authorized to draw checks on the accounts.

For an unincorporated company to open a bank account, the banking institution might require the company to provide a doing business as (DBA) registration, fictitious name registration, or business registration certificate. Generally, the required documentation depends on the applicable laws.

Negotiated (Canceled) Checks

Checks are a type of negotiable instrument—a written order promising to pay a sum of money—that instructs a financial institution to pay a specific amount of money from the check writer's account to the entity named on the check.

Negotiated (canceled) checks are checks cleared by a bank or other financial institution, and may serve as proof of payment. A check becomes canceled once it is processed and all appropriate accounts have been credited. Once canceled, a check is no longer negotiable.

Canceled checks written by a subject or received from others can provide valuable information. Canceled checks provide information on, among other things, the amounts, payees, and endorsees of payments made by check, and this data can provide leads and help identify a subject's assets.

Canceled checks can lead to hidden funds. For example, the absence of a check for a recurring payment for a particular month might indicate a cash payment, which in turn would indicate possible undisclosed cash income.

The back of canceled checks can contain many items of interest. A deposited check might show the name of the entity to whose account the money has been deposited and the account number. Also, it might contain the names of the financial institutions through which the check traveled.

In addition, the depository stamp on a check can identify the bank at which the check was cashed, and this information might provide a lead to another bank account.

When examining financial records, fraud examiners should study the checks written on the subject's account. Checks written on the subject's account can reveal various things, such as:

- Other bank accounts held by the subject
- The subject's credit cards
- Assets the subject has purchased
- The locations of the subject's assets (e.g., through the payment of real estate taxes, broker's fees, or utility payments)
- Loans the subject has obtained (which can provide valuable leads through the loan applications and financial statements that might be attached)

Also, the absence of a check for a recurring payment for a particular month might indicate a cash payment, which in turn would indicate a possible undisclosed income source.

Even though records of negotiated checks might contain valuable information, check usage has fallen, being partly replaced by electronic payment systems.

TRACING CHECKS

Fraud examiners can use bank identification symbols to trace negotiated checks. Fraud examiners do not have to understand the internal bookkeeping procedures used by banks to trace checks, but they should be familiar with the concept of bank identification numbers.

All checks printed for banking institutions contain a bank code (also known as institution number, routing code, and clearing code), and this number can be used in the tracing

process. The bank code enables a check to be routed to the bank of origin, and it is essential for delivering payment through the clearing system. In the process of routing, a trail is left.

Bank codes and the rules governing them, however, vary from country to country. Canada uses routing numbers, the United Kingdom uses Sort Codes, Ireland uses National Sort Codes, Germany and Austria use Bankleitzahl (BLZ codes), Switzerland uses Bankenclearing-Nummer (BC) and SIX Interbank Clearing Codes (SIC), France uses Code Banque and Code Guichet, and Australia uses Bank State Branch (BSB) numbers.

In the United States, checks contain an ABA transit number (also known as a routing number or routing transfer number), and banks use this number to identify specific financial institutions in the United States. ABA transit numbers are based on an identification code developed and assigned by the American Bankers Association, and a check's ABA number identifies the bank on which it was drawn. The ABA number was designed to facilitate the sorting, bundling, and shipping of paper checks back to the check writers' accounts. The ABA number is also associated with online banking and electronic funds transfers, and designates automated clearinghouses.

Such national codes, however, differ from the SWIFT Code (also known as the BIC Code). The SWIFT Code is the standard format used to identify a financial institution when transferring money internationally between banks.

MAGNETIC INK CHARACTER RECOGNITION

Many countries use magnetic ink character recognition (MICR) technology to facilitate the processing and clearing of checks, drafts, and similar items. MICR is a machine language, and the MICR encoding, called the MICR line, is comprised of numeric information that is printed on the bottom of checks using magnetic ink. This coding is electronically scanned by computers that convert the magnetic ink notations into electronic impulses that can be scanned and read by MICR readers.

Checks, drafts, or similar items that are not encoded with magnetic ink cannot be processed through the clearing system without special handling.

MICR information is printed in groupings called fields. Typically, the MICR is composed of the branch transit (routing) number, the customer's account number, and the amount field, and some checks contain serial numbers. The transit number indicates the institution on

which the check was drawn. The account number field shows the drawer's assigned account number at the bank. The amount field shows the amount of the check. When a check is processed through a bank, this field is added to the check. The dollar amount of the check should always equal the encoded MICR amount. These two figures should be compared to make sure that the subject did not alter the returned check.

The fraud examiner should physically inspect checks to ensure that the MICR information is consistent with any other written or printed information on the check's face. It is particularly important to ensure that the check has not been defaced and the MICR information has not been altered in any way.

Deposit Tickets

All deposits into financial institutions are accompanied by some type of deposit ticket. Deposit tickets are written records of money deposited into accounts. The deposit ticket is the principal source document for crediting the customer's account. Banks use them to keep track of money deposited.

Deposits are first recorded on the deposit ticket or slip and usually show the respective amounts of bills, coins, checks, and other forms of currency deposited. If the deposit was in check form, the deposit slip might show the bank identification number (e.g., ABA code in the United States) identifying the bank on which the deposited check was drawn.

Financial institutions, however, will only accept cash items (e.g., currency, checks, and bond coupons) and cash equivalents.

Deposit tickets can provide various leads. With the information contained on deposit tickets, fraud examiners can identify and trace deposits to their sources. Deposits made with checks can identify people who conduct business with the subject and other bank accounts the subject controls. In contrast, cash deposits can identify patterns of the subject's activities.

Also, when working with deposit tickets, the fraud examiner must remember that sometimes the depositor splits the deposit, meaning only part of the money is actually deposited. In these instances, the depositor either receives cash or requests that part of the proceeds be applied to a note or interest due to the bank.

Wire Transfer Records

A *wire transfer* is a transfer of money from one bank to another through a secure system. These transfers are processed by banks and by wire remittance companies such as Western Union and MoneyGram.

Often, fraudsters will move illicit funds abroad through wire transfers to break the audit trail and secure the funds in jurisdictions with relaxed standards. They also might use wire transfers to move assets abroad. Consequently, wire transfer records might contain evidence that money has been moved abroad.

As with other financial transactions, banks keep records of the wire transfers performed. Wire transfer records maintained by a bank might include:

- Fedwire, the Clearinghouse for Interbank Payments System (CHIPS), SWIFT, or other documents reflecting wire transfers of funds to, from, or on behalf of (the subject)
- Documents reflecting source of funds for wire transfer out
- Documents reflecting disposition of wire transfer in

Generally, to send a wire transfer, the issuing party will need the following information:

- The receiver's name
- The receiver's address
- The receiver's account number
- The name of the receiver's financial institution
- Wiring instructions for the receiving financial institution
- The city and state of the receiving financial institution
- The name and address of the person sending the wire

Thus, the information contained on a wire transfer generally will include the following items:

- The amount of the transfer
- The date of the transfer
- The name of the sender or originator
- The routing number of the originating bank or financial institution
- The identity of the designated beneficiary or receiver of the funds
- The routing number of the recipient bank

The following is a list of the forms and documents produced in connection with a wire transfer that the originating bank or financial institution might maintain:

- The wire transfer request form
- A copy of the wire transfer

- An advice statement or confirmation confirming the wire transfer
- An entry of the wire transfer that appears on the originating customer's account statement as a debit memo
- The originating customer's monthly account statement
- An internal log of outgoing wires
- A journal entry

Wire transfer documents maintained by the recipient institution might include:

- The wire transfer request form
- A copy of the wire transfer
- The credit memo the originating bank or financial institution sent to the beneficiary (if deposited)
- The customer's monthly account statement
- A journal entry
- A cashier's check
- Information on interbank book transfers that banks keep to clear transactions

Accordingly, wire transfer records might contain valuable information. The records of a wire transfer will identify who sent the wire, where it was sent, the date, and the amount. Also, the records of an international wire transfer will vary depending on the laws and policies of the receiving and origin countries and the receiving institution. Thus, if the wire transfer was sent out of the country, tracing the transfer depends on the laws and policies of the relevant countries and institutions. If, however, the wire transfer was sent to a bank in the United States, the recipient bank should have a record of the number of the account into which the funds were deposited.

Intrabank Transfer Records

Intrabank transfers are transfers of funds between different accounts (e.g., checking and savings) that a customer has at the same bank. Other departments within a bank can credit the depositor's account for funds collected, such as the proceeds of loans or items held by the bank for collection. Items held by the bank for collection are not always deposited to the customer's account; they are sometimes remitted directly to the customer.

Electronic Payment Records

Electronic payments (or e-payments) refer to any type of noncash payment that does not involve a paper check. Methods of electronic payments include credit cards, debit cards, and

the automated clearing house (ACH) payments, which include direct deposit of payroll, social security benefits and tax refunds, direct payment of consumer bills, direct debits, business-to-business payments, federal tax withholdings, and electronic checks (e-checks). Despite the numerous methods of electronic payments, there are three main types of electronic payment transactions:

- *One-time customer-to-vendor payments*: This type of transaction occurs when a customer needs to pay a company or individual one-time and where a continuing relationship is not expected.
- *Recurring customer-to-vendor payments*: This type of transaction occurs when a customer pays a bill through a regularly scheduled direct debit from his checking account or an automatic charge to his credit card.
- *Automatic bank-to-vendor payments*: Bank-to-vendor payments occur when bank customers make payments electronically from their bank accounts via electronic check or from their credit cards and debit cards directly to vendor accounts. Online bill pay is an automatic bank-to-vendor payment method.

Electronic payment records can be valuable in tracing investigations. They can serve as proof of payment, and they can reveal, among other things:

- Assets the subject has purchased
- The locations of the subject's assets (e.g., through the payment of real estate taxes, broker's fees, or utility payments)
- The locations of the subject's residences and businesses (e.g., through analyzing the payments of utility bills)
- Loans the subject has obtained (e.g., through analyzing loan payments)
- Payments made to nonexistent employees with direct deposit
- The cities and countries in which the subject conducts business (e.g., through analyzing the payments for carrier services to deliver packages)
- Assets ostensibly owned by family members or close associates but effectively controlled, held, or gifted by the subject
- Hotel payments
- The true owner of a property (e.g., through analyzing the mortgage payments and payments for home owner insurance)

Also, the absence of a recurring payment might indicate a cash payment, which in turn could suggest possible undisclosed source income.

Generally, records of a subject's electronic payments can be obtained from various sources. Financial institutions maintain electronic payment records. Also, businesses must record all electronic payments; therefore, vendors will have records of one-time customer-to-vendor payments, recurring customer-to-vendor payments, and automatic bank-to-vendor payments. Moreover, the subject might keep records of his online payments. When a customer makes an electronic payment online, he will receive payment confirmation. Often, customers print, write down, or otherwise save their payment confirmation information.

Savings Account Records

Savings accounts are accounts maintained by financial institutions that pay interest but cannot be used directly as money. Often, savings accounts are referred to as *time deposits*, which are money deposits that cannot be withdrawn for a certain period of time. Thus, sometimes savings accounts are not as readily available to the customer as checking account deposits. Funds in a savings account might be subject to a 30-day notice of withdrawal.

Certificates of Deposit

Certificates of deposit (CDs) are interest-bearing investment products that provide limited access to the money invested and a modest rate of interest. CDs are intended to be held until maturity, at which time the money may be withdrawn together with the accrued interest. Many banks impose penalties on money withdrawn from a CD before maturity.

The financial institution issuing a CD will maintain records related to the CD. The records will contain information identifying the customer purchasing or presenting the CD (i.e., name, address, and taxpayer identification number), and they will describe the CD, note the method of payment if purchased, and list the date of the transaction.

Account Statements (Bank Statements)

An *account statement* (or *bank statement*) is a summary of all the transactions and financial activity of a bank account and the account holder for a specified period (usually a month). Account statements are provided for all types of bank accounts, including checking accounts, money market accounts, savings accounts, CAP accounts (used by those who often deal in securities transactions), and others.

Account statements contain important information. In general, the details on an account statement include:

- The name and address of the bank in which the account is held
- The name and address of the account holder

- The account number
- The opening balance of the account for a specified period
- A record of all debit transactions (e.g., cash withdrawals from a teller, automated-teller machine (ATM) cash withdrawals, ATM payments, check payments, online payments, debit card payments, or bank fees) from the account for a specific period
- A record of all credit transactions (e.g., direct transfers, cash deposits, or check deposits) on the account for a specific period
- The account's closing balance for a specific period

In general, when examining account statements, fraud examiners should look for various things. In particular, they should seek to identify significant deposits made into the account. When doing so, fraud examiners should:

- Note whether there are any unusually high monthly balances. If there are, this fact might provide circumstantial evidence of illicit funds, even if the individual deposits cannot be identified.
- Identify deposits in even numbers, deposits made on regular dates, or deposits that cannot be connected to legitimate sources of income. (Legitimate deposits can be determined by comparing dates and amounts to company payroll information.)
- Identify large or unusual currency transactions or credit memo entries. Memo entries might indicate wire transfers, loans, certificates of deposit, investments, or other hidden assets.
- Obtain copies of any suspicious deposit items from the financial institution, if possible.

In addition, when examining account statements, fraud examiners should seek to identify the origin of the funds entering the account and the location where the funds have been transferred.

Moreover, when looking at account statements, fraud examiners should try to:

- Identify any large transfers or withdrawals.
- Identify any pattern transfers deposited on a regular basis.
- Identify unusually large deposits, deposits in even numbers, deposits made on regular dates, or deposits which cannot be connected to legitimate sources of income, and determine if any of the deposits are legitimate. (Legitimate deposits can be determined by comparing dates and amounts to company payroll information.)
- Identify any unusually high monthly balances because they could demonstrate the existence of illicit funds, even if the individual deposits cannot be identified.

- Identify large or unusual currency transactions or credit memo entries. Memo entries might indicate wire transfers, loans, certificates of deposit, investments, or other hidden assets.
- Identify any transfers to a friend or family member on a so-called debt.
- Identify any ATM withdrawals that do not reflect normal spending patterns.

Furthermore, when reviewing the subject's account statements, fraud examiners should review any checks written on the account, looking to identify:

- Other bank accounts
- Credit cards
- The purchase of major assets
- The location of major assets
- Evidence of loans (which can provide valuable leads through the loan applications and financial statements that might be attached)
- The absence of a check for a recurring payment because it might indicate that the payment was made in cash, which could indicate an undisclosed cash income
- Any checks made out as payable to "cash" (record where the check was cashed)

Exchange Instruments

Exchange instruments are vehicles by which the bank transfers funds, including cashier's checks, bank drafts, traveler's checks, bank money orders, and certified checks. Bank exchange instruments are often purchased with currency; therefore, they might be good sources of information about a subject's currency transactions.

CASHIER'S CHECKS

Cashier's checks (also called *bankers' drafts, bank checks,* or *certified checks*) are checks that have been issued and certified by a bank with itself as the drawer. These items are called *treasurer's checks* when issued by a trust company. Cashier's checks are frequently an excellent lead to other bank accounts, stock, real property, and other assets. Because cashier's checks can be held indefinitely, subjects sometimes purchase cashier's checks instead of keeping large amounts of currency on hand.

To reconstruct a subject's transactions with cashier's checks, the fraud examiner must be sure that all checks are accounted for because subjects sometimes exchange previously purchased checks for new ones.

Bank checks, such as cashier's checks, can be extremely time consuming and expensive to locate unless the fraud examiner knows the date and number of the check. However, if the subject has deposited a bank check into his account or purchased a bank check using a check from his account, copies of bank checks are much easier to obtain because the subject's account records will reveal the date and number of the bank check.

BANK DRAFTS

Bank drafts are checks drawn by the issuing bank on its account with another bank. Often, this other account is in the geographical area where the purchaser desires to make a payment. Bank drafts also can be used when a subject does not want to carry a large amount of cash.

TRAVELER'S CHECKS

Traveler's checks are checks issued in predetermined amounts by the American Express Company and other banks.

Traveler's checks are traced by their serial number. The issuing company usually keeps records of traveler's checks sent to it by the selling bank. The local bank that sold the checks might keep a copy of the sales order that lists the serial numbers. If the numbers are not available, the issuing bank might be able to supply the information if it is known when the checks were purchased. Canceled checks can be obtained from the issuer.

A target can purchase large amounts of traveler's checks from one bank and place them in another bank to avoid arousing suspicion by depositing cash.

It is important to note, however, that traveler's checks are declining in use. According to the U.S. Federal Reserve, usage of traveler's checks has declined each year since their peak in the mid-1990s.

BANK MONEY ORDERS

Bank money orders are similar to cashier's checks but usually are for small amounts. As with cashier's checks, subjects who are reluctant to use cash might use money orders.

CERTIFIED CHECKS

Certified checks are customer's checks stamped with the paying bank's guarantee that the maker's signature is genuine and that there is enough money available in the holder's account

to cover the amount to be paid. Certified checks are liabilities of the bank and, when paid, are kept by the bank. These checks are immediately charged against the customer's account by debit memorandums. Some banks permit customers to retrieve the original checks by surrendering the debit memorandum.

Loan Records

Loan records can provide important information regarding a subject. When a bank makes a commercial loan to an individual, it requires detailed statements of assets and liabilities from the borrower (e.g., income and the value of assets, such as homes, vehicles, real property, and business interests), and these records will be contained in the loan records. The loan file also might include the results of credit inquiries regarding paying habits, loan amounts, and present unpaid balances.

A bank credit department generally maintains the following basic records:

- *The credit or loan file*: This file includes the customer's loan application, financial statements, and general economic history.
- *The liability ledger*: This contains the customer's past and present liability to the bank. These sheets also contain information such as the loan date, note number, amount of the loan, interest rate, due date, and payments.
- *The collateral file*: This contains a complete description of the items pledged as security for loans. Records of such collateral can provide valuable information about a subject's assets.

When examining loan records, fraud examiners should look for red flags of unusual loans, including loans in odd amounts or loans that were not deposited into the subject's bank account.

Moreover, fraud examiners should look for loans with unusual repayments and trace them. Lump-sum payments, payments in odd amounts, accelerated payments, and large paydowns are unusual. These are all considered red flags indicating that an individual is seeking to conceal ill-gotten assets through a loan repayment, and loans with any such red flag should be investigated further.

If a fraud examination involves a loan with proceeds that have been disposed, the fraud examiner should trace the disposition of the loan's proceeds. *Loan proceeds* refer to the net amount a lender disburses to a borrower under the terms of a loan agreement. A fraud

examiner can trace loan proceeds to determine if hidden accounts were used for loan payments or if the proceeds were deposited into hidden accounts. Also, because loans might be secured by hidden assets or co-signed by previously unknown cohorts, tracing loan proceeds can uncover hidden assets or unknown witnesses. Moreover, if the subject has taken out a loan for someone else, tracing the disposition of the loan proceeds will uncover those leads.

Fraud examiners should also trace the source of loan payments for leads. For instance, if the loan payments were made from a previously unknown account, tracing the payments will uncover the unknown accounts. Payments made by a third party might reveal a cohort, kickback, or bribery scheme.

Tracing the disposition of loan proceeds is similar to tracing deposit transactions. When a lender disburses loan proceeds to a borrower, the borrower can use the proceeds in various ways. The borrower can deposit the proceeds into an account he has with the lender or into an account in someone else's name. The borrower can use the proceeds to purchase a certificate of deposit. The borrower might send the proceeds of a loan to another bank through a wire transfer. But commonly, the lender gives the borrower the loan proceeds in the form of a bank check, and if this occurs, the lender should be able to trace the check to determine where it was deposited or cashed.

Also, when fraud examinations involve loans with proceeds that have been disposed, fraud examiners should consider examining the loan application. The loan application should contain a financial statement, or its equivalent, on which the subject might identify other accounts and assets. The file might also contain tax returns, credit agency reports, and notes of interviews by the loan officer. The security used to obtain the loan, if any, might be a hidden asset.

LINES OF CREDIT

Lines of credit are another type of loan service that banks offer, and records of this type of loan services might contain valuable information. A line of credit is an arrangement between a bank and a customer whereby the bank extends a maximum loan balance that the customer can draw on when needed, as long as the customer does not exceed the maximum amount established in the agreement. And with most lines of credit, the customer makes payments only on the credit he actually used.

Generally, line of credit privileges are recorded on the customer's checking account, and the loan statement and check statement become one and the same. Copies of loan agreements and statements can be obtained from the bank files.

MORTGAGE LOAN FILES

Mortgage loan files often contain the most detailed financial statements submitted by a subject. The mortgage loan file should identify the party (e.g., title company or lawyer) that handled the closing, the homeowner's insurance carrier, the closing attorney (if applicable), and perhaps the real estate broker.

Additionally, the title company files often contain copies of the cashier's checks used for the down payment, and this can identify new accounts.

Also, the closing attorney will have many of the same materials that the title company maintains.

Similarly, the real estate broker might keep copies of personal checks used for deposits, and he might be able to provide information about other real estate transactions by the subjects. A mortgage loan file often contains a copy of the borrower's home owner's insurance policy, which might also contain valuable information. It might contain a rider that lists the homeowner's valuable assets, such as jewelry or furs, perhaps with appraisals and purchase receipts.

Fraud examiners should remember to look for accelerated or lump sum payments on the mortgage balance.

INSTALLMENT LOANS

Installment loans are loans in which the principal and interest are repaid in periodic installments. Often, installment loans are lent to individuals for personal, family, or household purposes. Loaning institutions create computer-generated reports that record the loan particulars and payment history.

Credit Card Records

Credit card records are important in tracing assets because they reveal a great deal of personal and business information about the account holder or cardholder. Among other things, credit card records show card purchasing limits, previous payment history, account

balance, when and where the subject has traveled, restaurants frequented by the subject, and assets the subject has acquired. In short, these records show the movements and habits of the person to whom the records pertain.

The credit card application and the bank's copies of monthly statements sent to the cardholder are the records that are most valuable to fraud examiners. Credit card applications require a considerable amount of financial information, and they generally require the same type of information found on a bank loan application. In today's environment, credit cards may be tied to bank accounts and may not require a separate application.

Credit card statements also contain a great deal of important information. Generally, these statements contain the name of the credit card issuer, the cardholder's account number, a summary of the transactions on the account, payment information, and a list of all the transactions that occurred during that month's billing cycle (i.e., purchases, payments, credits, cash advances, and balance transfers). Credit card records will document out-of-town travel and, often, they will name people with whom the subject conducts business.

Moreover, an abnormally high balance on credit cards might provide circumstantial evidence that the subject has a hidden source of income.

Additionally, information on credit card charges might provide leads to identifying hidden assets. For example, if a fraud examiner notices that the subject used his credit card to purchase items at a marina, the fraud examiner should investigate further to determine if the subject owns a boat.

Prepaid Access Card Records

Prepaid access cards are similar to debit and credit cards, but unlike debit and credit cards, prepaid cards do not require a checking or savings account or an extension of credit. Instead, with prepaid access cards, users pay in advance on an account and can use the funds anywhere credit and debit cards are accepted. Some cards even allow users to withdraw cash from the account at any ATM in the world. This payment method is popular with the so-called under-banked, or people who cannot or do not want to open traditional checking accounts (e.g., someone with bad credit, foreign travelers or laborers). The requirements for setting up a prepaid access card account are less stringent than those at traditional banks.

Bank Collection Department Records

The bank's collection department, which is normally involved in collecting amounts due on installment contracts and notes, can be used to collect personal checks (usually in large amounts and with special instructions), thus circumventing the normal recordkeeping associated with checking accounts. Such a transaction will not be reflected on the target's regular checking account statements but will appear in the collection department records.

Safe Deposit Box Records

Safe deposit boxes are private vault spaces rented by banks to customers. The nature of the relationship may vary between banks and their safe deposit box holders.

Banks keep no record of safe deposit box contents and rarely know what the boxes contain, but generally, banks maintain the following related records:

- Rental contract records
- Access records and entry logs

A safe deposit box's rental contract records, however, identify the renters, the person or people who have access to the boxes, their signatures, and the dates of the original agreements and later renewals. They also might contain other identifying information, including the name of the initiating bank officer. The officer's name could be significant if the subject (who might have used an alias in renting the box) must be identified.

Records showing access to the boxes vary from bank to bank. But generally, they contain the signatures of the people entering the boxes and usually the dates and times of entry. The entry records are filed in box-number order. The frequency of entry and the times and dates of entries might be significant and might correspond to the times and dates of deposits, withdrawals from other accounts, the purchases and sales of securities or property, and in other situations. Of course, proper authorization must be obtained before the bank will turn over any such records.

Because the bank records will not show the contents of the box, the fraud examiner can request permission to inventory the box with the presence of someone who is authorized to access it. If the fraud examiner does this, he should carefully note and describe the box's exact contents (e.g., legal description on deeds, numbers of insurance policies).

Financial Intelligence Unit Documents and Reports

Financial Intelligence Units (FIUs) are national centers that are responsible for receiving and analyzing information on suspicious or unusual financial activity in order to combat international financial crimes. FIUs are also designed to improve global cooperation and promote mutual exchange of financial intelligence information.

Financial regulations and legislation obliges banks and other financial institutions to file reports detailing large cash transactions or suspicious activity with FIUs, and the documents and reports filed with FIUs might contain valuable information that can be useful in tracing hidden assets.

In the United States, for example, the Bank Secrecy Act (BSA) sets forth a system of reporting and recordkeeping requirements designed to help track large or unusual financial transactions. Under the BSA, banks and other financial institutions are required to file reports detailing large cash transactions or suspicious activity with the Financial Crimes Enforcement Network (FinCEN), the U.S. version of a FIU. FinCEN was designed to safeguard the financial system from the abuses of financial crime, and it works to maximize information sharing among law enforcement agencies and its international partners in the regulatory and financial communities.

FinCEN maintains information from various reports and forms that might be relevant to an asset investigation, including:

- Currency Transaction Reports (CTRs)
- Suspicious Activity Reports (SARs)
- Foreign Bank and Financial Account Reports (FBARs)
- Currency or Monetary Instrument Reports (CMIRs)
- IRS/FinCEN Form 8300

Similarly, in Australia, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) sets for the reporting obligations designed to combat money laundering or terrorism financing. The Australia Australian Transaction Reports and Analysis Centre (AUSTRAC), which is the Australian FIU, regulates the AML CTF Act.

In the United Kingdom, the law provides that organizations must report activity that may be linked to money laundering or terrorist financing to the National Crime Agency (NCA). A report to the NCA is commonly known as a suspicious activity report (SAR).

In Canada, similar reporting obligations are imposed under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's FIU.

Like their U.S. counterpart, the anti-money laundering and counter-terrorist financing laws in countries around the globe impose reporting and recordkeeping requirements on banks and other financial institutions within their jurisdictions. Such laws require that suspicious transactions be reported to the FIUs, and these reports contain, among other things, the identity of the persons making the transactions and the amount of the transactions. They can also provide valuable information that can be used to:

- Identify illegal activity.
- Detect the flow of illicit funds.
- Identify leads to assets purchased with ill-gotten gains.

Stock Brokerage Records

When attempting to trace illicit transactions, the fraud examiner should, if available, look at the subject's brokerage account records. Because brokers place customer orders, maintain customer accounts, and send account statements to customers, a subject's broker or brokerage firm will have all source documents relating to the subject's securities account activity.

Many stock brokerage houses now offer the same type of services as banks, such as check-writing privileges, credit cards, and loans (against the value of securities held), as well as their normal securities business.

If stock brokerage records are at issue, the fraud examiner should request all records pertaining to the subject; however, he should make sure that the request specifically includes the following items:

- *Account application:* When a customer opens an account, he will typically fill out an account application that will contain personal and financial data, such as bank accounts.
- *Customer account information:* This information is usually computerized and is kept in the broker's files for reference. It will include all transactions conducted for the customer.
- *Signature card:* A signature card should be on file that will show all those authorized to conduct transactions on the account.
- *Securities receipts:* These receipts are issued to a customer when he delivers securities to the broker for sale.

- *Cash receipts:* These receipts are issued to a customer when he delivers currency to the broker.
- *Confirmation slips:* These are issued to a customer to show the type of transaction (buy or sell) and the amount involved in the transaction.
- *Securities delivered receipt:* This receipt is signed by the customer when a securities purchase is delivered to the customer.
- *Brokerage account statement:* This statement is usually issued monthly and provides information on all transactions conducted during the reporting period. It lists all purchases and sales, the name of the security, the number of units, the amount per unit, the total amount of the transaction, the account balance, payments received from the customer, disbursements to the customer, and the securities that are held by the brokerage firm for the customer.

When looking at stock brokerage records, the fraud examiner will be primarily interested in the source of the funds used to purchase securities or deposited to a cash account. The subject's monthly account statements, which are somewhat more complex than equivalent bank statements, reflect these transactions. Monthly account statements can be interpreted with the help of explanatory material on the statement or with the assistance of a brokerage firm employee.

All receipts for the purchase of stock should note whether the payment was made in currency or check. If payment was made by check, the fraud examiner should make a note of the bank code on which the check was drawn. This information might lead to a previously undiscovered bank account. Bank codes for check processing vary from country to country. Many countries, especially in Europe and the Middle East, use International Banking Account Numbers (IBAN), which is an international format for banking account numbers designed to avoid confusion in international transactions. SWIFT is the official registrar of IBAN numbers. U.S. banks will be listed under an American Bankers Association (ABA) code.

Additionally, the fraud examiner should look at any checks the brokerage firm issued to the subject for proceeds generated from the sale of stock.

Moreover, the fraud examiner should look for purchases the subject might have made under other names, since stocks, bonds, mutual funds, and so on can be purchased easily through a stockbroker or under the names of friends and relatives.

Tax-Related Documents

Tax-related documents (such as W2s and 1099s in the United States) might explain what entities earn and what deductions they take.

Personal tax records, if available, might provide indirect evidence of illicit payments, such as profits or losses from previously undisclosed business ventures, or interest and dividends on hidden CDs and bank accounts. Tax records might also reveal deductions and expenses that can lead to previously unknown funds or assets.

In addition to examining the subject's tax records, fraud examiners should interview the subject's accountant and tax preparer, and, if possible, obtain their files and work papers.

Specifically, tax-related documents can provide the following information:

- Where the subject works
- The subject's interest income
- The subject's dividend income
- Details about the subject's businesses and partnerships
- Income-producing property owned by the subject
- Royalties the subject receives
- The subject's sources of income
- The subject's government identification number

Accounting Records

Businesses record financial transactions through journal entries that identify account names and amounts, and these entries are summarized in each entity's financial statements, which include the income statement, balance sheet, and cash flow statement.

Accounting records can be valuable to a fraud examination because fraudsters often manipulate accounting records to conceal their misconduct. Thus, fraud examiners should review any relevant financial account and transaction records, such as bank statements, the cash journal, the petty cash journal, expense reports, and so on.

Purchase and Sale Documents

Documents concerning the purchase or sale of assets can be of value to an asset investigation. Such documents might include land registry documents, purchase agreements, sale agreements, loans, mortgages, tax returns, or credit card statements.

When a fraud examiner has obtained purchase or sale documents, he should examine the following items:

- The date of the purchase and sale
- The value at the date of the purchase and sale
- The name of the seller and buyer
- The method of payment used
- The source of the funds used

Indirect Methods of Tracing Financial Transactions

If illicit transactions cannot be traced directly to the subject, then an indirect method of proof might be required to corroborate evidence of illicit transactions. In contrast to the direct approach method, which relies on specific transactions, the indirect approach relies on circumstantial proof.

Circumstantial proof refers to evidence that tends to prove or disprove facts in issue indirectly, by inference. For example, in a bribery case, the prosecuting attorney might offer circumstantial evidence that the defendant, who is accused of receiving bribes, has lived beyond his means for over seven years. To show that the defendant has been living beyond his means, the government might present a summary of the defendant's assets and compare them to his reported income during those seven years; this analysis serves as circumstantial evidence that the defendant has been living beyond his means.

Almost all individuals and business entities determine income by the specific-items or specific-transactions method. Most entities that engage in legitimate pursuits maintain books and records in which they record transactions as transactions occur, and their income computations are based upon the total transactions during a given period. In fraud examinations, income can usually be established more readily by the direct approach; for this reason, it should be used whenever possible.

But in many cases, a subject's books and records are not made available to the fraud examiner, and in such cases, he must use an indirect approach. An indirect analysis can reveal that a suspect has more money available than can be accounted for from legitimate sources. In addition, evidence that the suspect lives beyond his means might demonstrate that he has unexplained income. Such evidence can also be used to corroborate the

testimony of co-conspirators as circumstantial evidence of the underlying misconduct or as evidence to impeach testimony denying the allegations.

Generally, fraud examiners should use indirect methods of proof in the following situations:

- The subject's books and records are not made available to the fraud examiner, and therefore, he must use an indirect approach to establish the subject's income.
- The fraud examiner suspects that the subject's books do not reflect all income.
- The subject experienced a significant increase in net worth.
- The subject's gross profit percentage, which represents how much sales revenue is spent on providing the goods and services sold, changes significantly.
- The subject's expenses exceed his reported income without cause.
- The subject has a large amount of income from unidentified sources.

There are two basic approaches that use circumstantial proof to prove a subject's sources of funds: the net-worth method—the asset method and the expenditures (source and application of funds) method—and the bank deposit analysis method.

Net-Worth Method

Examining for fraud not only involves the examination of the subject's books and records, but it might also entail the estimation of the fraud suspect's change in net worth or expenditures. If fraud is suspected, then using either of the net-worth methods might help in establishing evidence of a fraud.

The net-worth method (or comparative net-worth analysis) is used to prove illicit income circumstantially by showing that a person's assets or expenditures for a given period exceed that which can be accounted for from known or admitted legitimate sources of income. The net-worth method is a reliable method for estimating a person's ill-gotten gains. The method is used extensively by criminal investigators around the world, especially in drug and money laundering cases.

The net-worth method relies on the balance sheet format readily recognizable in the business world, and using the net-worth method will present a complete financial picture of a subject. The net-worth method is based on the theory that a party's income can be determined by the increases or decreases in that party's net worth during a period, adjusted for living expenses.

Net worth can be defined as the difference between assets and liabilities at a particular point in time.

Under the net-worth method of analysis, the fraud examiner determines the increase or decrease in the subject's net worth from year to year by comparing it at the beginning and end of the period, usually a calendar year, in question. Once the fraud examiner makes this determination, he can make adjustments for the subject's living expenses to calculate income (i.e., money derived from all sources). By subtracting the subject's funds from his known sources of income (e.g., salary, wages, interest, or dividends), the fraud examiner can identify funds that the subject received from unknown or illegal sources.

Fraud examiners should use the net-worth method when several of the subject's assets or liabilities have changed during the period under examination and when the target's financial records are not available.

To use the net-worth method, fraud examiners must obtain information about the subject's assets, liabilities, and living expenses. Such information can be determined from a variety of sources, such as:

- Interviews with:
  - The subject
  - Informants or sources
  - The subject's companions or associates
- Surveillance (i.e., observing targets for information-gathering purposes)
- Real estate records
- Court judgment and lien records
- Bankruptcy records
- Motor vehicle records
- Loan applications
- Financial statements
- Accountant's work papers
- Lawsuits and depositions
- Credit card applications or statements
- Tax returns
- Insurance records
- Child support and divorce records
- Canceled checks and deposited items
- Employment applications and salary checks
- Commercial database vendors and investigative service providers
- Online sources (e.g., commercial databases, websites, social networking sites)

One might question why items that do not change should be included when calculating the net-worth statement, particularly because they have no bearing on the final result. The answer is that a net-worth statement gives a complete financial picture of the subject; therefore, it should be as complete as possible so that the target will not be able to contest it on the grounds that items were omitted. Additionally, the net-worth statement can be the foundation for an examination of the subject, and a complete statement will prove extremely valuable at that time.

There are two basic methods for performing a net-worth analysis to examine a subject's sources of income: the *asset method* and the *expenditures* or *sources and applications of funds method*. Each of these methods is appropriate in different circumstances. Fraud examiners should use the *asset method* when the subject has invested illegal funds to accumulate wealth and acquire assets, causing his net worth (value of assets over liabilities) to increase from year to year. The *expenditures method* works best when the subject spends illicit income on consumables (e.g., travel and entertainment), because when the subject spends the illicit income, it will not cause an increase in net worth.

The asset method and the expenditures method involve similar steps. Both begin by assembling the financial and behavioral profile of the subject. Once the fraud examiner has assembled the financial and behavioral profile, he should identify all major assets and liabilities, sources of income, and major expenses during the relevant period. After these items are identified, the fraud examiner should perform a net-worth analysis, comparing the increase, if any, in the subject's net worth or the level of expenditures to the legitimate funds available. Unaccounted funds might be inferred to come from illicit or hidden sources.

Develop a Personal Profile of the Subject

Again, to perform the asset method or the expenditures method, the fraud examiner should assemble the personal—financial and behavioral—profile of the subject.

THE FINANCIAL PROFILE

When using the net-worth method of analysis, the fraud examiner should begin by establishing a financial profile for the subject. The *financial profile* is essentially a financial statement about an individual. It shows what the subject earns, owns, owes, and spends at any given point, or over a period; it reflects the subject's income, expenses, assets, and liabilities.

The subject's financial profile contains financial information that can identify inappropriate activity. The numbers in a subject's financial profile will indicate where the subject's money is coming from (income) and where it is going (expenses).

Accordingly, the financial profile can serve various purposes. The financial profile might yield direct evidence of illegal income or hidden assets, or circumstantial evidence thereof, by showing that the suspect's expenditures exceeded known sources of income. It can be used to establish the level of criminality, to build evidence for litigation, to support a request for an enforcement order, to identify fund transfers between entities, and so on.

The financial profile can reveal transactions involving significant amounts, such as large deposits or expenditures, but not smaller currency transactions, particularly transactions for concealed activities, consumables, or unusual one-time expenses, such as medical bills.

Fraud examiners can create a financial profile with the subject's books and records (e.g., financial records, tax records, accounting records, payroll records), but without access to such books and records, fraud examiners can rely on circumstantial proof that suggests or leads to information from which a subject's financial standing can be inferred. Typically, fraud examiners can develop a subject's financial profile by:

- Conducting interviews with the subject and his associates
- Observing the subject's lifestyle, habits, and assets (e.g., observing the subject's residence, hobbies, and vehicles)
- Using public records (e.g. criminal court records, civil court records, business filings, or real property records)
- Using online resources
- Viewing the subject's charitable contributions
- Obtaining anecdotal information

To prepare the financial profile, examiners should take the five steps discussed below.

STEP 1

First, identify all significant assets held by the suspect. An *asset* is cash (on hand) or anything else of value that can be converted into cash.

Cash on hand comprises coin and currency (e.g., bills, coins, notes) in the subject's possession (i.e., on the subject's person, in the subject's residence or other place in a

nominee's hands, or in a safe deposit box). Cash on hand does not include money in any account with a financial institution.

When using the net-worth method, the amount of cash on hand might be the most difficult item to verify. Usually, suspects will claim that their cash on hand is sufficient to account for any unknown sources of income.

To establish a firm starting net worth, the fraud examiner must show that the subject had no large cash sums for which he was not given credit. This is usually done by offering evidence that negates the existence of a cash hoard. Such evidence might include:

- Written or oral admissions of the subject concerning net worth (a signed net-worth statement or an oral statement as to cash on hand)
- Low earnings in pre-examination years, as shown by records of former employers and/or tax returns filed by subject
- Net worth, as established by books and records of the subject
- Financial statement presented for credit or other purposes at a time before or during the period under examination (banks, loan companies, and bonding companies are some of the better sources from which to obtain this type of document)
- Bankruptcy before examination periods
- Prior indebtedness, compromise of overdue debts, and avoidance of bankruptcy
- Installment buying
- History of low earnings and expenditures, and checks returned for insufficient funds (a financial history covering members of the subject's family also might be helpful)
- Loss of furniture and business because of financial reasons
- Receipt of some type of public assistance

STEP 2

Second, identify all significant liabilities. A *liability* is an obligation (debt) arising from an oral or written promise to pay, and it includes mortgages, loans, credit card debt, installment loan payments, and other debts. Record all of the subject's liabilities.

STEP 3

Third, identify all income sources during the relevant period. *Income* includes money, or other things of value, received in exchange for services or goods. Income is never included as an asset. Loan proceeds are not included as income but are treated as an asset that is offset by a corresponding liability.

STEP 4

Fourth, identify all significant expenses incurred during the relevant period. An *expense* is any payment for consumables, for personal or business reasons, over the relevant period. Expenses are not included as liabilities.

STEP 5

After identifying a subject's assets, liabilities, income, and expenses and assigning them values, analyze the collected information using the following charts.

The Financial Profile

TYPICAL ASSETS	**For each significant asset, determine:**
• Residence • Real estate • Bank accounts • Stocks and bonds • Automobiles • Insurance • Cash on hand • Jewelry • Clothing • Collectibles • Pensions • Home furnishings • Boats	—When was it acquired and from whom? —How much did it cost? —How was it paid for (currency, check, cashier's check)? —What source of funds was used to acquire it? —What documentation exists for the purchase and where is it?

TYPICAL LIABILITIES	**For each significant liability, determine:**
• Mortgage(s) • Other loans • Lines of credit • Credit cards • Installment purchases • Accounts payable • Taxes and other bills • Alimony and child support	—What was the original amount of the liability? —What is the present balance due? —When was the liability incurred? —What was the purpose for the loan or debt? —How were the proceeds used and where were they deposited? —What security (collateral), if any, was given for the debt? —What documentation exists for the transaction and where is it? —Was the debt written off as a bad loan for tax purposes? —Who was the creditor or lender?

TYPICAL SOURCES OF FUNDS		For each source of funds, determine:
• Salary • Gifts • Rental income • Dividends • Interest • Sale of assets	• Insurance proceeds • Commissions and fees • Awards • Inheritances • Disability payments	—What was the total amount during a given period? —What was the source? —How was it paid for (currency, check, other means)? —When were the funds received? —Where was it deposited? —How was it spent? —What documentation exists and where is it?

TYPICAL EXPENDITURES		For each major expenditure item, determine:
• Rent and mortgage • Health costs • Interest on loans • Credit cards	• Car payments • Travel • Clothing • Utilities • Food • Insurance	—What was the total amount spent? —How was it paid for? —Where were the funds obtained to pay the expense? —What documentation exists and where is it? —When was the payment made?

THE BEHAVIORAL PROFILE

Situational factors can affect the reliability of a financial profile. A financial profile might have information gaps, but such factors and gaps can be filled in by preparing the behavioral profile. The behavioral profile is comprised of outside pieces of information that can support estimates and fill information gaps.

The behavioral profile complements the financial profile. While the financial profile works best for large transactions, the behavioral profile is best at identifying smaller activities and smaller currency transactions.

The behavioral profile contains information about the suspect's personal characteristics (e.g., carries large amounts of cash, wears expensive clothes, or has club memberships), home and furnishings, automobiles, and leisure activities.

Accordingly, the behavioral profile reveals the subject's lifestyle habits (or lifestyle indicators) that might lead to identifying hidden wealth or assets—what is important to him that would cause the fraudster to start accumulating illicit income (e.g., where he travels, what type of expenditures he makes, associates, significant others, pertinent habits, interests, and addictions). Thus, the information in the subject's behavioral profile might suggest that he is

living beyond his apparent means, and thus probably has hidden income or hidden sources of income.

The following table contains lifestyle indicators that, if present, might suggest that the subject is living beyond his apparent means or has hidden wealth or assets.

Lifestyle Indicators			
Personal Characteristics	**Lodging**	**Transportation**	**Leisure Activities**
Large amounts of cash	Expensive housing	Luxury or exotic cars	Expensive vacations
Designer clothes	Expensive furnishings	Numerous vehicles	Cruises
Expensive jewelry	Valuable art	Late model vehicles	Boats
Club memberships	Vacation homes		Planes
Fitness clubs/spas			

Information for the behavioral profile is gathered from interviews and observation of lifestyle and habits, as well as from documentary sources.

To illustrate the behavioral profile, consider the conduct of convicted fraudster Donald Boyd. While working for Audio Aid, a telecommunications company, Boyd manipulated the company's financial records to skim $6 million, and once he began the scheme, Boyd made many changes to his lifestyle. Among other things, Boyd purchased high-priced cars, boats, jewelry, and a lake house where he enjoyed golfing, horseshoes, and boating. Boyd also frequented a casino where he gambled more than $260,000.

Information gathered for the behavioral profile might indicate the existence of illicit income or hidden assets. For example, if the suspect spent significant amounts of cash but had no corresponding cash withdrawals from his known bank accounts and no disclosed sources of cash income, the fraud examiner might presume that he has other, undisclosed sources of income.

Additionally, the behavioral profile might also provide evidence of a possible motive of the crime, such as large debts, as well as additional evidence of illicit funds. For example, if the suspect spent significant amounts of cash and had no corresponding cash withdrawals from

his disclosed bank accounts or no admitted sources of cash income, he must have other undisclosed sources of income.

Perform a Net-Worth Analysis

After profiling the subject, the fraud examiner should perform a net-worth analysis to look for unexplained changes in the subject's income, expenses, lifestyle, and behavior to determine whether the subject has any undisclosed sources of income.

The net-worth analysis is based on the reality that any recipient of income, whether honest or dishonest, can dispose of his income in only four ways: save it, buy assets, pay off debts, or spend it.

Net-worth analysis should begin once the suspect's financial profile is complete. By identifying the suspect's assets, liabilities, income, and expenses, the fraud examiner can develop a net-worth statement. Once the fraud examiner has developed a net-worth statement by identifying a suspect's assets, liabilities, income, and expenses, he can compare changes in the suspect's net worth to his known income. If the comparison reveals any differences, it can be inferred that the differences stem from unknown sources.

Again, there are two basic methods to examine a subject's sources of funds using a net-worth analysis: the *asset method* and the *expenditures* or *sources and applications of funds method*.

ASSET METHOD (COMPARATIVE NET WORTH)

Again, fraud examiners should use the asset method when it is suspected that the subject has accumulated wealth and acquired assets with illicit proceeds, which causes the subject's *net worth*—the difference between a person's assets and liabilities at a particular point in time—to increase.

The asset method allows the fraud examiner to prove income circumstantially by showing that the subject's assets for a given period exceed those that can be accounted for from known or admitted sources of income. Under the asset method, the fraud examiner determines the increase or decrease in the subject's net worth from year to year by comparing the subject's net worth at the beginning and end of the period in question. And, once the fraud examiner makes this determination, he can make adjustments for the subject's living expenses to calculate the subject's income (i.e., money derived from all sources). Specifically, by subtracting the subject's funds from his known sources of income

(e.g., salary, wages, interest, or dividends), the fraud examiner can identify funds that the subject received from unknown or illegal sources.

Although the asset method can be applied for any number of years, it is best to start with the year before the suspected fraudulent activity began.

The formula for the asset method is:

	Assets
–	Liabilities
=	*Net worth*
–	Prior year's net worth
=	*Net worth increase*
+	Living expenses
=	*Income (or expenditures)*
–	Funds from known sources
=	*Funds from unknown sources*

When using the asset method, consider the following issues:

- All assets should be valued at cost, not fair market value. Subsequent appreciation or depreciation of assets is ignored.
- The amount of funds available to the subject from legitimate sources should be estimated or computed generously. The amount of the subject's expenditures, particularly hard-to-document living costs, such as food and entertainment, should be estimated conservatively to give the subject the benefit of any doubt.
- The subject should be interviewed to identify all alleged sources of funds and to negate defenses that he might raise later.

To compare the subject's net worth using the asset method, first establish the starting point, generally the year before the target's illegal activities begin. This will be referred to as year one in the following computations.

Next, compute the target's net worth at the end of year one. Identify all assets held by the subject, valued at cost, including assets acquired earlier, and the amount of current liabilities. Calculate the difference between the value of the assets and the liabilities to determine the target's net worth at year one, or opening net worth.

EXAMPLE

Year One

Assets at Cost		Liabilities	
Residence	$100,000	Mortgage balance	$ 90,000
Stocks and bonds	30,000	Automobile loan	
Automobile	20,000	balance	10,000
TOTAL	$150,000	TOTAL	$100,000

Assets	$150,000
Liabilities	-100,000
Net Worth	$50,000

Compute the target's net worth for year two, using the same method.

EXAMPLE

Year Two

Assets at Cost		Liabilities	
Residence	$100,000	Mortgage balance	$50,000
Stocks and bonds	30,000		
Automobile	20,000	Automobile loan	
CD	50,000	balance	0
TOTAL	$200,000	TOTAL	$50,000

Assets	$200,000
Liabilities	-50,000
Net Worth	$150,000

Note that in the example the target's net worth increased by $100,000 during year two. To determine the source of such an increase, determine the target's known income during year two and subtract known expenses for year two.

EXAMPLE

Year Two

Income		Expenses	
Salary	$30,000	Mortgage interest payments	$20,000
Commissions	20,000	Living expenses	10,000
TOTAL	$50,000	TOTAL	$30,000

The difference between the target's income and expenses equals the increase (or decrease) in net worth from year one to year two, which can be attributed to known sources. Here it is $20,000. Subtract the increase in net worth from known sources from the total increase in net worth to determine the amount from unknown sources.

EXAMPLE

Total increase in net worth	$100,000
Increase attributed to known sources	<20,000>
Dollars from unknown sources	$80,000

Repeat these steps for subsequent years as necessary.

EXPENDITURES (SOURCES AND APPLICATION OF FUNDS) METHOD

The expenditures method (also known as the sources and application of funds method) compares the suspect's known expenditures and known sources of funds during a given period of time. That is, this analysis seeks to quantify the cost of the subject's lifestyle and determine whether the subject's reported income is sufficient to support his lifestyle.

To conduct this analysis, quantify the subject's known living expenses (e.g., groceries, mortgage, auto lease, insurance, credit card payments, income taxes), and then compare those expenses to the subject's known sources of income, such as wages, bonuses, dividends, gifts, and loan proceeds. If, after conducting this analysis, there are differences between the subject's expenses and the known income (i.e., the subject's spending exceeded the known sources of income), it is likely that the remaining differences can be attributed to hidden income.

The expenditures method is closely related to the net-worth analysis; they are accounting variations of the same principle.

This method is best used when the subject spends illicit income on consumables (e.g., travel and entertainment) that would not cause an increase in net worth. Thus, this method might be valuable in the following situations:

- There is evidence that the subject's income cannot support his lifestyle and spending habits.
- The subject operates mostly on a cash basis.
- The subject has little or no net worth, but he has large expenditures.
- The subject experiences little or no change in assets or liabilities.

The following table illustrates the formula used to analyze a subject's income using the expenditures method. The steps are discussed in greater detail here.

	Expenditures (application of funds)
–	Funds from known sources
=	*Funds from unknown sources*

To analyze the subject's financial status using the expenditures method, follow three steps:

1. Establish the subject's known expenditures for the relevant year. Expenditures include the use or application of funds for any purpose, including deposits to bank accounts, purchase of major assets, travel and entertainment expenses, and payment of loan and credit card debts.
2. Identify all sources of funds available to the subject, including loans and gifts, as well as cash on hand from previous years.
3. Compute the difference between the amount of the suspect's expenditures and his known income to determine the amount attributed to unknown sources.

EXAMPLE

Subject	Year One	Year Two
Application of funds:		
Increase in bank balance	$2,000	$10,000
Down payment on residence	——	10,000
Purchase of automobile	10,000	———
Mortgage payments	8,000	20,000
Credit card payments	5,000	10,000
Other expenses	15,000	30,000
TOTAL	**$40,000**	**$80,000**
Less funds from known sources:		
Cash on hand	1,000	
Salary	30,000	38,000
Interest earned on savings		
Account	1,000	2,000
Loan proceeds	8,000	
TOTAL	**$40,000**	**$40,000**
Funds from unknown or illegal sources	**0**	**$40,000**

Bank Deposit Analysis Method

In addition to the net-worth method, the bank deposit analysis method is another method that can be used to prove unknown sources of funds by indirect or circumstantial evidence. It is a variation of the source and application of funds method in which deposits to financial institutions are compared to legitimate income.

The bank deposits method computes income by showing what happened to a subject's funds. It is based on the theory that if a subject receives money, he can only do two things with it: He can deposit it or he can spend it.

The bank deposit analysis method is best applied in situations when the majority of the subject's income is believed to be deposited into known bank accounts, the subject's assets and liabilities are fairly constant from year to year, and there are no indications of extravagant expenditures.

Under this method, the subject's income is established by analyzing the subject's deposits to financial institutions, canceled checks, and the subject's currency transactions. Next, adjustments for non-income items are made to compute the subject's income.

The basic formula for the bank deposits method is:

	Total deposits to all accounts
–	Transfer and redeposits
=	*Net deposits to all accounts*
+	Cash expenditures
=	*Total receipts from all sources*
–	Funds from known sources
=	*Funds from unknown or illegal sources*

The bank deposits method is recommended as a primary method of proof when most of the subject's income is deposited and the subject's books and records are unavailable, withheld, incomplete, or maintained on a cash basis. The use of the bank deposits method is not limited to these circumstances, however. Even if the target's books and records might appear to be complete and accurate, the bank deposits method can still be used.

The basic sources of information for conducting a bank deposit analysis include interviews, analyses of the books and records, and analyses of the bank accounts. An interview with the subject should seek to determine the subject's expenditures by cash and checks, bank accounts, and loans and other receipts.

Total Deposits to All Accounts

The subject's total deposits consist of amounts deposited to all bank accounts maintained or controlled by the target and also deposits made to accounts in savings and loan companies, investment trusts, brokerage houses, and credit unions. Total deposits also include the accumulation (increase) of cash on hand. Because some subjects have bank accounts in fictitious names or under special titles, such as "Special Account No. 1," "Trustee Account," or "Trading Account," the investigator should look for this type of account during the investigation. If a subject lists checks on a deposit ticket and deducts an amount paid to him in cash (split deposit), only the net amount of the deposit should be used in computing total deposits.

Additional items that must be included in deposits are property and notes that the subject received in payment for services. The accepted practice is to consider these items as depositories into which funds have been placed for future use.

Net Deposits to All Accounts

Once the total deposits to all accounts has been established, the net deposits must be established. To calculate net deposits, subtract all transfers or exchanges between bank accounts, as well as funds that are redeposited as non-income items from total deposits. Failure to eliminate these items will result in an overstatement of income.

Cash Expenditures

Next, determine the subject's cash expenditures and add them to the amount of net deposits to determine the total receipts from all sources. Cash expenditures consist of the total outlay of funds less net bank disbursements.

The basic cash expenditures formula is:

	Total outlay of funds
–	Net bank disbursements
=	*Cash expenditures*

TOTAL OUTLAY OF FUNDS

The total outlay of funds includes all payments made by cash or check. There is no need to determine which part was paid by cash and which part by check. Total outlays include, but are not limited to:

- Purchase of capital assets to investments (determined from settlement sheets, invoices, statements, and the like)
- Loan repayments (determined from loan ledgers of banks or other creditors)
- Living expenses (can be determined from the same sources presented in the net worth and expenditures sections)
- Purchases, business expenses (less noncash items, such as depreciation), rental expenses, and the like

NET BANK DISBURSEMENTS

The net bank disbursements can be determined using the following formula:

	Net deposits to all accounts
+	Beginning balances
=	*Net bank funds available*
–	Ending balances
=	*Net banking disbursements*

Funds from Known Sources

Once the total receipts from all sources is determined, calculate the funds from unknown sources by subtracting the funds from known sources from the total receipts (of income) from all sources.

Funds from known sources include, but are not limited to, salaries, business profits, insurance proceeds, gifts received, loans, and inheritances. Funds from known sources are subtracted from total receipts (or income) to arrive at funds from unknown or illegal sources.

Rebutting Defenses to Indirect Methods of Proof

If a party uses an indirect method to prove the defendant's illicit assets circumstantially, the defendant will try to rebut such evidence. Often, the defendant will claim that the excess income came from legitimate sources. The defendant might claim that the funds are cash that he accumulated earlier or cash from other legitimate sources, such as loans or gifts from relatives.

To counter such defenses, the fraud examiner must specify the amount of cash the defendant had on hand at the beginning of the relevant period and do the following:

- Develop a financial history of the subject and subject's spouse, showing the dates and places of their employment, their salary and bonuses, and the sources of any other legitimate income.
- Establish that the defendant did not have a cash hoard by showing that he borrowed money, made installment purchases, incurred large debts, was delinquent on his accounts, had a poor credit rating, or filed for bankruptcy.
- Establish that the funds did not come from private loans from family or friends by showing that the alleged lender was incapable of generating the amounts supposedly lent,

that there is no documentation reflecting the source of the alleged loan (i.e., no bank account withdrawals), and that there was an absence of funds available to the alleged lender.

Indirect methods of proof are significant tools in documenting ill-gotten gains. With this as a basis, the following section covers the major schemes used to commit fraud against companies and governmental agencies.

Locating Hidden Assets

Fraudsters tend to hide their illicit assets. To review, an *asset* is anything of material value or usefulness that a person or organization owns. Thus, everything a person owns is potentially an asset.

Although any type of asset can be hidden, fraudsters tend to hide *liquid assets* (assets that can be purchased and sold quickly) more frequently than *illiquid assets* (assets not easily converted into cash). Nevertheless, illiquid assets, such as real property, vehicles, boats, and planes, can be hidden by transferring ownership and title to another person or entity.

And generally, asset hiders look to conceal their assets with financial vehicles that have certain characteristics. For one thing, asset hiders want products that are difficult to trace or untraceable. With such instruments, asset hiders can break or obscure links between the initial receipt of the assets and their final disposition. For another thing, asset hiders want products that are secure and accessible. Assets hiders also want products that are liquid.

Why People Hide Assets

People hide assets for a variety of reasons, such as to:

- Fraudulently reduce the holdings of a marital estate in divorce proceedings.
- Keep them away from creditors or remove them from bankruptcy.
- Misrepresent the assets of their company.
- Avoid having to pay a civil judgment.
- Evade taxes.
- Conceal their connection to a criminal act and to disguise illicit assets as legitimate.

Common Ways to Hide Assets

Fraudsters can use many techniques to hide ill-gotten gains, but some common ways individuals hide assets include:

- Hoarding assets
- Hiding assets in someone else's name (e.g., the name of a spouse, other relative, friend, business partner)
- Depositing funds into financial institutions
- Converting cash into negotiable instruments (e.g., traveler's checks, savings bonds, cashier's checks)
- Overpaying taxes
- Purchasing real estate
- Using assets to pay down debt (e.g., mortgages, credit card balances)
- Purchasing assets and collectibles, such as art and antiques
- Transferring assets into tax havens
- Transferring assets into secrecy jurisdictions
- Transferring assets into trusts
- Using assets to purchase insurance products
- Investing assets
- Hiding assets in businesses
- Purchasing prepaid access cards

Hoarding Assets

Hoarding is the most basic way to hide assets and occurs when a person stores assets in a hidden location, usually in his home or on his property. This is the proverbial "cash under the mattress" technique.

There are many places to hide assets in a typical home. For example, an individual can hide precious metals and jewelry in a layer of cooking grease at the bottom of a pot. Also, an individual can hide assets in the space beneath the bottom drawer of bureaus, chests, and cabinets. Loose bricks in a wall or fireplace can disguise small spaces for hiding things, and assets can be hidden in furniture.

Additionally, the structure of a home itself provides options for hiding assets. Assets can be hidden in walls and beams. Cunning hiders might construct false walls in closets or pantries, or they might dig a cavity into a wall and then cover it with a mirror or painting.

Moreover, asset hiders often hide currency and other valuables in locations outside their homes. For instance, they might place their assets in bank *safe deposit boxes*, which are private vault spaces rented by banks to customers. Banks keep no record of the contents of safe deposit boxes, and they rarely know what the boxes contain. Often, to better conceal assets, individuals place assets in safe deposit boxes that are held in someone else's name.

Hiding Assets in Someone Else's Name

Another method used to hide ill-gotten gains is to transfer them into another person's name by gift, loan, or other means. By creating the illusion that the assets are in someone else's possession, these techniques serve to protect the assets from taxes, seizure, and creditors. They are designed to leave little or nothing in the debtor's name so that he becomes essentially judgment proof (i.e., lack sufficient funds to satisfy a legal judgment).

When an individual gives assets to relatives or friends as gifts, the gifts might be exempt from creditors or court judgments. If, however, an individual transfers his assets to evade a creditor's efforts to collect against the asset, the transfer is fraudulent and voidable. A *fraudulent transfer* is a transfer that a debtor makes to try to defeat a creditor's efforts to collect against the asset.

Also, asset hiders might use loans—fraudulent or otherwise—to conceal their assets. Often, hiders make fraudulent loans to friends, relatives, or other close associates to create the appearance that the assets have been disbursed and are no longer in the loaner's possession, even though no money ever changes hands.

Deposits to Financial Institutions

Often, fraudsters deposit their illegal proceeds into accounts in financial institutions. Banks and other depository institutions are susceptible to individuals attempting to hide illicit funds because they are the primary gateway to the financial system, and once funds are placed in a depository institution, the proceeds can be concealed by commingling them with legitimate funds or transferring them to different accounts.

To conceal their illegal proceeds, fraudsters might deposit funds into accounts in financial institutions and then use wire transfers to move the funds between different accounts and break the audit trail. Wire transfers are used to move money from one account to another. Many fraudsters use wire transfers to transmit their illegal proceeds to offshore accounts.

EXAMPLE

Simon instructs his bank, Brinkley Bank, to transfer $10,000 of his funds to his business associate, Wilson. Brinkley Bank debits Simon's account $10,000 and credits its own account with $10,000. Brinkley Bank then sends an instruction—known as a payment order—to Wilson's bank, Grand Union Bank. Because Brinkley Bank and Grand Union Bank are corresponding banks, the payment order tells Grand Union Bank to debit the Brinkley Bank's correspondent account by $10,000 and place the money in Wilson's account.

Depository institutions are required to take measures to prevent efforts to conceal unlawful assets. Generally, depository institutions must attempt to confirm the identity of customers, report suspicious activity, and meet various other requirements. Despite such requirements, there are many schemes by which asset hiders attempt to escape detection, including:

- Structuring transactions to evade currency reporting requirements by breaking down a large transaction into a number of smaller ones (i.e., smurfing or structuring)
- Using temporary bank accounts
- Colluding with employees of depository institutions

Negotiable Instruments

Cashier's checks, traveler's checks, and other *negotiable instruments*—written orders promising to pay a fixed sum of money—can also be used to hide assets. These instruments are useful to asset hiders for several reasons, including:

- They disguise an individual's financial dealings.
- They reduce the amount of currency to be carried.
- They can be exchanged almost anywhere in the world.

Tax Overpayment

Some individuals choose to overpay their taxes, and by doing so, a perpetrator causes his money to be safely held by the agency responsible for tax collection (e.g., the Internal Revenue Service in the United States) until it is refunded at the end of the year.

To identify advance payments, look for payments to tax collection agencies that are larger than they should be.

Real Estate

Often, individuals conceal their assets by purchasing real estate, although real estate investments leave an audit trail. An asset hider might try to conceal such investments by making them in his spouse's maiden name, in the name of other family members, or in corporate names.

Asset hiders often invest in real estate in different jurisdictions because real estate investments can be made almost anywhere, making it difficult to locate real estate holdings in different jurisdictions.

Moreover, the real estate industry offers a vast array of financial transactions that often involve multiple parties (e.g., brokers, agents, and appraisers), which can obscure the source of funds and the identity of the true owner. Although real estate is less liquid than many assets, it can generate additional profits, especially in vibrant or rebounding markets.

Pay Down Debt

Often, fraudsters use illicit funds to pay the interest or repay the principal on their debt (e.g., mortgage loans, credit card debts, or personal loans).

Frequently, asset hiders use illicit funds to pay the interest or repay the principal on mortgage loans, converting the illicit income into seemingly legitimate profits when the property is sold.

Paying down mortgage loans is attractive to asset hiders because mortgage payments raise less suspicion than other types of transfers (e.g., wire transfers or offshore transfers), but mortgage payments are easily traced. Often, when a subject uses illicit gains to pay down his mortgage, a fraud examiner can document the subject's mortgage payments to show that the subject has undisclosed or hidden income from other sources.

Other Assets and Collectibles

Individuals also might use their illicit funds to purchase other assets or collectibles, to pay for vices, or to fund a lavish lifestyle.

Tax Havens

People commonly hide their assets offshore in *tax havens*—countries that offer favorable tax treatment to investments. Tax havens can be legal or illegal, depending on the nationality

and the residence of the individual and the tax code of the country where the activity takes place.

Secrecy Jurisdictions

Some people hide their assets offshore in secrecy jurisdictions, which are countries that have laws that afford financial secrecy. Such jurisdictions may provide financial secrecy through domestic bank secrecy laws that bar insight by outsiders or through blocking statutes that prevent the disclosure, copying, inspection, or removal of documents located in the host country. Moreover, many secrecy jurisdictions prohibit legal depositions in connection with judicial proceedings being undertaken abroad.

Trusts

Another method of hiding assets is to transfer them into trusts. A *trust* is a fiduciary relationship in which a person (the trustee) manages property for the benefit of another (the beneficiary).

A trust requires a settlor, a trustee, beneficiaries, and a trust agreement. The *settlor* is the person creating the trust. The *trustee* or *trustees* are responsible for administering and carrying out the terms of the trust. The *beneficiaries* are those who are entitled to trust income or principal either at the current time or in the future. The *trust agreement* is the written agreement between the settlor and the trustee, and it provides that the settlor will transfer certain assets to the trustee and the trustee will hold those assets in trust and administer them to the named beneficiaries.

Trusts offer several benefits that appeal to asset hiders. They can be used to minimize or defer taxes, and they can ensure the smooth transfer of assets from generation to generation. Also, trusts can be designed to limit the interests of beneficiaries in a way that precludes creditors from collecting against the assets; a creditor's ability to access a trust is limited to the beneficiary's interest in the trust.

There are many types of trusts, but often, asset hiders transfer their property into foreign trusts (asset protection trusts). A *foreign trust* is a trust formed under the laws of a foreign jurisdiction and controlled by foreign trustees without a local business presence. A number of jurisdictions (e.g., Cook Islands, Liechtenstein, the Isle of Man, and Gibraltar) have enacted laws to make their jurisdictions more attractive to settlors.

Assets transferred to foreign trusts generally are liquid (e.g., bank accounts or brokerage accounts), but they can include intellectual property and interests in legal entities. Moreover, assets transferred to foreign trusts can be located anywhere in the world.

Asset hiders use foreign trusts for three primary reasons. First, by putting their assets in foreign trusts, they place their assets beyond the reach of local courts. Second, they can place their assets in foreign trusts located in favorable foreign jurisdictions that have relatively short statutes of limitations on fraudulent transfers. Third, the majority of plaintiffs and creditors do not pursue assets contained in foreign trusts because such structures make assets too difficult or expensive to reach.

Foreign trusts, however, are not immune from attack. If, for example, the settlor retains control over the appointment of the foreign trustee, a court may force either of these parties to dissolve the trust. Thus, foreign trusts are most effective for fraudsters when the settlor relinquishes all control over the foreign trust and the foreign trustee.

Insurance Products

Due to the recent growth in the financial products offered by insurance agents and brokers (including savings products, investment products, and tax-planning services), the insurance industry has become increasingly attractive to asset hiders. This is because many insurance products contain features that make them vulnerable to exploitation by those who need to hide illegal funds.

Asset hiding in the insurance industry primarily involves life insurance policies (typically, those with a cash surrender value or investment features). For example, someone purchases single-premium insurance bonds with illegal cash and then redeems the bonds at a discount. That is, dirty money is used to buy an insurance policy, and when the perpetrator cashes out, he receives a clean check from the insurer.

Some life insurance policies can be purchased with a single down payment.

Under the terms of a whole life or universal life insurance policy, a borrower might make additional payments on the policy. These payments accrue at a high rate of interest and enhance the overall value of the insurance policy. A sophisticated hider might deposit substantial funds into an existing insurance policy thinking that an investigator will not look beyond the face value of the policy.

Furthermore, individuals can over-fund policies with illegal money and then receive clean disbursement checks from the insurer upon withdrawal. There is generally an early withdrawal penalty associated with this type of transaction, but compared to the benefit of being able to hide illegal funds, it is usually considered an acceptable cost.

Also, asset hiders can use illicit funds to purchase life insurance policies or other redeemable insurance contracts. Often, such transactions are *viatical*—pertaining to the purchase of insurance policies from terminally ill policyholders. In a *viatical settlement*, a terminally ill insured sells the death benefit of his insurance policy at a discount to a third party. In this type of settlement, the owner of the insurance policy receives cash, and the buyer becomes the new owner, or beneficiary, of the life insurance policy. A *viatical investment* is an investment in which the investor purchases an interest in the death benefit of a life insurance policy.

Investments

Many asset hiders invest their illegal proceeds in securities, real estate, insurance products, or some other type of investment. *Investments* refer to any use of capital with an expected return.

Businesses

An asset hider might choose to use a business to hide cash and other assets.

Individuals can use various bookkeeping schemes to conceal funds by filtering them through a legitimate business, otherwise known as a *front business*. Front companies are legitimate organizations that engage in legal commercial activity, but their funds are commingled with illegal money disguised as revenue.

Closely held businesses such as restaurants, retail stores, medical offices, construction companies, car dealerships, and law practices are prone to abuse. Most closely held businesses have finances that their owners can easily manipulate, which makes it easy to process illegal funds.

In addition, an asset hider might transfer his assets into certain types of corporate business structures to shield them from creditors and disguise the source of the funds.

COMMON BUSINESS ENTITIES USED TO PROTECT ASSETS

Often, to protect their assets, fraudsters place them in various types of business structures to shield them from creditors and disguise the source of the funds, including:

- Limited partnerships and international variations
- Corporations
- Limited liability companies (LLCs) and international equivalents

LIMITED PARTNERSHIPS

Limited partnerships are easy and inexpensive to set up. Generally, assets tied up in a limited partnership are difficult to reach because the assets are not owned by the individual partners and the liability of a limited partner is restricted to the amount of his investment.

Numerous countries have variations on limited partnerships, but the laws differ in scope and application.

In some countries (e.g., New Zealand and the United States), a limited partnership comprises two types of partners: general partners and limited partners. General partners have management responsibility for the partnership, can incur obligations on behalf of the partnership, and have unlimited liability for the partnership's activities. A limited partner's liability, however, is restricted to the amount of his investment.

Also, in such countries, creditors cannot directly reach the limited partner's assets. Instead, they must obtain a charging order, which gives the creditor the right to receive any distributions made to the limited partner. The creditor cannot force the partnership to make distributions to that partner.

Other countries that have variations on limited partnerships include:

- *United Kingdom*: In the United Kingdom, limited partnerships are governed by the Limited Partnerships Act 1907.
- *Japan*: Historically, Japanese law has provided for two business forms similar to limited partnerships: goshi gaisha and tokumei kumiai. The *goshi gaisha* is structured like limited partnerships. In these structures, the limited partners do not share in management and are liable only to the amount of their contributions. The general partners have management responsibility and unlimited liability. The *tokumei kumiai* is a silent

partnership in which a silent partner(s) contributes funds for the partnership's operation and operating partners manage the partnership.

- *New Zealand*: In New Zealand, limited partnerships involve general partners and limited partners.

CORPORATIONS

A *corporation* is defined as a body of persons granted a charter legally recognizing them as a separate entity having its own rights, privileges, and liabilities distinct from those of its members. Therefore, a corporation's shareholders, directors, and officers generally are not personally liable for a corporation's debts and liabilities.

Asset hiders exploit this liability protection by transferring their assets into a corporate entity. In the event that the asset hider is sued by a creditor, his assets are shielded because they are legally owned by the corporation, not the asset hider himself; therefore, they are out of the reach of any judgment or court order directed against the asset hider as an individual.

LIMITED LIABILITY COMPANIES

A *limited liability company* (LLC) and its international equivalents is a non-corporate business that provides its owners (members) with limited liability and allows them to participate in the entity's management. LLCs generally shield members from the company's debts, obligations, and liabilities.

Much like corporations, LLCs are separate legal entities, but LLCs can be administered and maintained without the rigid requirements applied to corporations. LLC members are essentially free to manage the company and divide the profits in any manner, and this aspect of administrative freedom can be of great benefit to the asset hider.

LLCs also have advantages over limited partnerships. Limited partnerships, for all their protections, still expose each partner to a degree of personal liability. An LLC, in contrast, provides its members with complete protection from all liabilities associated with the company. Theoretically, none of the members are personally responsible for any debts or claims against the LLC.

PIERCING (OR LIFTING) THE CORPORATE VEIL

Although limited partners, LLC members, and shareholders of corporations are generally free from personal liability for their entities' obligations, there are exceptions to this rule. A party may be able to access an owner's assets by piercing the veil of the corporate entity.

Under the doctrine of *piercing the veil of a corporate entity*, the separate personality of a corporation may be disregarded if it is used for fraudulent or illegal purposes or to escape the faithful compliance of an obligation. Although the doctrine was originally created as a way to pierce the special protection afforded to corporate shareholders, it has been adapted and applied to pierce the veil of LLCs and impose liability on their members.

To pierce the corporate veil, the party bringing the action must convince the court that the corporation is not a truly separate entity; it is just a shell that has been established to control the private assets, debts, and interests of its owners. If the court determines that the corporation is a sham and has no true, separate existence from the wrongdoer, the court is justified in ruling that the corporation and the wrongdoer should be considered as one and the same "person" for purposes of determining liability to satisfy a judgment.

Prepaid Access Cards

Often, fraudsters purchase prepaid access cards with their illicit assets in an effort to hide their assets from creditors. Again, prepaid access cards are similar to debit and credit cards, but unlike debit and credit cards, prepaid cards do not require a checking or savings account or an extension of credit. They can be used anywhere credit and debit cards are accepted.

There are various types of prepaid access cards, including:

- Gift or debit cards
- Credit cards, which can also be found in cash management accounts (CMAs) offered by stock brokerage firms
- Insurance premiums
- Mobile phone accounts

Methods to Obtain Information for Locating Assets

This discussion looks at some common methods fraud examiners can use to obtain information that can be helpful in fraud examinations. Some possible methods include:

- Using commercial database vendors and investigative service providers
- Performing surveillance

- Conducting interviews
- Searching digital media
- Using online sources
- Using legal processes

Commercial Database Vendors and Investigative Service Providers

There are many commercial database providers and investigative service providers that offer various services and tools that fraud examiners can use to find hidden assets.

Surveillance

Surveillance—the covert observation of targets for information-gathering purposes—can be used to locate residences, businesses, or other places of interest to the investigation, and it can be used to produce important evidence concerning the scope and nature of a person's activities.

Interviews

Asset examinations should involve *interviews*—question-and-answer sessions designed to elicit information—of those who might have relevant information concerning the matters at issue. Typical interviewees in asset investigations include the target; any complainants; business associates, ex-spouses, friends, relatives, neighbors, employees, or other associates of the target; business rivals; employees of financial institutions; people who have a stake in an asset at issue; and other individuals who have been in contact with the target.

When seeking information about unknown assets, a fraud examiner should determine how the subject is hiding assets, and he should ask interviewees for records or documents that might identify, trace, and locate assets.

Digital Media

Today, information is typically created, stored, and disseminated electronically. Consequently, fraud examiners must understand that electronic devices might contain information about hidden assets, such as bank account numbers, the names of nominees, location of accounts, the existence of shell companies, and so on.

Online Sources

When searching for information, fraud examiners should use online sources. Online sources include commercial databases, websites, social networking sites, and any other sites available

online. Such sources offer a quick, easy, and cost effective way to gather information. For more information, see the "Sources of Information" chapter.

Legal Processes

If a legal action has been filed, information relevant to a search for hidden assets may be obtained by using some legal process, such as depositions, interrogations, and document requests.

In a civil case, nonpublic information such as bank account records, brokerage account records, travel records, credit card records, records held by credit agencies, and telephone records may be obtained by a subpoena or its equivalent. A *subpoena* is a legal order to produce documents, witnesses, or other things.

Law enforcement agencies may also subpoena records, of course, but usually, law enforcement will not disclose the contents of such records with the victim or third parties.

Some administrative agencies can access records through administrative subpoenas or interrogatories, and some agencies working overseas are able to access overseas records through written or verbal requests of bank officials. But, accessing records in countries with strict bank secrecy laws can be very difficult.

Locating Assets Stored Abroad

Often, international barriers hinder asset investigations. A fraudster can move his ill-gotten gains across borders, complicating the task of identifying the proceeds of crime.

This discussion provides guidance for fraud examiners seeking to find assets stored abroad by covering the following topics:

- Common challenges fraud examiners face when investigating abroad
- Legal avenues available for locating assets abroad in criminal investigations
- Legal avenues available for locating assets abroad in civil investigations
- Approach for finding assets located abroad

Challenges in Locating Assets Abroad

An investigation of assets stored abroad can be challenging due to obstacles in varying laws, language barriers, culture differences, and other things. Common challenges fraud examiners encounter when trying to find assets abroad include:

- Countries lack the resources or capacity
- Political influence and power of corrupt officials
- Financial secrecy through domestic bank secrecy laws that bar insight by outsiders or through blocking statutes that prevent the disclosure, copying, inspection, or removal of documents
- Language differences and communication barriers
- Differences in legal systems across jurisdictions where the crime occurs and where the funds are stored
- Different privacy standards and rules concerning the transmission of personal data to outside countries

Legal Avenues Available in Asset Investigations

In addition to Internet sources, commercial databases, and public records, there are numerous legal mechanisms available for finding and seizing assets stored abroad. The tools available to government investigators in criminal investigations, however, vary from those available to private parties in civil matters.

Common legal avenues for finding and seizing assets located abroad include:

- Discovery (or disclosure) in civil proceedings
- No-say orders
- Deposition by stipulation, notice, or commission
- Mutual legal assistance
- Letters rogatory
- Information exchanges under tax conventions

DISCOVERY (OR DISCLOSURE) IN CIVIL PROCEEDINGS

In civil proceedings, the parties generally are entitled to *discovery*, which refers to the formal process whereby the parties to litigation collect evidence and learn the details of the opposing side's case.

Also, during discovery, the parties can obtain documents from third parties by court order, including third parties located abroad.

NO-SAY ORDERS

If a plaintiff in a civil case seeks an order for disclosure by a third party, the court may impose a no-say or gag order to prevent the third party from informing the defendant that a disclosure order exists.

DEPOSITION BY STIPULATION, NOTICE, OR COMMISSION

Deposition by stipulation, notice, or commission are the three procedures by which a U.S. litigant can obtain a deposition of a foreign witness without assistance from foreign authorities. But to use these procedures, the witness must submit to the deposition voluntarily, and there can be no foreign laws that prohibit the deposition.

MUTUAL LEGAL ASSISTANCE

Mutual legal assistance (MLA) is a process by which countries request and provide assistance in law enforcement matters, such as gathering information, obtaining provisional remedies, and enforcing foreign orders and judgments. In most jurisdictions, however, MLA is available only in criminal investigations. Private parties do not have access to MLA.

Multilateral conventions, treaties, and agreements contain binding provisions in which countries agree to assist one another in criminal law enforcement matters. To obtain assistance from a foreign government, the government seeking assistance makes an MLA request. An *MLA request* is a written request to the government of a foreign country that is used to obtain assistance in law enforcement matters.

Generally, MLA can be used to obtain assistance in matters such as conducting searches, gathering evidence, compelling sworn testimony and the production of documents, issuing search warrants, issuing subpoenas, serving process, exchanging affidavits, obtaining provisional remedies, and providing assistance in forfeiture proceedings.

A government may request a wide variety of information when it makes an MLA request, including information on bank accounts and bank account documents.

Many countries that are bound to multilateral conventions, treaties, or agreements have a central MLA authority through which MLA requests are made. For example, in the United States, MLA requests are made through the U.S. Department of Justice, Office of International Affairs (OIA). Similarly, in the United Kingdom, the Home Office deals with most MLA requests in England, Wales, and Northern Ireland. In Australia, the International

Crime Cooperation Central Authority is responsible for mutual assistance. In certain circumstances, these MLA authorities can offer assistance to fraud examiners seeking to recover assets stored abroad.

MLA offers the following advantages:

- Available at the investigation stage
- Might not require dual criminality
- Allow for a wide range of assistance

A foreign jurisdiction, however, may refuse assistance. An MLA request may be refused for any of the following reasons:

- Request is for property that is of a *de minimis* value (i.e., so minor as to merit disregard)
- Assistance would prejudice the jurisdiction's essential interests (e.g., sovereignty, public order, security, and burden on resources)
- Assistance requested when there is no reasonable prospect of conviction
- Request involves a party that has already been convicted or acquitted of the same crime
- Request involves a party that is involved in ongoing proceedings or investigations involving the same conduct
- Target has immunity from prosecution

Many of the tools that can be used to trace assets stored abroad will require an MLA request, including:

- *Account monitoring orders*: Account monitoring orders, which might be available in criminal investigations, are ex parte orders (i.e., orders based on one party's request without hearing from the other side) by a court or, in some jurisdictions, the investigating magistrate that allow investigators to conduct real-time financial surveillance and require specified financial institutions to provide account information for the identified accounts.
- *Search warrants*: In criminal investigations, law enforcement officials of one country may request that the courts of a foreign country issue a *search warrant*—a court order that grants authorities the right to search a premises or property for information pertinent to the case—authorizing them to search for and obtain evidence from otherwise protected places, persons, and institutions.
- *Production orders*: A production order is a court order requiring that a specified person produce the evidence specified in the order. Production orders generally are used to

obtain nonpublic information, including information held by banks, accounting firms, law firms, insurance companies, email service companies, Internet service providers, and so on.

- *Forfeiture orders*: A forfeiture order (or a confiscation order) is a court order authorizing a specified official to confiscate specified property obtained in connection to criminal activity.

LETTERS ROGATORY

If an MLA is not available, government officials may be authorized to make a formal government-to-government request for assistance, or letters rogatory, to obtain foreign evidence. These are the customary method that courts use to request assistance from their counterparts abroad in the absence of a treaty. That is, *letters rogatory* are formal requests that a court in one country makes to seek judicial assistance from a court in another country. Letters rogatory also permit formal communication among the judiciary, a prosecutor, or a law enforcement official of one country and their counterpart in another country.

The most common types of assistance sought by letters rogatory are service of process and taking of evidence.

Some countries, such as Australia, do not distinguish between MLA requests and letters rogatory.

Letters rogatory can be used in civil and criminal matters. In civil proceedings, letters rogatory can be issued only after a case has been initiated through the filing of a complaint, but in criminal proceedings, letters rogatory can be issued in support of a criminal investigation before charges are filed.

Typically, letters rogatory are handled through each country's respective ministry of justice (i.e., the agency charged with justice). In the United States, for example, letters are made through the U.S. Department of Justice, Office of International Affairs (OIA). In Canada, requests are submitted through the International Assistance Group at the Department of Justice.

Requests for foreign assistance under letters rogatory are usually slower and less efficient than MLA requests.

TAX INFORMATION EXCHANGE AGREEMENTS

In a tax information exchange agreement, two governments seek to prevent tax evasion by establishing an official system to provide for the exchange of information in tax matters between their respective tax authorities.

Generally, this avenue is available only to government investigators.

Approach to Finding Assets Stored Abroad

When searching for assets located abroad, the fraud examiner should take the following steps:

- Identify all jurisdictions where the subject's assets might be located.
- Establish contact with foreign counterparts and seek cooperation.
- Research the laws applicable to the foreign jurisdictions.
- Investigate by identifying and locating the proceeds of crime and collecting evidence of ownership.

IDENTIFY ALL JURISDICTIONS WHERE THE SUBJECT'S ASSETS MIGHT BE LOCATED

First, the fraud examiner should identify where the subject might have stored his assets, not only to secure assets that might become subject to a judgment, but also to assess potential obstacles that might arise in each foreign jurisdiction.

ESTABLISH CONTACT WITH FOREIGN COUNTERPARTS AND SEEK COOPERATION

Early on, contact foreign counterparts for help identifying and assessing potential issues, developing a strategy, gathering information, obtaining informal assistance, and creating goodwill. Establishing contact early gives the foreign jurisdiction an opportunity to prepare for its role in the investigation.

RESEARCH THE LAWS APPLICABLE TO THE FOREIGN JURISDICTIONS

Research and analyze the laws that apply to the jurisdictions where the subject might have stored his assets and examine how the laws might affect recovery. Among other things, the fraud examiner should determine whether the local laws he plans to use can be applied extraterritorially, and he should also identify and analyze the foreign laws that might affect the investigation (e.g., discovery restrictions, data privacy laws, human rights legislation).

INVESTIGATE

The investigative phase involves identifying and locating the proceeds of crime and collecting evidence of ownership. This phase involves the typical steps involved in an asset investigation, which were previously discussed.

REPORT WRITING

The Importance of Writing Effective Reports

Writing effective reports is a critical skill for fraud examiners. A thorough investigation or keen analysis will often do little good if the fraud examiner cannot convey the information in a written format. Fraud examiners typically must be very flexible in their writing technique, because reports should generally be tailored to the situation, as well as to the needs of the party requesting the report. Even so, many aspects of good writing—such as accuracy, relevancy, and clarity—are universal to all reports.

Types of Reports

The two most common types of reports fraud examiners are engaged to create are fraud examination reports and expert reports.

Fraud Examination Reports

A *fraud examination report* documents the results of a fraud examination and is generally created by one or more critical members of the fraud examination team. Documenting results is a particularly important function in fraud examinations. The fraud examination report conveys all evidence necessary to evaluate the case, and it can be used to corroborate previously known facts. An accurate report will add credibility to the fraud examination and to the fraud examiner's work. Additionally, requiring a written report will force the fraud examiner to consider his actions during an investigation by requiring that he documents his process. And a well-written report will omit irrelevant information, thereby allowing pertinent facts to stand out. A first-rate fraud examination report is based on a first-rate fraud examination.

Expert Reports

Many fraud cases benefit from the assistance of an expert witness, who (unlike most witnesses) may provide technical opinions through his testimony. Typically, fraud examiners who serve as expert witnesses in litigation are tasked with providing an *expert report*, which requires them to provide particular information about their qualifications, their opinions, the bases of those opinions, and various other pieces of information. The purpose of an expert report is to inform the parties, the judge, and the jury (if applicable) about the expert's opinion of the case, as well as his credibility for commenting on such issues.

The content of the expert report is highly dependent on the needs of the situation. For example, the expert witness might provide an expert opinion on an organization's auditing practices. If the expert used a fraud examination report as part of the basis of forming the opinion, the fraud examination report would likely need to be attached to the expert report. However, each report in this scenario is a separate document with its own structure. In some situations, the person who wrote the fraud examination report might also be called as an expert witness, so it is important to keep in mind the different purposes of each report.

The Judicial Proceeding Standard

A guiding principle for writing reports is: "Would I be able to defend this report in a judicial proceeding?" Most fraud cases will not be presented in such proceedings, but the purpose of the report is to give an objective and reliable account and analysis of the facts of a case. A court or administrative hearing is the ultimate test of a report, because the judge or the opposing parties will thoroughly scrutinize it. Therefore, even when litigation is unlikely, producing a written report that can withstand scrutiny in a judicial proceeding is the ideal goal. Fraud examiners should always know what reliable evidence is available to back up each statement expressed in the report and make sure that case analysis is of professional quality.

Preparation

Fraud examiners must properly plan their written reports. Proper preparation entails analyzing what is to be expected as an end product. It should also involve having a good idea of what is to be learned from each witness.

Active listening is an essential function of effective report writing. The fraud examiner must have good listening skills so that the information is properly assimilated, evaluated, and communicated to others. Listening skills are learned. Listening involves perceiving what the respondent is actually communicating. To listen properly, the fraud examiner must set aside any preconceived notions and listen objectively, not only to what is being said, but to how it is said and why. The fraud examiner should withhold judgment until he has heard the entire message.

Active listening often involves participating with the respondent during the information-gathering process. Participation conveys interest in the subject and promotes rapport.

Participation might require reacting openly to information communicated by verbal and nonverbal responses.

Additionally, during the planning phase of an engagement, the fraud examiner should discuss the anticipated scope of the engagement with the retaining party. The fraud examiner should identify the likely areas that will be addressed in the report based upon that scope and the requirements of the ACFE Code of Professional Ethics, including that "a Certified Fraud Examiner shall reveal all material matters discovered during the course of an examination, which, if omitted could cause a distortion of the facts." Based upon that paradigm, the fraud examiner should develop an understanding of the documentation and other evidence that typically would be available within the scope and purpose of the engagement.

After developing the initial engagement plan, the fraud examiner should prepare an estimated cost for the expected preliminary tasks. Obtaining the retaining parties' approval of the cost and overall procedures to be performed is an important step toward establishing an agreement about the areas to be addressed and the expectations of the parties.

While the fraud examiner can established an initial work plan based on the expected engagement scope and purpose, no conclusions or opinions should be released until he has:

- Accumulated sufficient evidence to meet the preponderance of the evidence burden of proof (or established that doing so is not feasible)
- Thoroughly addressed, analyzed, and documented that all probable alternative explanations have been considered and excluded as likely explanations that would affect his conclusions or opinions
- Accumulated sufficient evidence to identify all material matters which, if omitted, could cause a distortion of the facts

Characteristics of a Good Report

A well-written report contains the following four characteristics:

- Accuracy
- Clarity
- Impartiality and relevance
- Timeliness

Accuracy

Written reports must be accurate. Inaccuracies will affect the credibility of the report and the report's author. Each contact a fraud examiner makes during the course of a fraud examination should be recorded on a timely basis in a separate memorandum that documents the details of the interview. Ordinarily, there is no need to recapitulate testimony word for word, but the fraud examiner should include all facts of possible relevance for accuracy's sake. Sometimes, a verbatim quote regarding a witness's keywords is critical. For example, a suspect might accurately use a technical word or phrase that implies knowledge of the relevant subject.

Fraud examiners should reconfirm dates and supporting information with the respondent. It is important to reconfirm the facts *before* the report is written, not after. Attachments to the report, if any, should be completely described. Inaccuracies and careless errors are inexcusable; they can harm the report's credibility and potentially render it useless.

Clarity

Reports must also show clarity. Investigative reports on fraud examinations should convey pertinent information in the clearest possible language. If necessary, quote the respondent directly (provided the quotation does not distort the context). Only convey objective facts (i.e., unbiased evidence that is not influenced by personal feelings, interpretations, or prejudice); do not editorialize or opine on guilt or innocence. The goal of the fraud examiner's written report and sworn testimony is to help the trier of fact to understand the evidence or to determine the fact at issue. Failure to meet this threshold might prevent the report or the sworn testimony from being admitted as evidence at trial. Also, try to avoid using jargon because the report might be read by people who are not familiar with esoteric or technical terminology. Use complex or technical terms in their proper contexts, and, where necessary, explain their meaning.

Impartiality and Relevance

Additionally, a written report must be impartial and relevant. Fraud examiners should report all relevant facts without bias, regardless of which side a particular fact favors or what it proves or disproves. In litigation, the judge rules on the relevance, in whole or in part, of a fraud examiner's written report and testimony. Sections deemed not relevant will not be allowed into evidence.

Also, at the outset of a fraud examination, the fraud examiner should carefully determine what information will be needed to prove or disprove the case and attempt to include only this information. A report should include only those matters that are relevant to the examination. Fraud examiners should use their professional judgment to determine whether something is likely relevant. However, because almost every investigation yields much information of which the relevance is not immediately known, in such cases it is best to opt for completeness.

In the context of expert reports, the purpose of such reports is not to "win" cases. The fraud examiner's job in this capacity is to objectively assist the trier of fact by offering reliable and relevant expert conclusions and opinions (regardless of the consequences to any party in the matter) backed up by a thorough and supportive basis. The fraud examiner may be an advocate for the credibility and reliability of his expert conclusions and opinions and the related supportive basis in reporting or testifying; however, he must not become, or even appear to become, an advocate for one party or the other.

The relevance of an expert report depends on whether it is helpful to the trier of fact. If a layperson, such as a jury member, can perform the same procedures, such as simple calculations or a simple reiteration of the background of the facts of the case, then the expert's specialized knowledge was not required in those portions of the report. The judge may rule that those portions of the expert report are not relevant and, therefore, not admissible.

Timeliness

Written reports must be timely. The timeliness of reports is extremely important because it tends to enhance the accuracy of witness testimony, as well as preserve the fraud examiner's memory of the interview(s). Thus, all interviews should be documented in a memorandum of interview as soon as possible after the questioning—preferably on the same day of the interview.

In short, the fraud examiner should, upon completing the examination, prepare a final or interim report (whichever is appropriate) as soon as possible.

Common Reporting Mistakes

This discussion examines some common mistakes fraud examiners make when preparing a written report.

Conclusions and Opinions

Fraud examiners must be cautious about providing conclusions and stating their opinions. In a report-writing context, conclusions and opinions are similar, but not identical. *Conclusions* are based on observations of the evidence, whereas *opinions* call for an interpretation of the facts.

Conclusions

The fraud examiner must be very circumspect about drawing conclusions. In most situations, the conclusions from the examination should be self-evident and should not need to be pointed out in the report. If the conclusions are not obvious, the report might need to be clarified. The fraud examiner's job is to obtain sufficient relevant and reliable evidence to determine the facts with a reasonable degree of forensic certainty. Assuming facts without obtaining sufficient relevant and reliable evidence is generally inappropriate. In the case of expert reports, whether the witness has adequately accounted for alternative explanations demonstrates whether he has employed the same level of intellectual rigor that characterizes the practice of an expert in the relevant field.

Opinions

The fraud examiner must also avoid stating opinions regarding the guilt or innocence of any person or party involved. The ACFE Code of Professional Ethics specifically prohibits statements of opinions regarding guilt or innocence, as this is the job of the judge or jury (see the Fraud Prevention and Deterrence section of the *Fraud Examiners Manual*).

Similarly, the fraud examiner should be careful not to include any statement of opinion as to the integrity or veracity of any witness even if the fraud examiner is convinced that the witness is being untruthful. Truthfulness, or lack thereof, can be demonstrated through conflicting statements by the witness or suspect.

Opinions regarding technical matters, however, are permitted if the fraud examiner is qualified as an expert in the matter being considered. For example, a permissible expert opinion might address the relative adequacy of an entity's internal controls. Another opinion

might discuss whether financial transactions conform to generally accepted accounting principles. Recommended remedial measures to prevent future occurrences of similar frauds are also essentially opinions, but are acceptable in fraud examination reports.

Conveying conclusions and limiting opinions to their proper scope can be challenging when the fraud examiner believes a fraud has been committed. To complicate matters, an employer or client will sometimes direct the fraud examiner to state whether fraud was committed in the report. The following are examples of proper and improper statements in fraud examination reports.

WRONG:

I interviewed the suspect on January 5th, and he claimed to know nothing about the transactions at issue. However, I later learned that this claim was false. On February 11th, I interviewed the suspect again and showed him fraudulent invoices of the transactions that he handwrote his initials on. The suspect initially lied, claiming that while the initials were his markings, he would not have approved the invoices if he knew about the nature of the purchases. However, after showing him additional evidence that he knew about the nature of the invoices, he confessed to the truth. His written confession is attached. It is my expert opinion that the suspect is culpable of a fraudulent crime.

RIGHT:

I interviewed the suspect on January 5th, and he stated that he had neither approved nor known about the transactions at issue. At a later interview on February 11th, I showed the suspect invoices for the transactions, which each had three handwritten letters on them matching his initials. The suspect then stated that he had written his initials on each of the invoices, but that he would not have approved them if he knew about the nature of the purchases. After showing the suspect further evidence I had collected, the suspect confessed to approving the transactions, knowing at that time that they were improper. His written confession is attached.

The first example is improper for several reasons. The writer goes beyond relaying the basic facts discovered in the case by making interpretations about those facts that should be left to the reader of the report. The report should include that the suspect made these statements, but it does not need to (and should not) go on to explain that the suspect was lying or being dishonest. Even if the confession and the facts make it seem overwhelmingly likely that the

suspect was lying, making that conclusion is ultimately speculative and not within the purpose of the report. The fraud examiner can point out the inconsistency and possible motive, but readers should be able to reach their own opinions as to the subject's veracity. Additionally, the first example is problematic because the fraud examiner states his opinion on the suspect's culpability. Simply calling the claim an expert opinion does not make it acceptable; expert opinions should be reserved for technical matters where a layperson would have difficulty interpreting the information.

As seen in the second example, the writer points out the inconsistent statements and then stops short of interpreting them. Additionally, note how it does not assume facts that the first example did, such as whether the letters on the invoices were meant to be the suspect's initials. That information might seem apparent, but it is better to let the suspect's statement confirm that they are his initials than for the fraud examiner to make that assumption. When a suspect confesses to a crime, it is almost always the case that he actually is culpable. Even so, the second example does not include the fraud examiner's opinion on the matter. If the fraud examiner is confident that a suspect would be found guilty if the case went to trial, the facts in the report should be accurate and substantial enough to demonstrate that likelihood.

Evidence

Legal standards provide guidelines for handling evidence and maintaining its integrity. The fraud examiner can avoid many problems of evidence maintenance by simply documenting—in memorandum form—the receipt or release of all evidence. The rules for handling and maintaining the integrity of evidence in criminal matters are often more ridged than the related rules in civil matters. The fraud examiner should seek guidance from the retaining counsel or, if necessary, from his personal counsel during the engagement planning stage to be certain that his actions do not inadvertently prevent a critical document from being admissible.

Copy Documents

Most evidence in fraud cases will be in document form, and when reporting the results of a fraud examination, it is best to include copies (not originals) of important documents in the formal report or in the attached appendices. Also, when operating under a lawful court order that compels a custodian to furnish original documents, the fraud examiner should copy those documents (preferably in the presence of the custodian). Then, the fraud examiner should furnish the custodian with a receipt describing the documents copied or

taken. A sample receipt can be found in the sample long-form fraud examination report located in Appendix E.

Safeguarding and Maintaining Documents

After the fraud examiner obtains the documents, he should secure them for evidence. He must be sure that only those people with an absolute need for the documents can access them. For practical purposes, it is usually best to copy all documents (original documents are usually not included in reports). The fraud examiner should mark all original documents in a unique manner, preferably by using initials and dates. To avoid defacing originals, he should use a small but distinctive tick mark or other form of identifier.

When documents are voluntarily furnished, the fraud examiner should leave the originals in place and work with the copies. If originals are later lost, stolen, or misplaced, the copies can normally be introduced in court under the "best evidence" rule, which states that to prove the contents of a document, at least a fair copy of the original must be available for inspection (see the Law section of the *Fraud Examiners Manual*).

Documents might come to the fraud examiner from the attorney. In civil matters, the fraud examiner should request that all documents provided be sequentially numbered (referred to as "Bates numbered"). Bates numbering provides a number of efficiencies throughout the course of the engagement. It can be done manually or digitally through software.

Fraud examiners must avoid taking shortcuts with evidence, and they should not lose or misplace crucial documents. It is inexcusable for a fraud examiner to mishandle evidence; doing so will almost certainly compromise the case.

While digital storage has made documents harder to permanently destroy, it has also made them easier to proliferate. Data that is stored on unsecured or poorly secured networks can be breached by data thieves. Employees should be instructed to always secure their personal electronic devices when not using them. Moreover, many people who routinely work with sensitive data at both the office and at home can lose sight of security. For instance, during a business trip, a British Petroleum employee lost a laptop that contained the personal data of 13,000 individuals who were claimants affected by the Deepwater Horizon oil rig accident in the Gulf of Mexico. The information included the individuals' government identification numbers, addresses, names, phone numbers, and dates of birth. Fraud examiners should not

leave sensitive data open to any unintended parties. It should be under lock and key, password-protected, and encrypted, if necessary, while not in use.

Organization of Information

Because fraud examinations can involve large amounts of data, it is imperative that the fraud examiner properly organize the information. If circumstances permit, an information database should be established early in the case. Information can be presented either in chronological order or by transaction when writing the fraud examination report. These two options are discussed here.

Chronological

Chronological organization presents facts in the order in which they were uncovered. For example, if an anonymous tip predicated the fraud examination, the information received would be presented first in the report. Thereafter, the reader would follow the development of each step as the case progressed.

Information from each witness should be presented in a chronological manner in the report. If interviewing an associate of the target, for example, relay the information in a fashion that begins at the point when the associate first met the target, and then proceed through the course of pertinent events that lead to the present.

It is important to distinguish chronological organization in the context of report writing versus evidence gathering. During the evidence-gathering stage of an investigation, chronologically organizing the documents that will later be used in drafting the report is not recommended because it will make searching for relevant information more difficult. But in writing the report, it might make sense to present information chronologically.

By Transaction

Organization by transaction involves grouping information of the same or similar transactions together. If a multitude of documents support several instances of fraud, this information should be presented by separating individual transactions. For example, in a case of internal fraud involving six different instances of embezzlement, the documents and the related interviews might best be understood if presented as a group. Thereafter, detail the remaining transactions chronologically in the report.

Analyzing the Reader

When drafting a report, fraud examiners must consider who might end up reading it. Fraud examiners should keep in mind that the fraud examination report will be read by the general public and adverse parties. *Under no circumstances should the fraud examiner prepare a communication with the idea that the information will not be disclosed to adverse third parties*. Fraud examiners should draft their reports with this caveat in mind. A fraud examination report should provide a full understanding of the investigation and its findings without the need for additional clarification.

In short, a fraud examination report should adequately answer the classic questions of who, what, when, where, why, and how. And if the report is prepared properly, the reader should not have to refer to any other documents to understand the issues.

Types of Readers

There are many individuals and groups that might end up reading a fraud examination report, including the following parties.

Company Insiders

Managers, executives, and the major investors and owners of private entities will probably review reports of cases involving internal fraud and misdeeds. Because these documents will likely be reviewed by people outside the company as well, they should not address internal control deficiencies, management issues, or other sensitive company considerations. Instead, these matters should be dealt with in a separate letter or other form of communication as directed by counsel.

Attorneys

Reports will be read by attorneys within the organization and others who are outside the entity. In reports prepared at the request of counsel, mark each page "privileged and confidential." This procedure will document any privilege claim (discussed later). Understand, however, that marking the report in such a manner will not necessarily ensure that the privilege will be sustained.

In adversarial proceedings, such as those in the United States and the United Kingdom, attorneys for the defendant(s) will likely gain access to a report during the discovery phase of civil litigation. Similarly, such information will likely be available to the judge and opposing

counsel in inquisitorial judicial systems. These parties will scrutinize the report for errors, omissions, and misstatements. Fraud examiners should be certain that the report is accurate down to the most seemingly unimportant detail. Adverse parties will often cite a minor error as evidence that the entire document is invalid.

In criminal cases, prosecuting attorneys and law enforcement personnel will also review written reports. These individuals will look primarily at evidence and witness statements that will best sustain a criminal prosecution.

Defendants and Witnesses

In either civil or criminal litigation, the defendants will eventually see most, if not all, of a report. If the case reaches court, the witnesses that the fraud examiner identified and interviewed will be provided with copies of their own statements, if not the entire report.

Media Outlets

In some instances, the media might gain access to a report. Report data might be obtained from information disclosed during litigation or, in some instances, from confidential sources. The media is particularly adept at uncovering mistakes and incorrect conclusions drawn by the fraud examiner.

Fraud examiners should assume that any report or affidavit they create, as well as any recorded depositions, are public information. Potential clients and attorneys might access such records to determine whether to retain the services of a particular fraud examiner. If testifying as an expert witness in a court proceeding, opposing counsel might use the information to challenge a fraud examiner's credibility during cross-examination.

Judges or Juries

When the case reaches trial, the fact finder (either a judge or jury, depending on the jurisdiction) will usually receive the fraud examiner's entire report for review and analysis. The fact finder might not have a background in business and accounting matters; therefore, *the report should be as simple and easy to understand as possible*. Of all the important individuals who will review the report, the fact finder in a judicial or administrative proceeding will be the most important by far.

Outlining

Outlines of reports and memoranda of interview can be helpful in long or complex fraud examinations. Report outlines can take many forms, depending on the type(s) of information one must relay.

In general, the outlining process can be divided into three steps. Although the following outlining technique is mechanical, it is easy to master and well suited to unraveling the complexities of large and difficult subjects. Also, most standard office software suites can be used to efficiently complete the outlining process.

Step One

Group naturally related items and write them down on note cards, and then determine whether they are exactly what is needed to meet the demands of the objective, the reader, and the scope of coverage. When they are grouped, arrange them in the proper order and label them with Roman numerals, letters, and numbers to show the level of information.

EXAMPLE

I. First-level head
   A. Second-level head
      1. Third-level head
         a. Fourth-level head
            (1) Fifth-level head

Step Two

Mark each of the note cards with the appropriate Roman numeral, letter, or number. Sort the note cards by major and minor headings. Transfer the notes to paper, converting them to complete sentences.

Step Three

Refine the rough outline. Check to ensure that the subordination of minor headings to major headings is logical and sequential. Check for unity. Stay within the established scope of coverage. Resist the temptation to report irrelevant facts. Check the outline for completeness; scan it to see whether more information is needed.

Grammatical Considerations

A report with grammatical errors will lead readers to question the overall quality—if the writer did not bother to check for typos and similar issues, then perhaps the facts of the case are in need of review as well. Consider the following issues when drafting and reviewing the fraud examination report.

Style

Write each report in a style that is clear, concise, and to the point. Poorly constructed or grammatically incorrect sentences can detract from an otherwise flawless fraud examination.

The purpose for writing a report is to convey information to a reader; therefore, it is the fraud examiner's responsibility to communicate effectively and efficiently. The two most common mistakes that prevent effective report writing are *vagueness* and *wordiness*. Common breaches of good writing include:

- Use of improperly placed or ambiguous modifiers (changes sentence context)
- Use of technical jargon, slang, idioms and/or colloquialisms (places the burden to understand on the reader)
- Use of unnecessary, pretentious verbiage (in an attempt to impress the reader)

Voice

In grammar, *voice* indicates the relation of the subject to the action of the verb. When the verb is in the active voice, the subject acts; when it is in the passive voice, the subject is acted upon.

EXAMPLE

John Doe *wrote* the report. (active)

OR

The report *was written* by John Doe. (passive)

In the above example, both of the sentences say the same thing, but each has a different *emphasis*. In the first sentence, emphasis is on the subject, *John Doe*, whereas in the second sentence, the focus is on the object, *the report*. Notice how much stronger and more forceful the active sentence is.

Always use the active voice unless there is good reason to use the passive. Because passive sentences are wordy and indirect, they are harder to understand.

EXAMPLE

Most instances of fraud *are reported* by coworkers. (passive)

OR

Coworkers *report* most instances of fraud. (active)

Person

Person indicates whether the written text refers to the writer (first person), to the reader or the person for whom the text was written (second person), or to an object or third party about whom the text was written (third person). Person is established through the use of personal pronouns.

EXAMPLE

First person: "*I* did not find a record of the deposit."

Second person: "*You* did not find a record of the deposit."

Third person: "*He* did not find a record of the deposit."

Point of View

Point of view indicates the writer's relation to the information presented, as reflected in the use of person. The writer usually expresses point of view in first-, second-, or third-person personal pronouns. The use of the first person indicates that the writer is a participant or observer ("This happened to me" or "I saw that"). The second and third person indicate that the writer is writing about other people ("This happened to you, to her, to them"). When writing a report, one should never use *the writer* to replace *I* or *me* in a mistaken attempt to sound formal or dignified.

CHANGE: *The writer* believes that this examination will be completed by the end of June.

TO: *I* believe that this examination will be completed by the end of June.

Constructing Clear Sentences

Sentences that make up a report should be simple and clear. Whenever possible, use uncomplicated sentences to state complex ideas. If readers must cope with a complicated sentence in addition to a complex idea, they are likely to become confused. Common sentence structure mistakes to avoid are discussed here.

Rambling Sentences

Sentences that contain more information than the reader can comfortably absorb are known as *rambling sentence*s. The remedy for a rambling sentence is to divide it into two or more sentences. Put the main message of the rambling sentence into the first of the revised sentences.

CHANGE: The payment to which a subcontractor is entitled should be made promptly in order that in the event of a subsequent contractual dispute, the general contractors might not be held in default of contract by virtue of nonpayment.

TO: Pay subcontractors promptly. Then, if a contractual dispute should occur, the general contractor cannot be held in default for nonpayment.

Run-On Sentences

A *run-on sentence* is two or more sentences without proper punctuation to separate them. Run-on sentences can be corrected by creating two sentences or by joining the two clauses with a semicolon (if they are closely related).

CHANGE: The new manager instituted several new procedures some were impractical. (run-on sentence)

TO: The new manager instituted several new procedures. Some were impractical. (period)

OR

TO: The new manager instituted several new procedures; some were impractical. (semicolon)

Omitted Verbs

Do not omit a required verb.

CHANGE: I never and probably never will locate the missing file.

TO: I never *located* and probably never will locate the missing file.

Omitted Subjects

Do not omit a subject.

CHANGE: He regarded price fixing as wrong, but until abolished by law, he engaged in it, as did everyone else.

TO: He regarded price fixing as wrong, but until *it was* abolished by law, he engaged in it, as did everyone else.

Unnecessary Compound Sentences

Avoid compound sentences containing clauses that have little or no logical relationship.

CHANGE: The ledger contains several examples of altered data entries, *and it is usually stored in the company's safe*.

TO: The ledger contains several examples of altered data entries. It is usually stored in the company's safe.

Misplaced Modifiers

A modifier (a word, a phrase, or a clause) is misplaced when it modifies, or appears to modify, the wrong word or phrase.

CHANGE: I *almost* located all the missing files.

TO: I located *almost* all the missing files.

Possible confusion in sentences of this type can be avoided by placing the modifier immediately before the word it is intended to modify.

CHANGE: All businesspersons are *not* talented in mathematics. (The implication is that *no* businessperson is talented in mathematics.)

TO: *Not* all businesspersons are talented in mathematics.

Paragraph Structure

A paragraph consists of several sentences that are grouped together and discuss one main subject. The first sentence of a paragraph should state the paragraph's main point, and subsequent sentences should support and clarify that main point.

For the purposes of report writing, paragraphs should be short. Readers can be daunted by long, complicated paragraphs that contain multiple issues. (Note also that short paragraphs result in more white space on the page, making the document more readable.)

Report Structure

Reporting formats vary widely. Some organizations, especially governmental investigative bodies, use report forms so that case information is provided in a consistent manner.

Also, because all fraud examinations differ, no single format can cover every specific case, company, or situation. Nevertheless, it can help to have a standard format from which to begin; a standard format can reduce the amount of time spent writing a report, while ensuring that all pertinent information is included.

Suggested Standard Format for Fraud Examination Reports

The following is a discussion of items the ACFE recommends that fraud examiners include in most fraud examination reports. Two sample reports are included in Appendix E.

Generally, the following sections should be included in fraud examination reports:

- Background
- Executive summary
- Scope
- Approach
- Findings
- Summary
- Impact
- Follow-up/recommendations

Background

Generally, a written report should contain a background section. The background section should usually be about two paragraphs. It should state very succinctly why the fraud

examination was conducted (e.g., an anonymous tip was received, an anomaly was discovered during an audit, money or property was missing). The background section may also state who called for the examination and who assembled the examination team.

Executive Summary

A written report should also include an executive summary, which should provide the reader with an overview of what was done during the examination process. The executive summary should also summarize what actions were performed during the fraud examination, such as reviewing documents, interviewing witnesses, or conducting analyses or tests.

Additionally, the fraud examiner should summarize the outcome of the examination at the end of the executive summary. For example, "$50,000 in checks was deposited into an account owned by Bob Wilson. When confronted with this information, Wilson stated that he had only borrowed the money and meant to pay it back."

For a simple fraud examination, the executive summary should be no more than four or five paragraphs. For a more complex case, the summary may reach a page or two in length.

Scope

Generally, a written report should include a section that identifies the examination's scope. For example, "Determine whether inventory was misappropriated from the warehouse" or "Determine why money is missing from the bank account." The scope section should be no more than one paragraph.

Approach

Also, a written report should include a section about the approach used. This section gives a brief description of the following items:

- Fraud examination team members
- Procedures (generally, what documents were reviewed or what tests were conducted)
- Individuals interviewed

The approach provides a quick and useful reference regarding who was involved in the fraud examination, what the team reviewed, what tests or analyses were conducted, and what individuals the team interviewed.

Findings

Additionally, a written report should include a section that summarizes the team's findings. The findings section contains the details of the fraud examination and generally will consist of several pages.

In the findings section, the fraud examiner should describe what tasks were performed and what was found. He should provide enough detail so that the reader understands what occurred, but not so much detail that the reader begins to lose interest or becomes bogged down in the details. For instance, the reader wants to know how many invoices were forged, who was involved, how they did it, and what proof you have.

If the fraud examiner's findings section is long, he may use subheadings for particular topics or individuals to make it easier for the reader to stay organized.

The information in the findings section can be presented either chronologically or by topic—whatever makes it easier for the reader to follow.

Summary

Furthermore, a written report should include a summary of the investigation. The summary should succinctly summarize the results of the fraud examination, and it should be one or two paragraphs long. The summary should be similar to the outcome stated at the end of the Executive Summary section.

Impact

A written report should also include a section addressing the impact of any misconduct identified during the investigation. The impact section should describe how the fraud affected the victim organization. In this section, the fraud examiner can provide an estimate of the dollar losses or any other type of tangible or intangible damage already suffered or that might occur in the future.

Follow-Up/Recommendations

A follow-up section is generally optional. This section identifies any aspect of the investigation that remains outstanding, usually because it is outside the mandate of the investigator. This could include the recovery of property that is in the possession of third parties or the collection of information held by vendors or suppliers.

If requested, the fraud examiner might identify and make any recommendations related to procedures and controls; however, the fraud examiner might want to convey recommendations related to flawed internal controls and other organizational failings to management in person or in a separate document. If included in the primary report, this information could potentially be seized upon by defense attorneys at a trial or by representatives at an unemployment hearing to push blame away from the suspect's actions and toward the organization's shortcomings.

Follow-ups or recommendations should state what action is necessary or recommended, including remedial measures such as a review of internal controls, the introduction of a fraud hotline, or an increase in security.

Suggested Format for Expert Reports

The form and structure of expert reports is generally more strict than fraud examination reports due to the procedural rules at trial. The expert report format is also complicated by the fact that the requirements often change based on the type of case and the jurisdiction. Criminal and civil courts, different jurisdictions, and different causes of action might have different requirements concerning the timing, content, and even the necessity of a written report. In certain situations, such as when working as a court-appointed expert, the judge may direct the expert not to issue a written report until after he verbally presents his findings in the court's chambers (i.e., not in open court and not on the written record) to only the judge and opposing parties. In some cases, the court might order the expert report to be sealed, which, for all practical purposes, means that it never existed and may not be disseminated by or to anyone.

Tailoring the report to the laws of the jurisdiction and any applicable court rules is essential. Due to the varying report requirements, fraud examiners serving as expert witnesses should work closely with the retaining party to make sure their expert reports are properly formatted and contain the necessary information. The following structure is a general recommendation, but fraud examiners should always defer to the rules of the relevant jurisdiction if there is a conflict in form, style, or content.

Background

A written report may contain a background section, which should generally be about two paragraphs. It should identify the expert witness and state very succinctly the issues to which

the expert's opinions and conclusions relate. However, in some jurisdictions, background sections in expert reports are excluded if they are nothing more than a recitation of the facts and are not helpful to the trier of fact.

Executive Summary

As in fraud examination reports, an expert report should also include an executive summary, which should provide the reader with an overview of what was done during the witness's examination of the case. Courts greatly appreciate executive summaries even when they grow to ten or more pages, as long as the summaries provide a good initial grasp of the facts at issue from the expert's perspective.

Scope

The expert report should include a section that identifies the scope of the analyses conducted. For example, "Determine whether the financial statements complied with generally accepted accounting principles" or "Determine the amount of financial losses that the plaintiff sustained as a result of the defendant's actions." The scope section should generally be no more than one paragraph.

Facts or Data Considered

In this section, the expert witness should list all information considered in forming the opinions. In significantly sized cases, the documents considered can include many tens of thousands of pages. Fraud examiners should consult with the retaining party on how to fulfill the requirements of this section. Generally, the expert should include:

- A list of any learned treatises, such as the *Fraud Examiners Manual,* that were consulted during the course of the engagement (whether supportive or not supportive of the methodology used)
- All sources, including articles, documents, and books, that the expert consulted
- A list of individuals interviewed
- Any generally accepted empirical studies used
- All case-related legal documents reviewed
- All deposition testimony transcripts reviewed
- All expert and non-retained expert reports reviewed

Methodology

Also, a written report should include a section about the methodology used that demonstrates that the methodology was properly applied to the facts to produce reliable opinions. The methodology section should:

- Explain the methodology used (as discussed in the "Opinions and Bases" section below).
- Explain how the expert properly applied the methodology in accordance with the steps documented in the peer-reviewed generally accepted literature.
- Include quotations from the peer-reviewed, generally accepted literature demonstrating that the methodology used was properly applied to reach the opinions offered by the expert (provide footnote citations to the full document quoted and reference to the location in the expert report's appendices).
- Explain, based on the peer-reviewed generally accepted literature, that the methodology enjoys general acceptance in the particular field.
- Explain, based on the peer-reviewed generally accepted literature, that the use of the methodology demonstrates the same degree of intellectual rigor as that which characterizes the practice of an expert in the relevant field.
- Explain the existence of any standards controlling the operation of the techniques (methodologies) and how the experts use of the methodologies complied with the relevant standards.

Opinions and Bases

Additionally, a written report should include a section that summarizes the fraud examiner's opinions and the bases for those opinions. The testifying expert forms opinions based upon all of the information examined. The opinions and bases section contains:

- A complete statement of all opinions the expert witness will express
- A complete statement of the underlying basis for each opinion
- A discussion and analysis of probable alternative explanations and the work performed by the fraud examiner to prove or disprove a fact at issue
- A discussion and analysis if there is a known or potential error rate for the methodologies used, including the potential impact on the expert's opinions

Exhibits

If the fraud examiner will use any exhibits to summarize or support the expert opinions, they should be attached to the report. Failure to timely provide exhibits and analyses might result in them not being admissible later at trial. Additionally, the expert should include a notice of the potential exhibits in the report, such as the following:

"Attached are the detailed narrative report and the integral exhibits which, together, along with this summary page, constitute my opinions and the related bases. The entire detailed narrative report and the integral exhibits that are included in the attached appendices may be used as exhibits during trial."

Qualifications

The report should mention education, professional experience, research, relevant degrees or certifications, licenses, and any other experience that would tend to support the person's expertise.

Special Considerations for Expert Reports

Experts must give careful consideration when preparing the report, as the expert's reputation is on the line.

Keep the following six tips in mind when preparing an expert report:

- Be brief.
- Avoid ambiguity or inexact language.
- Avoid generalizations; be specific.
- Add charts or graphs where appropriate.
- Reference your work.
- Meticulously check the report for accuracy and neatness.

Sometimes cases involve thousands or even millions of documents, but someone must present a report on the review of those documents at trial. Such cases might make it impractical or impossible to timely analyze all of the documents. It is common for complex cases to require delegation of tasks to create a fraud examination report, such as subordinates searching for key documents and creating document summaries.

An important problem in the preparation of reports and accounting summaries arises from the delegation of tasks to subordinates. If the expert presenting evidence has no direct knowledge of or has not examined the specific documents, he might be trapped under the hearsay rule (if applicable). Thus, if the expert delegates tasks, it is important that he review the delegated work and compare all original work documentation.

It also is important to know the effect of other assumptions on the conclusion or opinion reached in the report. It often is possible to trap an expert into giving alternate opinions

based upon assumptions that had not been considered. Generally, working papers and schedules supporting the report should not show contradictory conclusions because such contradictions may be produced in court. This is not to advocate that working papers should be deleted or amended; rather, it is a caution that these papers should be prepared with the precept that they could ultimately be submitted to the court. Thus, work papers should be appropriately prepared.

Once they accept a case, many experts immediately start assembling a narrative version of the events. A *narrative* is a detailed summary of the facts of the case, and it serves as the raw material for rendering an official opinion. When assembling a narrative, it is important that the text be written with care and professionalism because the text may (and probably will) be produced at trial.

If an expert report is required, include only what is necessary. Avoid gratuitous and unimportant comments.

Reporting Documents

There are a number of basic reporting documents, including:

- Memoranda
- Cover page
- Exhibits, documents, or enclosures
- Forms
- Indexes
- Transmittal letter

In general, fraud examination reports can be in a long-form report or a short-form report. The long-form report will consist of copies of the documents listed above. The long-form report included in Appendix E illustrates this approach.

The heart of the documentation is the memorandum of interview, and one memorandum should be prepared for each official contact. Once all the memoranda of interviews are completed, they are typically assembled in chronological order and indexed.

Memoranda

Use memoranda to document all interviews and other pertinent information discovered during the examination. Each memorandum should contain the following information where appropriate:

- Heading
  - File number or control number
  - Name of person reporting
  - Case name or subject
  - Subject of memorandum
  - Date
- Details of facts
  - If the interview was voluntary
  - The fact that one provided one's identity
  - The witness was informed of the nature of the inquiry
  - Date of inquiry
  - How the interview was conducted (in person, by telephone, etc.)
  - If the interview was electronically recorded
  - Facts learned during inquiry

Cover Page or Letter

A *cover page* summarizes the examination's prominent points. The cover page should be direct and succinct. If a report is submitted to an outside agency (e.g., law enforcement or outside counsel), it should be accompanied by a cover letter. The cover letter should briefly summarize the information in the report and include the principal witnesses. It is not necessary to list all witnesses on the cover page, but the cover page should contain a list of the most valuable witnesses.

Exhibits

As a general rule, copies of exhibits should be included in the report and not attached separately. However, bulky files (including working papers and similar exhibits) might be attached separately and referred to in the body of the report. The chain of custody should be maintained over original documents.

Forms

A complete fraud examination report must document every step of the information-gathering process. Because the orderly and legal presentation of evidence requires the fraud

examiner to organize a great deal of information, the fraud examiner should use the forms to facilitate this task (see Appendix C). As a general rule, these forms are kept in the file and are not included in the report unless necessary. These forms include the following items.

Consent to Search

A *consent to search* form requests a person's signature as an indication of agreement to a search. Although such forms can vary significantly between jurisdictions, they typically:

- Document the fact that the subject has been informed of any applicable legal rights.
- State that the written permission is given voluntarily and not because of threat, duress, coercion, or promise to induce permission.
- Indicate that the subject can refuse to consent to such a search.
- Describe the area or items to be searched.
- Explain that signing the form indicates that the subject is giving written permission to search his person or the premises in issue.

The signatures on the bottom of the form (subjects and witnesses) indicate that the person is voluntarily giving the fraud examiner written permission to search the premises and to remove pertinent papers, documents, or other property.

Receipt for Property

A *receipt for property* form is a multipurpose document used to list items of evidence that have been received, returned, or released. This form includes the following information:

- Date of transfer
- Property owner's name
- Owner's address
- Description of item(s)
- Signature lines ("Received by" and "Received from")

Telephone Recording Consent

A *telephone recording consent* form stipulates where, when, and with whom telephone conversations can be recorded. This form states that the subject has granted permission without threats or promises of any kind, and it must be signed by the subject and witnesses. Be cautioned that the form alone does not make the conduct of recording a telephone conversation legal. Fraud examiners must verify the legality of this type of recording within the associated jurisdiction(s) prior to engaging in such activity.

Consent to Record

A *consent to record* form documents the fact that an individual has given the fraud examiner permission to record specific conversations. This form must be signed and witnessed.
It details:

- The name of the individual
- His address
- The location of the conversation(s)
- Who might record the conversation(s)
- The name of the subject(s) with whom the individual might converse
- The date(s) of the conversation(s)

Customer Consent and Authorization for Access to Financial Records

This form authorizes a financial institution to disclose the customer's own records to the fraud examiner or other specifically listed individuals. It must be signed by the account holder.

Evidence Control Log

In cases where there are significant items of evidence, it might be advisable to prepare an evidence control log. The *evidence control log* is a form that documents:

- The evidence control center location
- The bank safe-deposit box location
- The location of other evidence
- The signature(s) of person(s) placing in or removing evidence from repository
- The reasons why evidence was moved
- The file case number
- The time(s) and date(s) when authorized individuals entered and departed the evidence repository

Indexes

The fraud examiner might decide to include an index in his report. The index should contain an alphabetical listing of names or topics and associated page numbers to where useful material relating to those names or topics can be found in the report.

Transmittal Letter

The fraud examiner might include a transmittal letter to provide the report's recipient with a specific context in which to place the report. Often, a transmittal letter will accompany a

report to inform readers of the report's context, and this type of letter can serve as a permanent record of having sent the report.

Visual Aids

Occasionally, the fraud examiner might include visual aids prepared either as part of the report or to be used as exhibits at trial.

People generally only recall a small percentage of what they hear, but they recall a much larger percentage of what they both hear and see. In a trial setting, some people do not care as much about what comes out of witnesses' mouths; they want to understand the information themselves, and they want to understand it in a familiar way. Moreover, people tend to process information better when it is presented in a visual format than when it is presented in a verbal format. Thus, visual aids can assist expert witnesses in clearly communicating their findings.

Visual aids should be kept simple. Several different types of visual aids are discussed here.

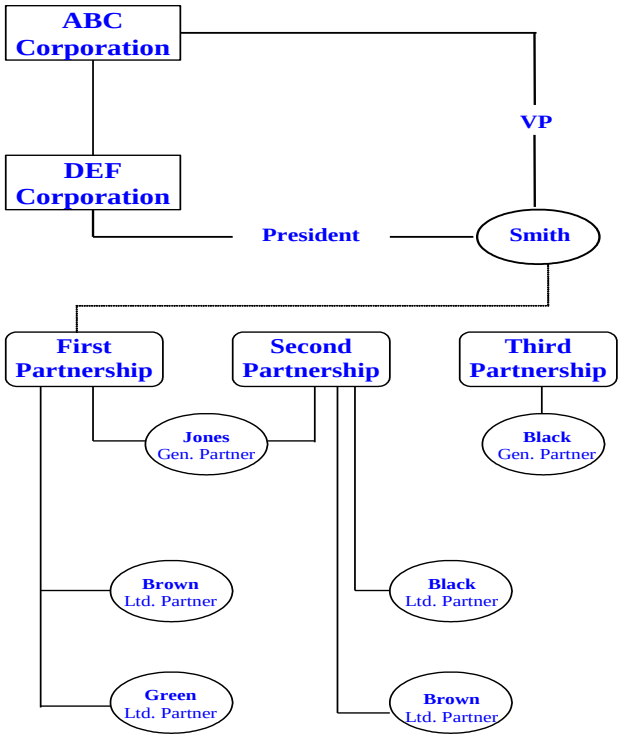
Link-Network Diagrams

Link-network diagrams show the relationships between people, organizations, and events. In these diagrams, different symbols are used to represent different entities: a square can symbolize an organization; a circle, a person; a triangle, an event; and so forth. It does not matter which symbols are used as long as they are used consistently. In link-network diagrams, confirmed connections between entities can be represented by a solid line or enclosure within another symbol. Speculative or presumed relationships can be indicated by broken lines. To achieve its intended purpose, a graphic should always be clear. Therefore, these diagrams should not contain lines that are crossed, if possible.

EXAMPLE

Smith is vice president of the ABC Corporation and president of the DEF Corporation, a subsidiary of ABC. Jones is general partner in the First and Second Partnerships. Brown and Green are limited partners in the First Partnership. Brown and Black are limited partners in the Second Partnership. Black is also a general partner in the Third Partnership. Smith also might have an interest in the First Partnership.

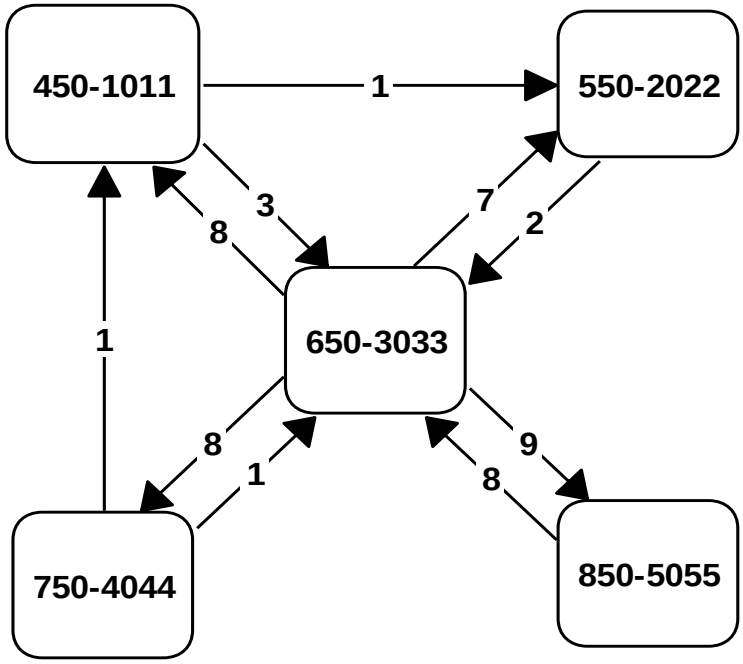
LINK NETWORK DIAGRAM



Matrices

A *matrix* is a type of visual aid in the form of a grid that shows the relationship (or points of contacts) between a number of entities. Known contacts can be differentiated from presumed contacts by means of a bullet or a circle.

A matrix can be used to identify the direction and frequency of telephone traffic between suspect parties.



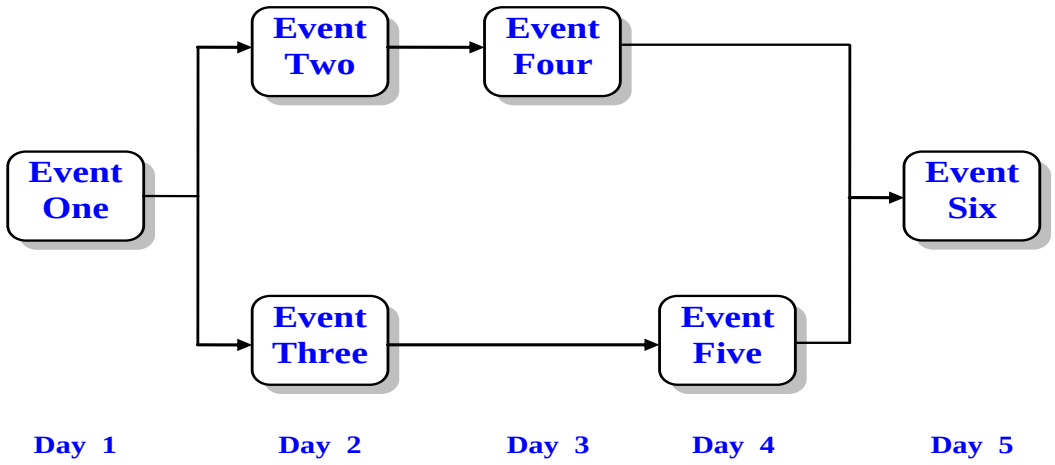
This information can also be represented in chart form.

	450-1011	550-2022	650-3033	750-4044	850-5055	Total Outgoing Calls
450-1011	X	1	3			**4**
550-2022		X	2			**2**
650-3033	8	7	X	8	9	**32**
750-4044	1		1	X		**2**
850-5055			8		X	**8**
Total Incoming Calls	**9**	**8**	**14**	**8**	**9**	

Time-Flow Diagrams

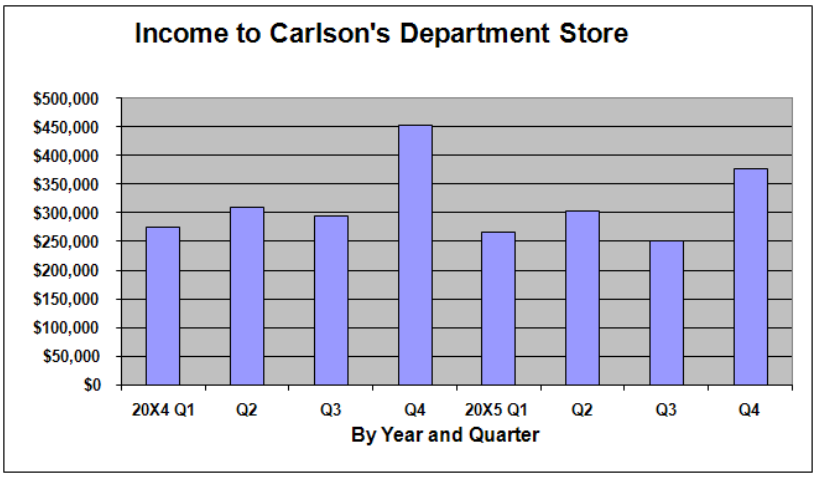
A time-flow diagram is a time-sequenced flowchart that represents a process showing the steps as boxes of various kinds.

The following chart shows the relationship of significant events, in the order in which they occurred.

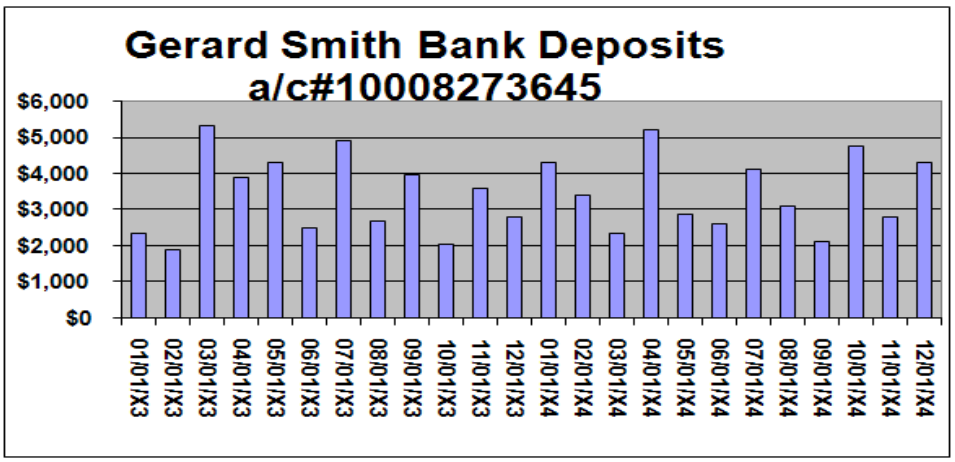


Time-Series Analysis

A time-series analysis, which can be conveyed with bar graphs and line graphs, is a particularly useful tool when displaying patterns of activity over time (e.g., by month, quarter, or year). The following example, which involves Carlson's Department Store, displays the cyclical nature of the store's income by quarter, and it provides a comparison between similar quarters in 20X4 and 20X5. The bar graph also shows that each quarter of 20X5 produced less income than the same quarter in 20X4, resulting in an overall decrease in income.



Another example of a time-series analysis follows; it conveys Gerald Smith's personal banking account, by month and year. It illustrates that his account fluctuated between $2,000 and $5,000 each month.



Timelines

A *timeline* is a summary of the events that have occurred (i.e., they summarize key activities), arranged along a line in chronological order. Although timelines are not always simple—in fact, they can be quite complex—they must be brief, and they must include all relevant information. Timelines are especially helpful to witnesses who are presenting a case to a judge or jury. This is because, in addition to summarizing key activities, timelines allow the witness to "tell the story" of what occurred in a simple, yet complete, way.

Suitable material for timelines includes data that contain numerous dates and activities. Such material might include witness statements, financial transactions, corporate records, communications (e.g., emails or telephone calls), contracts, meeting minutes, and other information. If dates are not present, a timeline can still be created if the sequence of events is known.

Summaries of Witnesses' Statements

To identify inconsistent statements and permit quick review of voluminous witness testimony, fraud examiners can reduce witnesses' testimony and witnesses' statements to summary form. When summarizing witnesses' statements, fraud examiners should identify pertinent passages by briefly indicating the topic being covered at a given point. They should also provide a synopsis of the statement (see the following example).

Summary of Evidence
Emily Watson

Page	Topic	Testimony
5	Watson hired 05/23/XX	Personnel file
5	Watson promoted to Purchaser 09/08/XX	Personnel file
8	Watson and Harrison friends	Gupta interview
15	Checks to Oscar	Silas interview
30	Indebtedness of Watson	Public records

When summarizing, fraud examiners should keep the synopsis as succinct as possible. Too much detail will impair the summary's utility. The fraud examiner or someone familiar with the facts and issues in the case should prepare the summary; it should not be prepared by an assistant who does not know what might or might not be relevant.

A summary of witnesses' statements can also be useful as a basis for a chronology.

The fraud examiner typically will also prepare other written documents, including, but not limited to, engagement and advisory letters. For more information on engagement and advisory letters, see the "Planning and Conducting a Fraud Examination" chapter at the beginning of this section of the *Fraud Examiners Manual*.

Presenting the Case to Prosecutors and Other Government Authorities

If fraud is discovered, the fraud examiner might also have to discuss it with the relevant individuals and determine whether the case should be presented to law enforcement or government authorities for prosecution. Some jurisdictions require criminal reporting under some circumstances, but victims often may choose whether to inform authorities.

Usually, the victim does not prosecute—or ultimately decide to prosecute—an offending individual. Instead, it is generally within the government's discretion to decide whether to bring criminal charges against a person, as well as with what crimes the individual will be

charged. In some jurisdictions, private parties are allowed to commence criminal actions in limited circumstances.

Even though these decisions generally belong to the government, however, there are several reasons an entity might seek prosecution of an offending employee. For example, prosecution punishes the offender and, hopefully, will deter others from engaging in similar offenses. In addition, criminal charges brought against an employee might help an organization defray the losses suffered as a result of fraud. Similarly, prosecution might aid the victim in pursuing civil remedies against an offender. In some jurisdictions, private victims can join criminal proceedings to recover damages resulting from the crime.

Even if the fraud examination establishes a solid case against a suspect, government authorities might be reluctant to bring criminal charges in a fraud case because of the time and expense involved, lack of expertise, the high standard of proof required for conviction, and so on.

Nevertheless, there are a number of issues that fraud examiners should be aware of when presenting a case to law enforcement or government authorities for potential prosecution. For instance, before presenting a case to law enforcement or the prosecuting party, it will benefit the fraud examiner to develop a relationship with either or both, or at least to have enough knowledge about both entities to know whom to call so that any submission of a case is not lost in the administrative netherworld of bureaucracies.

It is important to note that attorneys will generally take cases that enhance their reputations and statistics. Government lawyers have high conviction rates in the cases they prosecute, and this is due in part to their reluctance to take cases they might lose. Therefore, a prosecutor will be more likely to pursue the case if the evidence is strong or if the case involves significant losses, deals with notorious or important defendants (e.g., prior criminal records), and does not appear to be unduly complex. Furthermore, prosecutors, like all professionals, are very busy, handling enormous caseloads in clogged dockets around the country, and many prosecutors have a limited background in financial matters.

Nevertheless, fraud examiners can do a number of things to help their chances of prosecution, and this discussion will provide some basic rules for dealing with prosecuting parties.

First, fraud examiners should generally not submit a case to government authorities with a suspicion, but little incriminating evidence, that a fraud has occurred. In general, a prosecutor will only take a case when he believes he has competent evidence to meet the burden to prove that the defendant is guilty in a judicial proceeding. (Note that the laws of evidence are different from jurisdiction to jurisdiction—fraud examiners should have a fundamental familiarity with these laws prior to presentation of any case to the government authority.)

Second, fraud examiners should generally not submit the case to authorities unless their investigation is complete. Have all of the relevant documents been gathered? Has the fraud examiner made all of his observations? Has the fraud examiner interviewed all necessary witnesses? A case is more likely to be chosen for prosecution if the facts are fully developed.

Third, to get the full attention of the prosecutor or other government authorities, the fraud examiner must have his case ready to present in an organized and clear package. A fraud examiner might have done a great job in developing evidence, but that information must be communicated effectively to the government, which must be convinced that the case is worth the time and effort necessary to pursue legal action against the wrongdoer.

Moreover, fraud examiners can enhance their chances of prosecution if:

- They have obtained a legal and binding admission of guilt.
- They obtain a commitment from the outset for the government authority to consider pursuing the case based on the evidence obtained.
- They avail themselves to the government for aid in the prosecution.
- They follow up regularly with the person overseeing the investigation to ensure their case does not get forgotten or overlooked.

And if possible, the fraud examiner should present his case to a prosecutor or law enforcement agent who has:

- A successful track record in white-collar cases
- A reputation as a hard worker

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

FRAUD POLICY REVIEW PROPOSAL
(LONG-FORM FRAUD EXAMINATION ENGAGEMENT LETTER)

[Date]

[Client Company's Contact Person]
[Department]
[Company Name]
[Address]

RE: Fraud Detection and Deterrence Review

Dear [Name of Client Company's Contact Person]:

Pursuant to our discussion, [fraud examiner's company name] is pleased to present this proposal to the [prospective client's company name] (the Company) to perform a review of the Company's policies and procedures to detect and deter fraud.

This review is designed to assist in determining the Company's procedures concerning adequate fraud detection and deterrence methods. This review cannot be relied upon to provide assurances that fraud does not or will not exist within the company. Rather, it is designed to highlight weaknesses, if any, in the existing system. A potential review by [fraud examiner's company name] would also provide management with recommendations for a proactive fraud deterrence program.

The fee for these services will be $[full amount of services] plus expenses, which include, but are not limited to, travel expenses, telephone and photocopy charges, and charges for computerized research. One-half of the fee is due upon signing this letter and the other half upon delivery of the report. All expenses will be billed at the conclusion of each month and are due upon receipt. Any invoice remaining outstanding for more than 30 days will be subject to a rebilling charge.

Please review this proposal. If this proposal meets with your approval, please sign and return one copy along with your check for $ [half of the amount for services] in the enclosed envelope. If you have any questions, please do not hesitate to call. Thank you.

Sincerely yours,

[Signature, name, title, company name, and contact information of fraud examiner]

MENU

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

FRAUD EXAMINATION PROPOSAL
(SHORT-FORM FRAUD EXAMINATION ENGAGEMENT LETTER)

[Date]

[Name of Client's Legal Counsel or Representative], Esq.
[Legal Department]
[Company Name]
[Address]

RE: Fraud Examination

Dear [Name of Client's Legal Counsel or Representative]:

Pursuant to our discussion, [fraud examiner's company name] presents this proposal to the [name of company receiving the proposal] (the Company) to perform a fraud examination as a result of certain allegations that have come to the attention of the Company.

Our examination will be conducted in accordance with lawful fraud examination techniques, which include, but are not limited to, examination of books and records, voluntary interviews of appropriate personnel, and other such evidence-gathering procedures as necessary under the circumstances. We cannot provide assurances that fraud, if it exists, will be uncovered as a result of our examination.

The fee for this examination will be $ [amount of service per hour] per hour plus expenses, which include, but are not limited to, travel expenses, telephone and photocopy charges, and charges for computerized research. A retainer of $ [cost of retainer] is due upon signing this letter. All expenses will be billed at the conclusion of each month and are due upon receipt. Any invoice remaining outstanding for more than 30 days will be subject to a rebilling charge. The hourly rate will be applied against the retainer. Once the retainer reaches a fully applied status, an additional retainer of $ [additional amount after retainer] will be required. We estimate the entire engagement will not be more than $ [estimated amount], excluding any testimonial requirements. Any depositions or court appearances will be billed at the rate of $ [hourly rate for depositions and court appearances] per hour. All outstanding invoices must be paid before any testimonial appearances.

Please review this proposal. If it meets with your approval, please sign and return one copy along with your check for $ [cost of retainer] in the enclosed envelope. If you have any questions, please do not hesitate to call. Thank you.

Sincerely yours,

[Signature, name, title, company name, and contact information of fraud examiner]

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

FRAUD POLICY REVIEW
(FRAUD EXAMINATION ADVISORY LETTER)

[Date]

[Name of Client Company's Contact Person]
[Company Name]
[Address]

RE: Fraud Detection and Deterrence Review

Dear [Client Company's Contact Person]:

Pursuant to your request, [fraud examiner's company name] has performed a review of the policies and procedures of the [client's company] (the Company) for the purpose of reviewing their adequacy to detect and deter fraud.

This review does not provide assurance that fraud does not or will not exist. Having completed the following steps, we have determined that in order to strengthen its fraud detection potential, the Company's procedures need improvement in the areas outlined herein.

Part of the purpose of an internal control system is to ensure that the assets of the Company are properly safeguarded from employee or outsider misapplication. In addition, an adequate system of internal control contains detection methods so that if misappropriation takes place, the irregularity will come to the attention of those who can remedy the situation and take suitable action against it. An adequate system of internal control is not designed to prevent or detect a collusive fraud scheme among employees and/or management. Our review included some the following procedures:

[In this section, briefly describe the main procedures followed. For example]:

a. We read the Company's anti-fraud policies and procedures.
b. Through interviews with personnel key to the operations at the Company, we determined if the existing policies and procedures were being followed.
c. We charted the current flow of business transactions as they are being recorded at the Company.
d. We compared the flow of transaction approval and recording with the policies and procedures.

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

The following discrepancies were noted in [client company's] system of internal control:

[In this section, explain briefly the differences between the established internal controls and those procedures followed by the company's personnel.]

Based on our review, we recommend the following changes be instituted in the Company's internal controls system:

[In this section, make your recommendations.]

In addition to the above recommendations, we suggest the Company consider the following proactive approach to fraud deterrence:

[In this section, suggest proactive steps, such as:]

- An internal audit structure reporting to the board of directors
- Active inquiry of fraudulent transactions
- Hotlines
- Annual conflict of interest statements
- Annual review of employee expense accounts, etc.

This letter is not intended for general circulation or publication, nor is it to be reproduced for any purpose other than that outlined above. [Fraud examiner's company name] does not assume any responsibility or liability for losses occasioned to one or others as a result of the circulation, publication, reproduction, or use of our letter contrary to the conditions of this paragraph. The validity of our letter is predicated on the extent to which full, honest, and complete disclosure was made by all parties.

We will be in contact soon to discuss the details of this letter. In the meantime, please feel free to contact with questions.

Sincerely yours,

[Signature, name, title, company name, and contact information of fraud examiner]

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

EVIDENCE DOES NOT SUPPORT ALLEGATION (FRAUD EXAMINATION ADVISORY LETTER)

[Date]

[Name of Client's Legal Counsel or Representative], Esq.
[Law Department]
[Company Name]
[Address]

RE: Fraud Examination

Dear [Name of Client's Legal Counsel or Representative]:

We have conducted a fraud examination concerning a possible [list fraud event(s), such as misappropriation of assets] of [Company Name]. This examination was predicated upon [list reasons why fraud examination was warranted, such as information resulting from a routine audit of the company's books by the company's internal auditors].

Our fraud examination was conducted in accordance with lawful fraud examination techniques, which included [description of techniques, which may include examination of books and records; voluntary interviews of appropriate personnel; and other such evidence-gathering procedures as necessary under the circumstances].

Because of the nature of fraud, no assurances can be given that fraud does not exist. However, based on the results of our examination, we have found no evidence to support the conclusion that [description of how fraud event did not occur, such as the assets in question were misappropriated].

Sincerely,

[Signature, name, title, company name, and contact information of fraud examiner]

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

EVIDENCE SUPPORTS ALLEGATION
(FRAUD EXAMINATION ADVISORY LETTER)

[Date]

[Name of Client's Legal Counsel or Representative], Esq.
[Law Department]
[Company Name]
[Address]

RE: Fraud Examination

Dear [Name of Client's Legal Counsel or Representative]:

We have conducted a fraud examination concerning a possible [list fraud event(s), such as misappropriation of assets] of [Company Name]. This examination was predicated upon [list reasons why fraud examination was warranted, such as information resulting from a routine audit of the company's books by the company's internal auditors].

Our fraud examination was conducted in accordance with lawful fraud examination techniques, which included [description of techniques, which may include examination of books and records, voluntary interviews of appropriate witnesses/personnel, and other such evidence-gathering procedures as necessary under the circumstances].

Based on the results of our fraud examination, we find that there is sufficient evidence to support the conclusion that [description of fraud event that occurred and the extent of the monetary damage, such as assets in the amount of $ _____ were misappropriated from the company's bank account and that Mr./Ms. _____ appropriated these assets for his/her personal benefit].

Please call me to set up a meeting at your earliest convenience so we can present you with the details of the evidence we gathered during our fraud examination.

Sincerely,

[Signature, name, title, company name, and contact information of fraud examiner]

APPENDIX A

ENGAGEMENT AND ADVISORY LETTERS

INCONCLUSIVE EVIDENCE
(FRAUD EXAMINATION ADVISORY LETTER)

[Date]

[Name of Client's Legal Counsel or Representative], Esq.
[Law Department]
[Company Name]
[Address]

RE: [Fraud Examination]

Dear [Name of Client's Legal Counsel or Representative]:

We have conducted a fraud examination concerning a possible [list fraud event(s), such as misappropriation of assets] of [Company Name]. This examination was predicated upon [list reasons why fraud examination was warranted, such as information resulting from a routine audit of the company's books by the company's internal auditors].

Our examination was conducted in accordance with lawful fraud examination techniques, which included [description of techniques, which may include examination of books and records; voluntary interviews of appropriate personnel; and other such evidence-gathering procedures as necessary under the circumstances].

The results of our examination are inconclusive. Because of the nature of fraud, no assurances can be given that fraud does not exist. However, based on our examination, there is currently insufficient evidence to support the conclusion that [description of fraud event that was thought to have occurred, such as the assets in question were misappropriated].

Sincerely,

[Signature, name, title, company name, and contact information of fraud examiner]

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
1. Fully debriefed all informants and witnesses?		
2. Documented the allegation in writing?		
3. Established initial predication?		
4. Identified all possible schemes or indicators of fraud?		
5. Developed fraud theory?		
6. Notified legal counsel and discussed whether to proceed?		
7. Obtained, recorded, and filed all pertinent information and documents in the files?		
8. Determined the potential loss?		
9. Identified potential witnesses?		
10. Determined if an error or mistake was made?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
11. Reviewed internal controls?		
12. Developed an investigative plan?		
13. Determined the type of evidence needed to pursue?		
14. Identified indicators showing intent?		
15. Reviewed payroll records and canceled checks?		
– Identified all bank accounts?		
– Identified number of exemptions?		
– Identified who might be endorsing checks?		
16. Reviewed personal expense reports?		
– Identified unusually high expenses?		
– Identified credit card used?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
– Identified where suspect entertains clients?		
– Identified duplicate submissions?		
17. Performed background/asset check?		
– Driver's license violations?		
– Motor vehicle registration records?		
– Regulatory licenses?		
– Vital statistics?		
– Building permits?		
– Business filings?		
* Fictitious names indices?		
* Business licenses?		
* Corporate records?		
* Limited partnerships?		
* Filings with securities commission(s)?		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
– Local and state/provincial records?		
* Criminal?		
* Civil?		
* Domestic?		
* Probate?		
* Real estate?		
– Central/federal court filings?		
* Criminal?		
* Civil?		
* Bankruptcy?		
– Consumer credit records?		
– Business reporting services?		
18. Determined who should be interviewed?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
19. Developed interview approach?		
20. Performed financial analysis?		
– Vertical analysis?		
– Horizontal analysis?		
– Ratio analysis?		
– Industry analysis?		
– Net-worth analysis?		
21. Will an undercover operation be used?		
– Plan developed?		
– Approval received?		
– Operation completed?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
22. Will surveillance be used?		
– Plan developed?		
– Personnel set up?		
– Surveillance curtailed?		
23. Developed other informants?		
24. Use mail covers?		
25. Performed link analysis?		
26. Identified computers that might be linked to investigation?		
– Identify expertise needed?		
– Data downloaded?		
– Data printed?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
27. Performed forensic document analysis?		
– Handwriting?		
– Reviewed altered documents?		
– Ink analysis?		
– Document restoration?		
28. Interviews conducted?		
– Interviews documented?		
– Signed statements received?		
– Identified other witnesses to interview?		
– Interviewee knows how to get in touch with one or more investigation personnel?		
29. Completed documentation and report to management?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
30. Employee(s) terminated?		
– Received identification badge or deleted from system?		
– Notified security not to allow access to corporate premises?		
– Personal belongings identified and arrangements made for employee to collect?		
31. Report written?		
– Background?		
– Executive summary?		
– Scope?		
– Approach?		
– Findings?		
– Pertinent correspondence?		
– Documentation of interviews?		
– Pertinent evidence included?		
– Report approved by supervisor?		

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

	YES	NO
32. Appointment made with law enforcement agency?		
33. Follow-up contact made with investigators?		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Documents To Be Examined	To Do	Date Received
ACCOUNTING RECORDS		
Balance sheet		
Income statement		
Statement of cash flows		
Bank statement		
Expense account		
Computer password		
Other: _____		
_____		
Date of employment		
Signed ethics agreement (conflict-of-interest statement)		
Current address		
Prior addresses		
Spouse's name		
Maiden name		
Children's names		
Prior employment		
Prior supervisor		
Insurance information (covered dependents)		
Employee evaluation (performance reviews)		
Garnishments		
Vacation/holiday schedule		
Other: _____		
_____		
PERSONAL RECORDS		
Bank statements		
Tax returns		
Insurance policies		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Documents To Be Examined	To Do	Date Received
Mortgage records		
Brokerage statements		
Credit card statements		
Telephone records		
Other business records		
Investments		
Vehicle information		
Diaries (calendars)		
PUBLIC RECORDS—PERSONAL		
Civil filings		
Criminal filings		
Property tax records		
By name		
By address		
Tax liens		
Financing		
Other: _____		
_____		
Judgments		
Garnishments		
Domestic-relations records		
Divorce		
Property settlement		
Financial statements		
Tax returns		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Documents To Be Examined	To Do	Date Received
Depositions		
Probate records		
Bankruptcy filings		
Financial statements		
Bank statements		
Property ownership		
Education verification		
University/college		
Professional licenses		
Corporate records		
Company name		
Individual (incorporators)		
Assumed name index		
Vehicles owned		
Lienholder		
Boats owned		
Lienholder		
Aircraft owned		
Lienholder		
PUBLIC RECORDS—BUSINESS		
Utility records		
Commercial filings (e.g., UCC filings)		
Tax receipts		
Tax liens		
Who actually pays the taxes?		
Post office box application		
Civil filings		
Assumed-name index		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Documents To Be Examined	To Do	Date Received
Corporate charter (bylaws)		
Business credit history		
Dun & Bradstreet		
Better Business Bureau (or equivalent authority)		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Documents To Be Examined	To Do	Date Received
Other: _____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		
_____		

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Neutral Witnesses:

Name	Phone	Date Contacted	Interview Completed	Report Date

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Adverse Witnesses:

Name	Phone	Date Contacted	Interview Completed	Report Date

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Co-conspirators:

Name	Phone	Date Contacted	Interview Completed	Report Date

MENU

APPENDIX B

FRAUD EXAMINATION CHECKLIST

Case Name: _____ **Case No.:** _____

Suspects:

Name	Phone	Date Contacted	Interview Completed	Report Date

APPENDIX C

SAMPLE FORMS

CONSENT TO SEARCH

_____
(Date)

_____
(Location)

I, _____, having been informed of my right not to have a search made of the premises hereinafter mentioned without a legal order and of my right to refuse to consent to such a search, hereby authorize _____ and _____ to conduct a complete search of my premises located at _____. The above mentioned individuals are authorized by me to take from my premises any letters, papers, materials, or other property that they might desire.

This written permission is being given by me voluntarily and without threats or promises of any kind.

_____
(Signed)

WITNESSES:

_____

_____

This is to certify that on _____at _____, the individuals described above, conducted a search of _____. I certify that nothing was removed from my custody.

_____
(Signed)

Witnessed:

_____

_____

MENU

APPENDIX C

SAMPLE FORMS

CONSENT TO SEARCH

On (date) _____ item(s) listed below were:

_____ Received from

_____ Returned to

_____ Released to

Name _____

Address _____

Description of

Item (s): _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Received by: _____

Received from: _____

MENU

APPENDIX C

SAMPLE FORMS

CUSTOMER CONSENT AND AUTHORIZATION FOR ACCESS TO FINANCIAL RECORDS

I, _____, hereby authorize _____,
(Name of Customer) (Name of Financial Institution)

_____,
(Address of Financial Institution)

to disclose these financial records: _____

to _____
(Name of Persons)

for the following purpose(s):

_____

_____.

I understand that this authorization can be revoked by me in writing at any time before my records, as described above, are disclosed, and that this authorization is valid for no more than three months from the date of my signature.

_____ _____
(Date) (Signature of Customer)

_____
_____
(Address of Customer)

_____
(Witness)

MENU

APPENDIX C

SAMPLE FORMS

FRAUD INCIDENT REPORT LOG

Date Reported:		
Department(s) or Division(s) Involved:		
Type of Fraud:		
Suspect Employee(s):		
Suspect Third Parties:		

Estimate of money involved (if known):

How the suspected fraud became known:

How the fraud was carried out (if known):

APPENDIX C

SAMPLE FORMS

Additional information:

Actions taken in response:

APPENDIX C

SAMPLE FORMS

INVENTORY OF EVIDENCE AND CHAIN OF CUSTODY LOG

Case Name (Number): _____

Collected By (Name and Contact Information): _____ Date & Time Collected: _____

Inventoried By: _____ Date & Time Inventoried: _____

Location Where Collected: (location and how it was kept) _____

_____

Description of Evidence: (description, title, identification number, date created, etc.) _____

_____

CHAIN OF CUSTODY

Date & Time	Name and Signature of Person Logging Item Out	Name and Signature of Person Receiving Item	Purpose	Date Item Returned
	Name: Signature:	Name: Signature:		
	Name: Signature:	Name: Signature:		
	Name: Signature:	Name: Signature:		
	Name: Signature:	Name: Signature:		

MENU

APPENDIX C

SAMPLE FORMS

EVIDENCE CONTROL LOG

Bank Safe Deposit Box: _____ Location: _____
(Name of Bank)

Evidence Control Center Location: _____

Office Safe or Vault Location: _____

Other: _____ Location: _____
(File Cabinet, etc.)

(1) Signature of person(s) placing evidence in or removing from repository. If entry to facility for other reasons, briefly state in column 2.	(2) Reasons	(3) File Case No.	ENTERED		DEPARTED	
			Time	Date	Time	Date

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Directories

Directories provide data on national, trade, business, and commercial associations. Some of the more frequently used directories are discussed below.

Dun & Bradstreet Directories

Dun & Bradstreet (D&B) is a business and financial information services provider. D&B provides access to a variety of public records, including business registration information, secured financing transactions, unsecured credit transactions, lawsuits, liens, judgments, and bankruptcies.

Best's Insurance Reports

Best's Insurance Reports presents comprehensive statistical reports of the financial position, history, and operating results of thousands of property/casualty or life/health insurance companies operating in the United States, Canada, and around the world. The individual report on each institution includes a review of its history, management and operations, investments, operating results, and other statistical compilations.

City Directories

City directories usually contain the name, residence, occupation, and sometimes the place of employment of the city's influential people. Such directories can usually be found at public libraries, chambers of commerce, and secondhand bookstores.

Gale

Gale, part of Cengage Learning, is an educational publishing company. It is known for its online databases and multi-volume reference works. Some of its resources include: *Gale Directory Library*, *Gale Directory of Databases*, *Directories in Print*, *Gale Directory of Publications and Broadcast Media*, *Encyclopedia of Associations*, and *Encyclopedia of Business Information Sources*.

Gale Directory Library

The *Gale Directory Library* provides online access to some of Gale's most popular directories on companies, publishers, associations, and so on. It includes online access to *Gale Directory of Databases*, *Gale Directories in Print, Gale Directory of Publications and Broadcast Media*, *Encyclopedia of Associations*, *Encyclopedia of Business Information Sources*.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Users can use *Gale Directory Library* to find contacts, companies, individuals, or publications by searching with a name or keyword; generate lists and analyze trends by exporting data to Word or Excel; and search across a growing number of directory titles. Each directory can be searched individually by its own unique data fields, or the entire directory collection can be searched.

Gale Directory of Databases

The *Gale Directory of Databases* is a directory that provides detailed descriptions of thousands of publicly available databases, database products, online services, and database vendors and distributors worldwide in a variety of formats.

The directory's detailed listings provide complete information on databases, producers, and vendors. Database listings include content and subject coverage, type, language, time span, update frequency, geographic coverage, producer contact information, and vendor availability. The directory's producer and vendor entries feature full contact information, including address, phone, fax, website addresses, email addresses, former names, branch office locations, and a list of available databases and products. For online vendors (or hosts), entries cover conditions of access, networks used, and gateway access. The *Directory of Databases* is also available on the *Gale Directory Library*.

Directories in Print

The *Directories in Print* publication describes and indexes thousands of directories of all kinds, including business and industrial directories, professional and scientific rosters, foreign directories, and other lists and guides. The *Directories in Print* covers a wide range of subjects, including general business; manufacturing industries and commercial services; banking, insurance, and financial services; advertising, marketing, and public relations; health care services; law, military, and government; and associations, philanthropy, ethnic groups, and religion. The *Directories in Print* is available online on the *Gale Directory Library*.

Gale Directory of Publications and Broadcast Media

The *Gale Directory of Publications and Broadcast Media* is a directory containing information on thousands of radio and television stations, cable companies, and print-media publishers. Its entries provide addresses, phone and fax numbers, email addresses, website addresses, key personnel, owner information, hours of operation, and much more. Providing access to information on U.S., Canadian, and international media outlets, *Gale Directory of Publications*

and Broadcast Media also includes ad rates, circulation statistics, local programming information, and other data. The *Directory of Publications and Broadcast Media* is available online on the *Gale Directory Library*.

Encyclopedia of Associations

Gale publishes a series of Encyclopedia of Associations in regional, national, and international editions. It publishes the *Encyclopedia of Associations: National Organizations of the U.S.*, which lists each chartered public and private association in the United States and provides valuable information about each association's officers and purpose. In addition, Gale publishes the *Encyclopedia of Associations: International Organizations* and the *Encyclopedia of Associations: Regional, State, and Local*. These encyclopedias can be found online on the *Gale Directory Library*.

Encyclopedia of Business Information Sources

The *Encyclopedia of Business Information Sources* is a bibliographic guide to live, print, and electronic sources of information covering more than 1,000 subjects of interest to business professionals. Its citations cover abstracts and indexes, almanacs and yearbooks, bibliographies, CD-ROM and online databases, directories, encyclopedias and dictionaries, periodicals and newspapers, research centers and institutes, statistic sources, trade and professional societies, and many other sources of business information. *The Encyclopedia of Business Information Sources* is available online on the *Gale Directory Library*.

SEC Filings

EDGAR

EDGAR (Electronic Data Gathering, Analysis, and Retrieval) is a system that collects documents submitted by companies and others who are required by law to file with the Securities and Exchange Commission (SEC). EDGAR performs automated collection, validation, indexing, acceptance, and forwarding of SEC filings. Its primary purpose is to increase the efficiency and fairness of the securities market to benefit investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the SEC.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Not all documents that public companies file with the SEC, however, will be available on EDGAR. Even so, several important documents, such as Form 10-K or 10-KSB, are required to be filed on the EDGAR system. For more information, visit www.sec.gov/edgar.shtml.

Factiva

Factiva, from Dow Jones, is an information and research tool tailored for business and financial news searches that maintains a catalog of the world's leading news and business sources from many countries and in numerous languages.

Foreign Representatives in the U.S. Yellow Book

This directory has names and titles of thousands of executives and officials who manage the leading non-U.S. organizations, and it contains information on corporations, financial institutions, foreign nations, intergovernmental organizations, foreign press, and law firms.

Index to Legal Periodicals

Published by H. W. Wilson, the *Index to Legal Periodicals* offers international coverage and access to scholarly articles, symposia, jurisdictional surveys, court decisions, legislation, books, book reviews, and more. This source indexes about 1000 legal journals, law reviews, yearbooks, institutes, statutes, bar association publications, university publications, and governmental publications.

IHS Fairplay

IHS Fairplay, formerly Lloyd's Register—Fairplay, supplies a range of comprehensive shipping databases, maritime information, registers, online information, and a tailored research and system-development service for customers' specific needs. This resource can also be used to find the details of a ship, including what cargo it can carry and who owns it.

Magazines for Libraries

Magazines for Libraries lists almost every magazine (general, technical, and scholarly) that a library might wish to stock and describes the formats in which the magazines are available.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Martindale-Hubbell Law Directory

The Martindale-Hubbell Law Directory contains biographical information on most lawyers and law firms practicing in the United States, Canada, and 160 other countries.

Mergent

Mergent, like D&B, is a business and financial information service provider. Mergent's reports can provide information about firms listed on the New York and American stock exchanges, as well as companies listed on regional American exchanges. Mergent also provides Mergent Online, which offers Internet-based access to Mergent's comprehensive global database.

Mergent's Bank and Finance Manual and News Reports

Mergent's Bank and Finance Manual and News Reports is a business and financial information resource containing information on nearly 2,000 corporations. It covers the field of finance represented by banks, insurance companies, investment companies, unit investment trusts, and miscellaneous financial enterprises. It also includes information on real estate companies and real estate investment trusts. Additionally, it provides other relevant facts and figures, including information on corporations' auditors, general counsel, exchange and symbol, number of employees, number of shareholders, address, telephone and fax numbers, shareholder-relations contact, stock-price ranges, dividends, report of independent auditors, transfer agents, stock splits, and annual meeting date.

Mergent's Bank and Finance News Reports are published each month in print and each week online, and these reports contain material that updates *Mergent's Bank and Finance Manual.* The reports include news items, interim financial statements, personnel changes, new company descriptions, merger proposals, details about new debts and stock issues, security offerings, announcements of new financing, and call notices.

Reader's Guide to Periodical Literature

The *Reader's Guide* is a reference guide to articles published in periodicals and scholarly journals. The guide contains a full dictionary catalog of all articles by author, subject, and title, where possible. The entries refer to the volume, number of the periodical, starting and inclusive pages of the article, date of publication, and graphic material in the article, such as portraits. There is an electronic retrospective version of the guide available for 1890 to 1982.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Standard & Poor's NetAdvantage

NetAdvantage is a subscription-based service provided by Standard & Poor's. It is a comprehensive source of business and investment information, offering online access to Standard & Poor's independent research, data, and commentary on stocks, bonds, funds, and industries. This service also includes export tools to enable researches to download data into spreadsheet programs for further analysis. Some of NetAdvantage's premium publications include:

- The Corporation Records
- The Company Profile
- The Register of Corporations, Directors, and Executives
- The Register of Public Companies
- The Register of Private Companies
- Security Dealers of North America

Corporation Records

The Corporation Records directory has information on thousands of public companies. Each listing includes various types of information, including company background, stock and bond descriptions, balance sheet and earnings information, officers and directors, capital expenditures, subsidiaries, and more.

Company Profile

NetAdvantage also publishes a comprehensive company profile for thousands of publicly traded companies. Each profile includes a business description, an interactive charting tool, statistics, analyst ratings, valuation and financial information, as well as the latest stock price quote, company news, and information on competitors.

Register of Corporations, Directors, and Executives

The Register of Corporations, Directors, and Executives gives short summaries about corporate executives and directors, including their titles, the name of the company they work for, their academic credentials, membership in fraternal organizations, and available business and residential contact information.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Register of Public Companies

The Register of Public Companies provides brief descriptions of publicly traded companies, including stock symbol, total annual sales, number of employees, officer names, and North American Industry Classification System (NAICS) assignments.

Register of Private Companies

The Register of Private Companies provides information on thousands of private companies, including (when available) their address, telephone number, officers and directors, total annual sales, number of employees, line of business, primary and secondary NAICS classifications, principal bank, law firm, accounting firm, and more.

Security Dealers of North America

The Security Dealers of North America is a listing of North American securities dealers, providing a brief description of each dealer's business; a listing of the states in which it is registered to do business; the location of its main office; the names of its officers, clearing firm, associations, and memberships; and the number of employees and registered representatives it employs.

The Global Banking Resource

The Global Banking Resource (TGBR) is a comprehensive database of financial institutions, and it provides data on financial institutions' contacts, correspondents, subsidiaries, affiliates, financial information, payment information, and much more.

Banks and Financial Institutions

Types of Financial Records

As a general rule, financial information is private and can be obtained only by legal process or consent. If you are able to obtain financial records, the following financial information should be requested.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

Account Holder Records

The relationship between banks and their customers is confidential. Generally, information from banks can be obtained only by subpoena or other legal process. Requested records and the information they provide could include:

- The master file of customers
- Safe deposit box records
- Account opening records

MASTER FILES OF CUSTOMERS

The master files of customers (e.g., depositors, debtors, and safe deposit box holders) that are maintained by most banks should detail where all of its important records are stored.

SAFE DEPOSIT BOX RECORDS

Safe deposit box records usually provide the name(s) of the person(s) renting the box, how often a person visited it, the dates he visited it, and the times he visited it. The times and frequency of visits can be valuable if they correspond to times and dates of deposits or withdrawals from other accounts.

Banks usually require the customer's consent, a search warrant, or a court order before an authorized bank official can open a safe deposit box.

ACCOUNT OPENING RECORDS

To open a financial account, an individual or business must provide certain information, and the records of such information can also be valuable. The account opening records for a personal account might contain handwriting samples and personal information about account holders, varying from one bank to another. But typically, the account opening records for a personal account contain the account holder's name, address, telephone number, tax identification number, amount of the account's opening deposit, and security data.

Account Statements

Account statements, which are provided for all types of financial accounts, provide summaries of all the transactions on their corresponding accounts, and they contain information about the account holder and the financial institution in which the account is held (i.e., names and addresses). In short, account statements summarize the account

holder's financial activity (e.g., cashed checks, withdrawals, and deposits) for a specific period (usually a month).

Wire Transfer Records

Records of wire transfers—electronic transfers of money from one bank to another—can contain valuable information. Typically, transfer records identify who sent the wire, when and where it was sent, and its amount.

Financial Intelligence Unit Documents and Reports

Financial regulations and legislation obliges banks and other financial institutions to file reports detailing large cash transactions or suspicious activity with Financial Intelligence Units (FIUs), which are centers that collect information on suspicious or unusual financial activity.

Typically, reports filed with FIUs contain, among other things, the identity of the persons making the transactions and the amount of the transactions. In addition, they can provide valuable information that can be used to:

- Identify illegal activity.
- Detect the flow of illicit funds.
- Identify leads to assets purchased with ill-gotten gains.

International Financial Bodies

Society for Worldwide Interbank Financial Telecommunication

International transfers by financial institutions are generally conducted through the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Headquartered in Belgium, SWIFT was established in 1973.

Generally, SWIFT is not considered to be an electronic funds-transfer system such as Fedwire and CHIPS in the United States, but rather a specialized international cooperative communication service. As opposed to directly facilitating transactions, SWIFT sends payment orders to financial institutions, which then settle the transactions with correspondent accounts. A correspondent account is an arrangement in which one bank maintains a correspondent account at another bank for the purposes of settling transactions for itself or for its customers.

APPENDIX D

ADDITIONAL INFORMATION SOURCES

SWIFT acts as the gatekeeper to the records on these international financial transactions. However, access to this information can be difficult, given the high emphasis on privacy laws in the European Union. Even law enforcement agencies are restricted in many situations.

Many countries, especially in Europe and the Middle East, use International Banking Account Numbers (IBAN), which is an international format for banking account numbers designed to avoid confusion in international transactions. SWIFT is the official registrar of IBAN numbers. U.S. banks will be listed under an American Bankers Association (ABA) code.

International Law Enforcement Organizations

International Criminal Police Organization

The International Criminal Police Organization, better known by its radio designation as INTERPOL, is a network of National Central Bureaus in 190 member countries that share information with each other to assist law enforcement agencies in the detection and deterrence of international crime. Each bureau is an agency of the member country's government and serves as the liaison between that country's law enforcement agencies and the INTERPOL network.

To support ongoing investigations that require international assistance, INTERPOL provides information regarding:

- Location of suspects/fugitives/witnesses
- International wanted circulars
- Criminal history
- Terrorism prevention
- Stolen art
- Tracing of weapons and motor vehicles abroad
- License plate, driver's license records, and vehicle registration data

INTERPOL bureaus typically have case tracking systems that contain information about people, property, and organizations involved in international criminal activity. They can

determine the history of an international connection in an investigation or the existence of any previous international criminal activity.

While INTERPOL is a network of law enforcement agencies, it also may work with private financial institutions during international investigations. Not every country participates in INTERPOL, and those that do have varying levels of international coordination. Therefore, fraud examiners might need to take a more direct approach to working with foreign law enforcement officials.

International Chamber of Commerce Commercial Crime Bureau

The International Chamber of Commerce (ICC) established the Commercial Crime Bureau (CCB) in January 1992 to act as a focal point for fraud prevention and to encourage cooperation between commerce and law enforcement agencies. The CCB maintains an extensive database on all aspects of commercial fraud. The CCS also operates Fraudnet, a unique global network of law firms that specialize in tackling business crime.

World Criminal Justice Library Network

The World Criminal Justice Library Network (WCJLN) is a network that is used to share services and information concerning criminal justice. The group has developed an international network to disseminate national and international crime statistics and criminal justice profiles.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Following are two forms of fraud examination reports.

The first is a *short-form report* that summarizes the issues presented, the steps taken, and the information found.

The second sample is a *long-form report* that contains the substantive work produced during the fraud examination, including copies of relevant documents and memoranda of witness interviews.

MENU

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

SHORT-FORM REPORT

TO: **HAL B. MARLOW**
CHIEF EXECUTIVE OFFICER

FROM: **LOREN D. BRIDGES**
CERTIFIED FRAUD EXAMINER

RE: **EXAMINATION OF POTENTIAL ASSET MISAPPROPRIATION**

DATE: **MAY 23, 2015**

I. Background

On January 28, 2015, the fraud examination unit at Bailey Books received an anonymous telephone call on its fraud hotline from an unidentified man who claimed that he was a former supplier to Bailey. The caller alleged certain improprieties in the bidding and procurement process.

Based upon this initial predication, a fraud examination was conducted, which included reviews of relevant records and interviews of appropriate personnel.

II. Executive Summary

The fraud examination commenced when Loren D. Bridges, CFE, received a telephone call from an unidentified man who said that he had been a long-term supplier to Bailey for sundry office supplies and paper. The caller said that ever since Linda Reed Collins had taken over as Purchasing Manager, he had been gradually "squeezed out" from doing business with Bailey.

Linda Reed Collins has been employed in the purchasing department of Bailey Books since June 1, 2010. She was promoted to Purchasing Manager effective November 8, 2012.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

The fraud examination team reviewed selected purchases from 2012 to 2014 and conducted interviews of key participants and Bailey employees who we believed may have information regarding the misappropriation of assets. The team reviewed purchasing guidelines, personnel files of interviewees, and various financial documents relating to both Bailey Books and Linda Reed Collins.

After obtaining sufficient documentation, the team interviewed Linda Reed Collins, who gave a full signed confession to her misdeeds.

III. Scope

The objective of the fraud examination team was as follows:

- Determine the existence of a possible misappropriation of assets of Bailey Books, Incorporated. The examination is predicated upon an anonymous telephone call alleging improprieties on the part of Linda Reed Collins, Bailey's purchasing manager.

IV. Approach

Fraud Examination Team Members: Loren D. Bridges, CFE, Bailey Books; Tonya Vincent, CFE, Bailey Books

Procedures: As part of the examination of this matter, the team took the following actions:

- Obtained, reviewed, and analyzed memoranda pertaining to the anonymous call described previously.
- Obtained, reviewed, and analyzed Bailey Books' financial documentation, including purchase records, invoices, and canceled checks.
- Obtained, reviewed, and analyzed records from the St. Augustine County Courthouse regarding civil actions in which Edward J. Collins and Linda Reed Collins were named; records from the Florida Secretary of State's Office regarding Collins Marine Corporation; records of chattel mortgages held by Linda Reed Collins and Edward J. Collins; financial records from Dun & Bradstreet regarding Collins Marine Corporation; and public records regarding the financial condition of Linda Reed Collins and Edward J. Collins.
- Conducted surveillance activity in order to determine whether the two key individuals in the matter were involved in an illicit relationship.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Individuals Interviewed: The following individuals were interviewed in person by members of the fraud examination team:

- Mark W. Steinberg, CPA (Chief Financial Officer, Bailey Books)
- Roger Donald McGuire (Purchasing Agent, Bailey Books)
- Mary Rodriguez De La Garza (Purchasing Agent, Bailey Books)
- Sara Louise Dawson (Former Employee, Bailey Books)
- Thomas C. Green (Attorney, Sharp, Green and Langfrom, P.A.)
- Lincoln S. Wyzokowski (General Counsel, Bailey Books)
- Becky Robinson (Accounts Payable Clerk, Bailey Books)
- Ernie Quincy (Warehouse Manager, Bailey Books)
- David Levey (Director of Sales, Jerrico International Paper Company)
- James R. Nagel (Sales Representative, Orion Corporation)
- Owen Stetford (Chief Financial Officer, Orion Corporation)
- Linda Reed Collins (Purchasing Manager, Bailey Books)

V. Findings

Based on the documents reviewed, information collected, and interviews conducted during the course of the fraud examination, the team finds as follows:

- Did the fraud examination team determine the existence of a possible misappropriation of assets of Bailey Books Incorporated?

Yes. The documents and information reviewed and interviews conducted by the fraud examination team during the course of the examination indicate that Linda Reed Collins, together with James R. Nagel, did knowingly embezzle approximately $197,773 from Bailey Books over four years. During the fraud examination, the team analyzed financial documents and conducted interviews to corroborate the statements of an anonymous caller. The following is a summary of the evidence and information supporting the fraud examination team's findings:

On January 28, 2015, an anonymous call was received by the fraud hotline at Bailey Books, Incorporated, from a former supplier to Bailey Books. The caller alleged that after Linda Reed Collins took over as Purchasing Manager in 2012, she eliminated him as a supplier. A subsequent review of purchases made by Bailey Books from 2012 to 2014 showed that a

continuously increasing share of the company's paper business was being given to Orion Corp., even though Orion submitted written bids in only 63 percent of the cases.

On February 1, 2015, Mark W. Steinberg, CFO of Bailey Books, Inc., was interviewed. The purpose of the interview was to inform him of the proposed fraud examination, obtain his approval, and secure information from him regarding the purchasing process at Bailey Books. In addition to summarizing his responsibilities regarding purchasing at Bailey Books, Mr. Steinberg stated that in December 2012 he sent a memo to all the division heads at Bailey Books informing them that all purchases over $50,000 would from then on require at least three written bids.

We next examined the personnel records. A review of Linda Reed Collins's file showed only that she had been consistently rated "exceptional" by her supervisors in annual reviews.

On February 4, 2015, an interview was conducted with Roger Donald McGuire, purchasing agent at Bailey Books. After summarizing the purchasing process at Bailey Books, he stated that he had no knowledge of any improprieties committed by Ms. Collins.

The next interview conducted was with Mary Rodriguez De La Garza, a coworker of Ms. Collins's in the Purchasing Department at Bailey Books. During the interview, Ms. De La Garza stated that, regarding the purchasing process, it is sometimes not practical to obtain bids, such as in emergency situations or when they are short on time. She went on to reveal that she had suspected Ms. Collins was having an affair with James R. Nagel, the salesperson for Orion Corp. In addition, Ms. De La Garza said she believed that Ms. Collins and her husband were having marital and financial problems. She also mentioned that Sara Louise Dawson, a former employee under Ms. Collins, had left on bad terms.

The next interview was with Sara Louise Dawson, who wanted to consult with her attorney before making an official statement. Ms. Dawson's attorney, Thomas C. Green, later contacted the fraud examination team to let them know that Ms. Dawson was interested in making a statement, but only in exchange for an indemnity against all claims arising out of her cooperation. After meeting with Mark Steinberg and Lincoln S. Wyzokowski, General Counsel at Bailey Books, Ms. Dawson and Mr. Green's proposal was accepted.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

On March 3, 2015, Ms. Dawson made her statement, which included the following:

- After Ms. Collins was promoted to Purchasing Manager, she began favoring Orion Corp. for paper purchases.
- On two occasions in 2014, Ms. Collins authorized prepayment on substantial purchases from Orion, even though Ms. Dawson had complained about Orion's poor quality and service. Later Ms. Dawson found out that the orders were never received.
- Other vendors had complained of being squeezed out of business with Bailey Books after Ms. Collins became manager.

Ms. Dawson referred the team to Becky Robinson in the Accounts Payable Department for further information about the orders. Ms. Robinson was interviewed and provided copies of the two prepaid invoices to Orion Corp., the amounts of which were $102,136 and $95,637. In addition, Ms. Robinson said that Ernie Quincy in the Receiving Department would be able to verify if the two shipments had ever been received.

On April 8, 2015, Ernie Quincy, the Warehouse Manager at Bailey Books, was interviewed and verified that the two shipments in question were never received. The next day, copies of the two checks given to Orion Corp. for payment of the goods that were never received were examined.

An interview with David Levey from Jerrico International Paper Company yielded the following information:

- At the time Levey began at Jerrico, Bailey Books was a major customer of theirs, but since then their sales to Bailey had dwindled.
- Levey attempted to revive business with Bailey Books, but by then rumors were circulating about an inappropriate relationship between Mr. Nagel of Orion Corp. and Ms. Collins.
- According to Levey, Mr. Nagel had a "bad reputation" in the industry.

Ms. De La Garza phoned the team on April 13, 2015, to let them know that Ms. Collins had plans to meet Mr. Nagel at the bar at the Hotel Atlantic that afternoon. The team set up surveillance of their meeting and reported that Ms. Collins and Mr. Nagel met at 5:55 p.m. and ordered drinks. They held hands under the table, kissed, and left the bar at 7:02 p.m. to go to room 652.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

A review of St. Augustine County records showed that Edward J. Collins (Ms. Collins's husband) was a defendant in three civil actions. The circumstances of the actions indicated that the Collinses were having financial troubles.

A review of the Florida Secretary of State's records showed that the Collinses were the incorporators of Collins Marine Corporation.

A review of UCC filings showed that the Collinses had three liens in their name.

A net-worth analysis was performed on the Collinses based on information assembled from public records. It showed unexplained income of $31,632.

In an April 19, 2015 interview, Mr. Nagel stated that his relationship with Ms. Collins was purely professional and denied any improprieties regarding Orion's business with Bailey Books. Mr. Nagel also refused to provide any of Orion's financial information pertaining to the two invoices in question.

On April 21, 2015, Owen Stetford, the CFO of Orion Corp., was interviewed and stated he was unable to provide any copies of actual financial information, but that Orion had no record of any receipt of payment for the invoices in question, nor any record that such orders had been placed or shipped. In addition, Mr. Stetford said that Orion had no corporate accounts at Florida Marine National Bank, the bank at which the checks from Bailey Books were deposited. Mr. Stetford also stated that the correct corporate name is Orion Corporation, not Orion Paper Company, as the endorsements indicated.

On May 1, 2015, Mr. Nagel was again interviewed. After being confronted with questions and evidence regarding the two payments and the bank account to which they were deposited, Mr. Nagel voluntarily gave a statement attesting to his involvement with Ms. Collins in the embezzlement of funds from Bailey Books. He attested to the following:

- In 2014, Ms. Collins told Mr. Nagel that she would approve the payment of invoices to Orion Corp. for product that would not be delivered. Ms. Collins authorized the payment of two invoices in the amounts of $102,136 and $95,637, but no product was shipped on the invoices. Ms. Collins and Mr. Nagel established a bank account in the name of Orion Paper Company at Florida Marine National Bank and divided the proceeds of the invoices equally.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

On May 1, 2015, Ms. Collins voluntarily gave a statement, which included the following:

- Ms. Collins stated that, starting in 2013, she accepted money from Mr. Nagel to ensure that Orion Corp. received preferential treatment in supplying Bailey Books with stationery and paper products. On those occasions, she was aware that Bailey Books was not obtaining the best product at the lowest possible price from Orion; in other words, the price charged for the products was substantially higher than market value.
- Ms. Collins stated that on two occasions in 2014, she authorized the payment of invoices for $102,136 and $95,637 without any receipt of merchandise.
- Ms. Collins estimated that she received in excess of $150,000 in connection with Mr. Nagel.

VI. Summary

This report reflects that Linda Reed Collins, a purchasing agent for Bailey Books, Inc., furnished a signed statement on May 1, 2015, indicating she had accepted at least $197,773 in commercial bribes and other illicit income in a conspiracy with James R. Nagel, an account representative for Orion Corporation, St. Augustine, Florida.

The statements made by Collins are corroborated by the documentary evidence and the interviews of other witnesses as described herein.

VII. Impact to Bailey Books

Over the course of four years, Linda Reed Collins, in partnership with James R. Nagel, misappropriated an estimated $197,773 from Bailey Books, Incorporated.

Additional amounts were lost due to Bailey's overpaying for merchandise sold to it by Nagel. Those amounts have not been calculated.

VIII. Recommendations

It is the policy of Bailey Books to report such matters to the appropriate authorities and to assist in criminal prosecution. A full review of internal controls should be conducted to determine how such incidents can be detected in the future.

MENU

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

LONG-FORM REPORT

Bailey Books, Incorporated

6200 Bayshore Drive
St. Augustine, FL 32082

Personal and Confidential

May 23, 2015

Lt. Jason Fishbeck
St. Augustine Police Department
382 Harbor View Circle
St. Augustine, FL 32084

Re: Linda Reed Collins (File 08-4422)

Dear Lt. Fishbeck:

Attached is my report of a fraud examination dated May 23, 2015, with respect to the above captioned matter.

The report reflects that Collins, a purchasing agent for Bailey Books, Inc., furnished a signed statement on May 1, 2015, indicating she had accepted at least $197,773 in commercial bribes and other illicit income in a conspiracy with James R. Nagel, an account representative for Orion Corporation, St. Augustine. Orion is a supplier of paper and related products to Bailey Books.

If proved in judicial proceedings, Collins and Nagel could be in violation of Title 7, Section 323A of the Florida Criminal Code (Commercial Bribery).

It is the policy of Bailey Books to report such matters to the appropriate authorities, and to assist in criminal prosecution. Accordingly, we would be willing to supply assistance, documentation, and expertise to your department in the resolution of this case.

If I might be of assistance, please do not hesitate to call.

Sincerely,

Loren D. Bridges
Certified Fraud Examiner

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

6200 Bayshore Drive
St. Augustine, FL 32082

Personal and Confidential

May 23, 2015

Mr. Hal B. Marlow
Chief Executive Officer
Bailey Books Incorporated
6200 Bayshore Drive
St. Augustine, FL 32082

Re: Linda Reed Collins

Dear Mr. Marlow:

We have conducted a fraud examination concerning a possible misappropriation of assets of Bailey Books, Incorporated. This examination was predicated upon an anonymous telephone call alleging improprieties on the part of Linda Reed Collins, Bailey's purchasing manager.

Our examination was conducted in accordance with lawful fraud examination techniques, which include—but are not limited to—examination of books and records, voluntary interviews with appropriate personnel, and other such evidence-gathering procedures as necessary under the circumstances.

During the pendency of this examination, Ms. Collins and her confederate, James R. Nagel of Orion Corporation, voluntarily furnished signed statements indicating that they misappropriated at least $197,773 to their personal benefit.

Based upon the results of our examination and the confessions of Ms. Collins and Mr. Nagel, these actions, if proved in a court of law, could constitute a violation of criminal and/or civil law.

Very truly yours,

Loren D. Bridges
Certified Fraud Examiner

MENU

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

EXECUTIVE SUMMARY

CONFIDENTIAL

Linda Reed Collins has been employed in the Purchasing Department of Bailey Books since June 1, 2010. She was promoted to purchasing manager effective November 8, 2012.

On January 28, 2015, the fraud examination unit at Bailey Books received an anonymous telephone call from an unidentified man who claimed that he was a former supplier to Bailey. The caller alleged certain improprieties in the bidding and procurement process.

Based upon this initial predication, a fraud examination was conducted, which included reviews of relevant records and interviews of appropriate personnel. The fraud examination revealed multiple purchases by Bailey Books from Orion Corporation, the amount of which has increased significantly from 2012 to the present.

Interviews of Bailey personnel indicated that Ms. Collins might have a personal relationship with Mr. Nagel, an account representative of Orion Corporation. On May 1, 2015, Nagel and Collins were interviewed. Both furnished voluntary signed statements indicating that they had appropriated at least $197,773 from Bailey by establishing a fictitious vendor to which Bailey's checks were directed. The checks purported to be for supplies purchased by Bailey when, in fact, no supplies or other items were purchased for this amount. Nagel and Collins used the proceeds for their personal benefit.

As reflected by the attached letter dated May 23, 2015, based on all the evidence, Collins and Nagel could be in violation of Florida criminal and/or civil laws.

Loren D. Bridges
Certified Fraud Examiner

MENU

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

INDEX TO REPORT

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMO OF PREDICATION

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: ANONYMOUS TELEPHONE CALL
DATE: JANUARY 28, 2015

On January 28, 2015, at approximately 10:12 a.m., I received a telephone call from an unidentified man who said that he had been a long-term supplier to Bailey for sundry office supplies and paper.

The caller—who refused to reveal his identity—said that ever since Linda Reed Collins had taken over as purchasing manager, he had been gradually "squeezed out" from doing business with Bailey. The caller declined to furnish additional information.

Based on the predication supplied above, a fraud examination is being commenced.

(Page 1)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF SELECTED PURCHASES FROM 2012 to 2014
DATE: JANUARY 30, 2015

Attached is a schedule of purchases prepared from individual vendor files. The purchases reflect that Orion Corp. has received an increasing share of the paper business from Bailey over the last several years, but has submitted written bids in only 63 percent of the cases over that period.

(Page 2)

Bailey Books, Incorporated

Selected Purchases 2012–2014

Vendor	Items Purchased	Purchaser	2012	2013	2014	Date of Last Bid	% Increase (Decrease) Previous Yr. 2013–2014	% Increase (Decrease) Previous Yr. 2012–2013	% Increase (Decrease) Previous 2 Yrs. 2012–2014
Armour	Books	MRD	$683,409	$702,929	$810,100	12/01/14	15.2%	2.9%	18.5%
Burdick	Sundries	LRC	62,443	70,959	76,722	N/A	8.1%	13.6%	22.9%
Canon	Magazines	MRD	1,404,360	1,957,601	2,361,149	11/03/14	20.6%	39.4%	68.1%
DeBois, Inc.	Paper	LRC	321,644	218,404	121,986	06/08/14	(44.1%)	(32.1%)	(62.1%)
Elton Books	Books	RDM	874,893	781,602	649,188	07/21/14	(16.9%)	(10.7%)	(25.8%)
Fergeson	Books	RDM	921,666	1,021,440	1,567,811	09/08/14	53.5%	10.8%	70.1%
Guyford	Magazines	MRD	2,377,821	2,868,988	3,262,490	10/08/14	13.7%	20.7%	37.2%
Hyman, Inc.	Supplies	LRC	31,640	40,022	46,911	10/22/14	17.2%	26.5%	48.3%
Intertec	Books	RDM	821,904	898,683	959,604	11/18/14	6.8%	9.3%	16.8%
Jerrico	Paper	LRC	486,401	111,923	93,499	08/04/14	(16.5%)	(77.0%)	(80.8%)
Julian-Borg	Magazines	MRD	431,470	589,182	371,920	02/07/14	(36.9%)	36.6%	(13.8%)
King Features	Magazines	MRD	436,820	492,687	504,360	11/18/14	2.4%	12.8%	15.5%
Lycorp	Sundries	LRC	16,280	17,404	21,410	N/A	23.0%	6.9%	31.5%
Medallian	Books	RDM	---	61,227	410,163	12/15/14	569.9%	---	---
Northwood	Books	RDM	861,382	992,121	---	12/07/12	---	15.2%	(100.0%)
Orion Corp.	Paper	LRC	86,904	416,777	803,493	11/02/13	92.8%	379.6%	824.6%
Peterson	Supplies	LRC	114,623	---	---	N/A	---	---	---
Quick	Supplies	LRC	---	96,732	110,441	11/03/14	14.2%	---	---
Robertson	Books	RDM	2,361,912	3,040,319	3,516,811	12/01/14	15.7%	28.7%	48.9%
Steele	Magazines	MRD	621,490	823,707	482,082	11/03/14	(41.5%)	32.5%	(22.4%)
Telecom	Sundries	LRC	81,406	101,193	146,316	N/A	44.6%	24.3%	79.7%
Union Bay	Books	RDM	4,322,639	4,971,682	5,368,114	12/03/14	8.0%	15.0%	24.2%
Victory	Magazines	MRD	123,844	141,909	143,286	06/09/14	1.0%	14.6%	15.7%
Williams	Sundries	LRC	31,629	35,111	42,686	N/A	21.6%	11.0%	35.0%

(Page 3)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF MARK W. STEINBERG, CPA
CHIEF FINANCIAL OFFICER
DATE: FEBRUARY 1, 2014

Mark W. Steinberg, CPA, chief financial officer of Bailey Books, was interviewed in his office, Room 836, 6200 Bayshore, St. Augustine, Florida. The purpose of the meeting was to advise Mr. Steinberg of the proposed fraud examination, to obtain his approval of the proposed plan, and to secure basic information from him on the purchasing function.

Mr. Steinberg was advised of the nature of the anonymous allegations and the result of our initial vendor review. He was also informed of our plan to review personnel files and other internal company documents and to discreetly interview selected company personnel. He agreed to the above, asking that we conduct our examination quickly and in the least disruptive manner possible. He agreed that Ms. Collins and the Purchasing Department would not be notified of the examination until decided otherwise.

Mr. Steinberg has been with Bailey Books, Incorporated since 1998. Previously, he was assistant vice president for financial affairs from 1998 to 2006. He reports directly to Mr. Hal B. Marlow, president of the company.

As CFO, all operating divisions, including purchasing, report to him. It is his responsibility to establish and supervise the monitoring of internal controls within the operating divisions. In general, Bailey follows the policy of obtaining bids on as many purchases as possible. He pointed out that the competitive nature of the retail book industry requires constantly obtaining the maximum product for the minimum cost. He has reiterated to managers on many occasions the necessity of cutting costs.

Guidelines for purchasing procedures are set forth in Mr. Steinberg's memorandum to all division heads and supervisors dated December 12, 2012. The memo calls for purchasers to obtain bids on all purchases of more than $50,000. However, purchases of more than $10,000 generally are expected to be bid unless a justifiable reason not to exists. A copy of the memo was provided by Mr. Steinberg, and is attached. The copy provided has been initialed and dated and is maintained in the evidence file, Room 874, Bailey Books.

(Page 4)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: LINDA REED COLLINS, PURCHASING MANAGER
FROM: MARK W. STEINBERG, CHIEF FINANCIAL OFFICER
SUBJECT: PURCHASING GUIDELINES
DATE: DECEMBER 12, 2012

The purpose of this memo is to establish guidelines for major purchases.

Effective at once, purchasing will obtain at least three written bids for items of more than $50,000, in all cases. Bids should also be obtained for purchase amounts of $10,000 and above, where practical.

These bids should be maintained in the file for documentation purposes.

If the lowest bid is not selected, a memo of justification should be prepared and approved by me before any purchase is made. You are to be especially concerned with miscellaneous and sundry items, because these items are not price competitive.

Any deviations from the above-stated policy must be approved by me.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF PERSONNEL FILES
DATE: FEBRUARY 4, 2015

Francis Morris, personnel manager, provided the personnel files of Linda Reed Collins, Mary Rodriguez De La Garza, and Roger McGuire for review. Pertinent data included:

Mary Rodriguez De La Garza:

Sept. 15, 2010	Mary Rodriguez De La Garza hired as administrative assistant at annual salary of $20,000
Sept. 14, 2011	Merit salary increase to $22,000 annual
Sept. 17, 2012	Merit salary increase to $24,500 annual
Aug. 2, 2013	Transferred and promoted to purchasing agent at salary of $27,000
Aug. 4, 2014	Merit salary increase to $30,000 annual

Roger McGuire:

Feb. 20, 2011	Roger Donald McGuire hired as purchasing agent at salary of $28,000
Feb. 22, 2013	Merit salary increase to $31,000 annual

Linda Reed Collins:

June 1, 2010	Linda Reed Collins hired as purchasing agent at salary of $28,500
June 3, 2011	Merit salary increase to $31,250 plus participation in incentive plan
Nov. 8, 2012	Promoted to purchasing manager, salary increase to $36,000 annual, plus incentives
Nov. 10, 2013	Merit salary to $39,500 annual plus incentives
Nov. 11, 2014	Merit salary to $43,000 annual plus incentives

The personnel file reflected that Ms. Collins was consistently rated as "exceptional" by her supervisors in annual reviews. She has executed annual Conflict of Interest Questionnaires for 2010 through 2014 indicating that she and her spouse, Edward Collins, had no outside employment, investments, or interests with companies doing business with Bailey Books.

The file contained a copy of IRS form 668-W, Notice of Levy on Wages, Salary, and Other Income, dated June 2011, indicating that Ms. Collins and her spouse owed federal taxes of $53,219.09. An IRS Release of Levy, indicating that the amount due had been paid in full, was filed December 18, 2014.

(Page 6)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF ROGER DONALD MCGUIRE
DATE: FEBRUARY 4, 2015

Roger Donald McGuire, purchasing agent, Bailey Books, was interviewed at his office, Room 537, 6200 Bayshore, St. Augustine, Florida. After being advised of the identity of the interviewer and the nature of the inquiry, McGuire voluntarily provided the following information.

He has been employed by Bailey Books since 2011. He is a purchasing agent whose function is to purchase the book inventory. Purchasing policy guidelines require him to obtain bids for all purchases of more than $50,000. He said that bids are submitted in substantially all of his purchases of books, and that he estimates somewhere between 80 percent and 90 percent of his purchases are preceded by bids.

Whenever he deviates from selecting the low bidder for a product, he writes a memo of justification to the file with approval from his manager. This does not happen on many occasions. The reasons for not obtaining bids for products include (1) emergency purchases; (2) sole-source purchases; and (3) time pressures. McGuire is aware that the other purchases, made by Mary Rodriguez De La Garza and Linda Reed Collins, are made under the same guidelines.

He is not aware of favoritism regarding vendors. McGuire has received pressure from various vendors from time to time. Examples include "the hard sell" that many vendors try with purchasing agents and occasional efforts by the vendors to get paid early so they can earn and collect their commissions. Every now and then, a vendor will attempt to give him a gratuity, such as a free case of liquor or a small gift. However, McGuire says he avoids any ties to the vendor, as such are prohibited by Bailey's employee guidelines.

He is unaware of any other purchasing employees making any exceptions to purchasing policy. McGuire thinks a great deal of his coworkers Mary Rodriguez De La Garza and Linda Reed Collins. He does not know whether they have accepted gifts or gratuities from vendors. McGuire thinks it is somewhat unusual that Ms. Collins reserves purchasing functions for herself, since hers is primarily a management function. He cannot explain why she has reserved this duty. He once volunteered to take over her accounts, but she said she would prefer to handle some of the purchasing function herself, to "keep her hand in the business."

(Page 7)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF MARY RODRIGUEZ DE LA GARZA
DATE: FEBRUARY 5, 2015

Ms. De La Garza was interviewed at her office in Room 436, Bailey Building, 6200 Bayshore, St. Augustine, Florida. After being advised of the identity of the interviewer and the nature of the inquiry, Ms. De La Garza voluntarily provided the following information.

She has been employed at Bailey Books since 2010. In 2013, she was promoted and transferred to the Purchasing Department. Ms. De La Garza's function is to oversee the purchase of magazines and periodicals. She reports directly to Linda Reed Collins, the purchasing manager. The other employee in the department is Roger Donald McGuire.

Ms. De La Garza said that she is familiar with operating guidelines of the purchasing function. She is required to get bids for all purchases of more than $50,000, and, whenever possible, for purchases for less than that amount. As a rule, the purchases are bid for all items $10,000 and more.

In some instances, it is not practical or possible to obtain bids; this is especially the case with sundry purchases. In addition, whenever shortages of merchandise occur and time is of the essence, bids are not sought. For approximately the last year, she has observed that Orion Corporation, a supplier of paper to Bailey Books, has received most, if not all, of the paper business. The salesperson for Orion, Jim Nagel, seems to be very persuasive in dealing with Linda Reed Collins, Ms. De La Garza's boss.

When asked if there were any vendors who received preferential treatment, Ms. De La Garza hesitated. She finally said that something was bothering her, and she did not know how to discuss it.

When asked to explain, Ms. De La Garza said that she was concerned that any information she would offer might get back to Ms. Collins, and that she did not want to bring up false accusations. She said that there were several things that do not seem right.

(Page 8)

First, she said that Ms. Collins and her husband, Edward, had not been getting along for the past year or two. Edward has a charter boat business that has experienced serious financial problems, and she knew that Ms. Collins and he had been arguing over money.

She has seen Ms. Collins come to work several mornings in the last few months with red eyes, and it appeared that she had been crying. On one or two occasions, when Ms. Collins has arrived upset, she had telephoned Mr. Nagel, and Ms. De La Garza thinks Mr. Nagel comforted her.

Ms. De La Garza is not sure about the relationship between Mr. Nagel and Ms. Collins, but she does know that they are good friends. She is fairly certain that they have had lunch together on numerous occasions. Their friendship has been the subject of gossip and speculation; the office thinks that they are having an affair.

Ms. De La Garza knows that Mr. Nagel has received favored treatment as a vendor. Several months ago (exact date not recalled), she heard Ms. Collins call accounts payable and chew someone out who did not want to hand-cut a check for Mr. Nagel. She does not remember the exact circumstances, but she said that during the time she has worked at Bailey, Ms. Collins has never hurried up a payment for a vendor, with the exception of Mr. Nagel.

Ms. De La Garza does not believe Ms. Collins is doing anything illegal; she thinks, however, that Ms. Collins' judgment might be clouded by Mr. Nagel, whom she describes as a very good-looking and charming man.

When asked if anyone else had any knowledge of the business or personal relationship between Ms. Collins and Mr. Nagel, Ms. De La Garza replied that Sara Louise Dawson had worked on the Orion account before she left Bailey Books within the last several months. She believes Ms. Dawson had a falling out with Ms. Collins, which prompted her to quit.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF SARA LOUISE DAWSON
DATE: FEBRUARY 5, 2015

Sara Louise Dawson was interviewed at her residence, 2051 Wisconsin Ave., Apt. 16, St. Augustine, Florida, on a confidential basis. After being advised of the identity of the interviewer and the nature of the inquiry, she voluntarily provided the following information.

Ms. Dawson advised that she did not wish to answer any questions. She said that her employment at Bailey Books was a "closed chapter" in her life, which she did not wish to reopen. She described her relationship with Linda Reed Collins as "strained." She said that she wished she could be of assistance because "certain things at Bailey just weren't right," but she had "to get on with her life."

After further discussion with Ms. Dawson, in which the importance of her cooperation was emphasized, she agreed to speak to her brother-in-law, an attorney, about whether she should provide any information. She insisted that any communication with her, including this interview, be kept strictly confidential.

(Page 10)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO:	FILE (11-4422)
FROM:	LOREN D. BRIDGES, CFE
SUBJECT:	TELEPHONE CONVERSATION WITH THOMAS C. GREEN, ATTORNEY
DATE:	FEBRUARY 6, 2015

Thomas C. Green, an attorney with the law firm of Sharp, Green and Langfrom, P.A., 6600 Bayshore Parkway, St. Augustine, called me at my office at 10:00 a.m. on the above date.

Mr. Green said he had been contacted by Sara Louise Dawson, who had been referred by another attorney, regarding our request for an interview.

Mr. Green said he had interviewed Ms. Dawson and that her information would be "most helpful" to our inquiry. Mr. Green said he would not permit us to interview Ms. Dawson unless the company provided her with an indemnity against all claims arising out of her cooperation, and agreed to pay his attorney fees to attend the interviews.

Mr. Green would not provide any details about the nature of Ms. Dawson's information. He reiterated that we "would not be disappointed."

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: MEETING WITH MARK W. STEINBERG, CFO, AND LINCOLN S. WYZOKOWSKI, GENERAL COUNSEL
DATE: FEBRUARY 6, 2015

After discussing the facts, Mr. Steinberg and Mr. Wyzokowski agreed to provide an indemnity agreement to Sara Louise Dawson for her cooperation in the fraud examination regarding the purchasing function of Bailey Books, Incorporated. Wyzokowski agreed to prepare the indemnity agreement and to set up the interview of Ms. Dawson through her attorney.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
TONYA VINCENT, CFE
SUBJECT: INTERVIEW OF SARA L. DAWSON
DATE: MARCH 3, 2015

Sara Louise Dawson was interviewed at the office of her attorney, Thomas C. Green, at Suite 400, 6600 Bayshore Parkway, St. Augustine. Mr. Green was present for the entire interview. After preliminary discussions about the nature of the inquiry, Ms. Dawson voluntarily provided the following information.

Ms. Dawson was employed at Bailey Books Incorporated in the Purchasing Department from February 2011 through January 2015. Her duties included the purchase of magazines and periodicals as well as sundries and paper products. In that capacity, she worked for Linda Reed Collins from November 2011 until Ms. Dawson left the company.

After Ms. Collins's promotion, she began to favor Orion in paper purchases. Orion's prices were high and the quality of service was marginal. Deliveries often were late or incomplete, requiring Ms. Dawson to expend considerable time and effort in follow-up calls and correspondence.

On two occasions near the end of 2014, Ms. Collins directed her to make substantial purchases from Orion and to authorize prepayment. The orders were not bid, and prices quoted were higher than available from other, more reliable suppliers. Bailey Books also had a policy against prepayment of orders.

Ms. Dawson complained to Ms. Collins about Orion's past performance and suggested that other vendors be allowed to bid. Ms. Collins responded that the paper was needed now, that there was no time for bids, and that the price differential was insignificant. Ms. Collins also said that prepayment was necessary so that Orion could rush the order.

Ms. Dawson said that, in fact, there was no urgent need for the paper, but that, based on past experience with Ms. Collins, she believed it was fruitless to resist, and she complied with her instructions.

(Page 13)

Shortly thereafter, she checked with the receiving department and learned that the order had not been received. She advised Ms. Collins, who seemed unconcerned. Ms. Dawson then prepared a letter for Ms. Collins's signature requesting immediate shipment of the order. Ms. Collins declined to send the letter, saying it was not necessary, as Orion had assured her the shipment would be received shortly.

A few weeks later, Ms. Collins stopped by Ms. Dawson's office and closed the door. Ms. Collins told her that, because of Orion's "excellent service" and "loyalty" to Bailey Books, she wanted future purchases from them to be on a no-bid basis. Ms. Collins also instructed Ms. Dawson to prepay another order, in excess of $100,000 from Orion.

Ms. Dawson does not remember the exact dates or amounts, but suggested Becky Robinson in the Accounts Payable Department might be able to provide more information.

Ms. Dawson knew that the previous Orion order had not yet been shipped and informed Ms. Collins. Ms. Collins became "nervous and jittery" and insisted she was mistaken. She again instructed Ms. Dawson to place the order; Ms. Dawson said she would need approval from higher up and an argument ensued. She did not place the order or talk to Ms. Collins again. At that time, Ms. Dawson said she decided to look for new employment because her job had become too stressful.

Ms. Dawson also advised that other vendors, including Jerrico, had complained about being "squeezed" out by Bailey Books. Ms. Dawson thought that Jerrico's prices and service were superior to Orion's, but Ms. Collins would not take their product. Ms. Dawson, through Mr. Green, agreed to further interviews, as necessary.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF BECKY ROBINSON
DATE: APRIL 8, 2015

Becky Robinson, accounts payable clerk, Bailey Books, Incorporated, was interviewed at her office, Room 513, Bailey Building, 6200 Bayshore, St. Augustine, Florida. After being advised of the identity of the interviewer and the nature of the inquiry, she voluntarily provided the following information.

She has been employed by Bailey Books, Incorporated, since January 2009, and has always worked in the Accounts Payable Department. Her job is to review invoices for processing before payment. She checks the invoice mathematics and extensions, sees whether merchandise has been received, and verifies that the invoice has been approved for payment by the department head.

Ms. Robinson maintains the invoices. Canceled checks are maintained by the Treasury Office (she thinks in Ms. Deborah Roth's office). She provided copies of two invoices paid to Orion Corporation. The documents provided by her were initialed, dated, and secured in the evidence file maintained in Room 874, Bailey Books Corporation. Copies of the above-referenced documents are attached hereto.

A review of the invoices provided reflect a notation on invoices dated November 16, 2014 and December 5, 2014—in the amounts of $102,136, and $95,637, respectively—that payment was made before the merchandise was received. Ms. Robinson recalls that Ms. Collins called her on two occasions and said that Orion was experiencing cash flow problems, and to keep them as a vendor, it would be necessary to give them the money up front.

When Ms. Robinson told Linda Reed Collins that she was not supposed to approve payment before the merchandise had been received, Ms. Collins became agitated and told Ms. Robinson, "I am the senior purchasing official, and I am telling you to do what I say." Ms. Robinson did as she was instructed, but did not follow up to see if the paper had been received. Ms. Robinson did not report these incidents.

Ms. Robinson said that Ernie Quincy in the Receiving Department would be able to tell whether the two shipments above had been received.

(Page 15)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

ORION

Orion Corporation
2600 Industrial Drive
St. Augustine, Florida 32086

November 16, 2014

I N V O I C E

Bailey Books Incorporated
6200 Bayshore Drive
St. Augustine, FL 32082

1,075 packages of 80 lb. standard white paper @ 95/m…….	$102,136

TERMS: NET 30 DAYS

(Page 16)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

ORION

Orion Corporation
2600 Industrial Drive
St. Augustine, Florida 32086

December 5, 2014

I N V O I C E

Bailey Books Incorporated
6200 Bayshore Drive
St. Augustine, FL 32082

1006 packages of 80 lb. standard white paper @ 95/m…….	$95,637

TERMS: NET 30 DAYS

(Page 17)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF ERNIE QUINCY
DATE: APRIL 8, 2015

Mr. Ernie Quincy, warehouse manager of Bailey Books, was interviewed at his office, Room 114, Bailey Building, 6200 Bayshore, St. Augustine, Florida. After being advised of the identity of the interviewer and the nature of the inquiry, Mr. Quincy voluntarily furnished the following information.

A review of his outstanding invoices shows that two Orion invoices—dated November 16 and December 5, 2014—have not been received in the warehouse. He remembers that shortly after receiving the invoices in 2014, he called Ms. Robinson, who referred him to Linda Reed Collins. Mr. Quincy then called Ms. Collins about not having received the paper, and she told him not to worry about it; that they had an understanding with the supplier that the paper would be delivered later.

Mr. Quincy thought that this situation was unusual since no other shipments had been paid for in advance. He has been Bailey Books' warehouse manager for 12 years.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: CHECKS PAYABLE TO ORION PAPER COMPANY
DATE: APRIL 9, 2015

Margaret O'Boyle, Treasurer's Office, Bailey Books, Incorporated, provided copies of the checks described below. A review of Bailey Books, Incorporated, canceled checks, numbered 10106 and 10107, reflected the following:

Check No. 10106
- Date: December 12, 2014
- Amount: $102,136
- Payment for: Orion invoice dated November 16, 2014
- Endorsement: For Deposit to the Account of Orion Paper Company, Account No. 025269999 (stamped)
- Bank to which deposited: Florida Marine National Bank, St. Augustine
- Date deposited: December 14, 2014

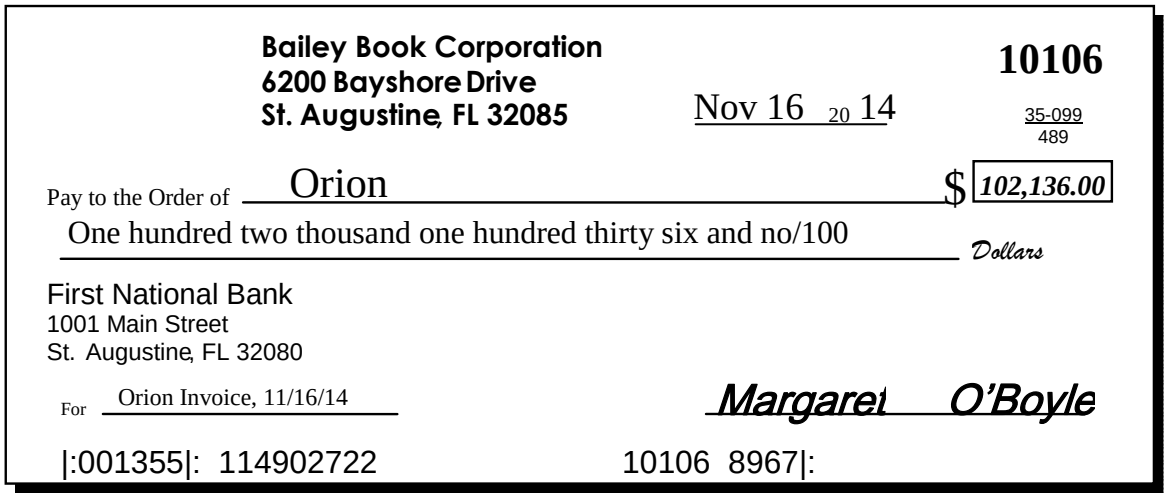
Check No. 10107
- Date: December 12, 2014
- Amount: $95,637
- Payment for: Orion invoice dated December 5, 2014
- Endorsement: For Deposit to the Account of Orion Paper Company, Account No. 025269999 (stamped)
- Bank to which deposited: Florida Marine National Bank, St. Augustine
- Date deposited: December 14, 2014

Copies of the fronts and backs are attached, and they have been initialed and dated.

(Page 19)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS



Bailey Book Corporation
6200 Bayshore Drive
St. Augustine, FL 32085

10106

Nov 16 20 14

35-099
489

Pay to the Order of Orion $ 102,136.00

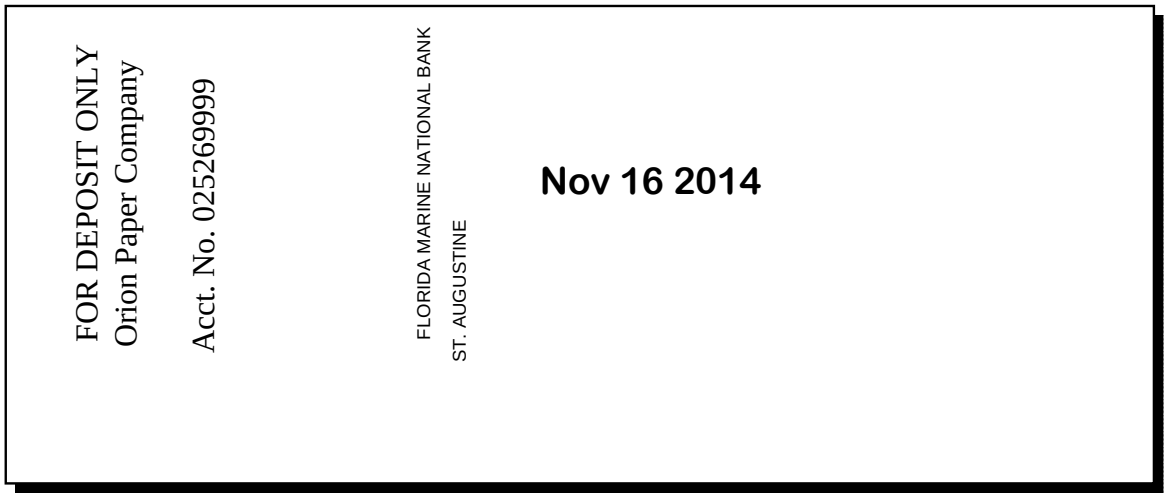
One hundred two thousand one hundred thirty six and no/100 Dollars

First National Bank
1001 Main Street
St. Augustine, FL 32080

For Orion Invoice, 11/16/14

Margaret O'Boyle

|:001355|: 114902722 10106 8967|:



FOR DEPOSIT ONLY
Orion Paper Company

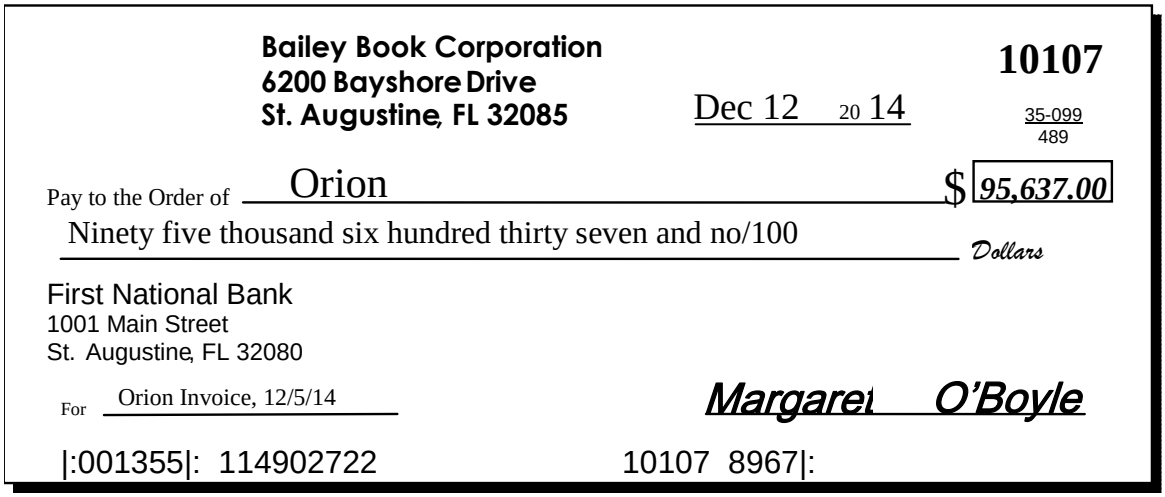
Acct. No. 025269999

FLORIDA MARINE NATIONAL BANK
ST. AUGUSTINE

Nov 16 2014

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS



Bailey Book Corporation
6200 Bayshore Drive
St. Augustine, FL 32085

10107

Dec 12 20 14

35-099
489

Pay to the Order of Orion $ 95,637.00

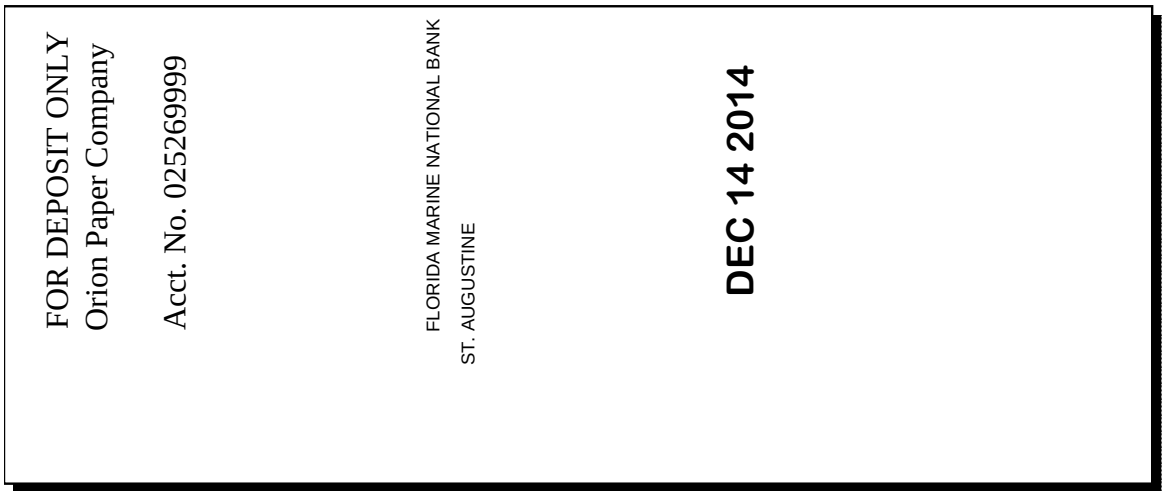
Ninety five thousand six hundred thirty seven and no/100 Dollars

First National Bank
1001 Main Street
St. Augustine, FL 32080

For Orion Invoice, 12/5/14

Margaret O'Boyle

|:001355|: 114902722 10107 8967|:



FOR DEPOSIT ONLY
Orion Paper Company

Acct. No. 025269999

FLORIDA MARINE NATIONAL BANK
ST. AUGUSTINE

DEC 14 2014

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF DAVID LEVEY, JERRICO INTERNATIONAL PAPER COMPANY
DATE: APRIL 9, 2015

David Levey, director of sales, Jerrico International Paper Company, 2901 Island Ave., Philadelphia, PA 19530, was interviewed by telephone at his office. After being advised of the identity of the interviewer, he provided the following information on a voluntary basis.

Mr. Levey assumed his present position in 2008. At that time Bailey Books, Incorporated, was a major customer, with sales in excess of $500,000 annually. Since then, the volume has consistently dwindled.

In January 2014, Mr. Levey met with Carl Sanderson, the owner of Jerrico, and discussed how to revive the Bailey Books account. Both Mr. Levey and Mr. Sanderson had heard "rumors" in the industry that Jim Nagel of Orion Corporation was "taking care of" Linda Reed Collins, Bailey's purchasing manager. Mr. Nagel has a very poor reputation in the industry and was caught "paying off" on another account several years ago. Mr. Levey declined to provide any further details or to identify the source of his information.

As a result of their meeting, Mr. Sanderson and Mr. Levey "decided to test the waters" at Bailey Books by submitting a bid at cost for a substantial quantity of Deluxe Bond and Standard White to see "if we could open the doors." The offer was made at the end of January 2014, and was not accepted. Since then, Jerrico does not even bother to bid and expects no further significant sales to Bailey Books.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: INTERVIEW OF MARY RODRIGUEZ DE LA GARZA
DATE: APRIL 13, 2015

Ms. Mary Rodriguez De La Garza phoned and said that she had overheard a telephone conversation between Ms. Collins and Mr. Nagel. She heard Ms. Collins arrange to meet Mr. Nagel for drinks this afternoon after work. Collins is supposed to meet Nagel at the bar at the Hotel Atlantic in St. Augustine. Accordingly, a physical surveillance was established, as set forth in the following log.

(Page 23)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: SURVEILLANCE LOG
DATE: APRIL 13, 2015

On April 13, 2015, commencing at 4:50 p.m., surveillance was established at the Hotel Atlantic, 6583 Bayshore, St. Augustine, Florida. The results of the surveillance are as follows.

Time	Event
4:50 p.m.	Established surveillance in lounge.
5:55 p.m.	Linda Reed Collins and white male arrive at lounge and order drinks. Collins and unidentified male hold hands at table.
6:20 p.m.	Collins and unidentified male order another drink.
6:27 p.m.	Unidentified male and Collins kiss at the table.
6:40 p.m.	Break—surveillance terminated.
6:44 p.m.	Surveillance reinstituted. Twosome still at bar.
7:02 p.m.	Observed white male paying for drinks in cash. Twosome leaves, holding hands, and proceeds to Room 652 at Hotel Atlantic. Both enter.
9:32 p.m.	Collins and male leave Room 652. Male gets into a late model Chevrolet, silver in color, Florida license MNX-782, and departs. Collins gets into a Nissan Z, license NRC-130, and departs.
9:35 p.m.	Surveillance terminated.

(Page 24)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: ANONYMOUS TELEPHONE CALL
DATE: APRIL 16, 2015

A telephone call was received advising that Edward J. Collins and his wife, Linda Reed Collins, had the following debts with the establishments listed below as of March 14, 2015.

Account	Total Balance	Monthly Payments
St. Augustine Bank	$46,482	$2,361
Sears	$2,378	$281
Marine Savings	$110,232	$1,377
Bailey Credit Union	$14,826	$787
MasterCard	$10,041	$397
American Express	$5,990	Balance
Norwood Corporation	$3,892	$461
Bally Fashions	$1,436	$124
	Total Fixed Payments	$5,788

The caller advised that Edward J. and Linda Reed Collins had held a joint checking account since 2005 at Sunshine Federal Bank. The account had an average balance of less than $1,000, and was frequently overdrawn. No other accounts were located.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF RECORDS
ST. AUGUSTINE COUNTY COURTHOUSE
DATE: APRIL 17, 2015

Records of the St. Augustine County Courthouse reflected the following information regarding Edward J. Collins and Linda Reed Collins as of April 11, 2015.

1. Edward J. Collins is a defendant in three civil actions as follows:

a. *Bertram Yachts, Incorporated v. Edward J. Collins and Collins Marine Corporation*, Case Number 00-4435. Bertram sued Collins individually and the corporation for nonpayment of $13,874 plus interest and attorney fees. The suit was filed April 23, 2013, and alleges that Collins took delivery of a marine winch on March 4, 2012, and that the amount is unpaid. The suit is still pending. Attorney for the plaintiff is Sherry T. Marshall, Cummins and Marshall, Vero Beach, Florida.

b. *Bradford L. Jenkins v. Edward J. Collins et al*, Case Number 01-0964. This suit alleges that on June 27, 2014, Jenkins paid a deposit for Collins's charter boat, the Mistress, and canceled within the period provided by the contract. Collins's check refunding the $3,500 was returned for insufficient funds. Collins did not make good on the check.

c. *Bayview Bank v. Edward J. Collins and Collins Marine Corporation*, Case Number 01-5412. Collins was sued on April 21, 2014, for nonpayment of a working capital note with a current balance off $31,423. The note is unpaid.

(Page 26)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF RECORDS
SECRETARY OF STATE
DATE: APRIL 17, 2015

The Secretary of State's Office, Tallahassee, Florida, records reflects the following information about Collins Marine Corporation.

The corporation was formed on July 23, 2006. Listed as incorporators are Edward J. Collins, James B. Vickers, and Linda Reed Collins. Officers are the same. Registered agent is Frank R. Bledsoe, attorney at law, 764 Front Street, St. Augustine, Florida.

The corporation's charter was suspended on February 15, 2014 for failure to pay $324 in taxes.

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF RECORDS
CHATTEL MORTGAGES
DATE: APRIL 17, 2015

A review of Chattel Mortgages in St. Augustine County, Florida, reflects the following records concerning Linda Reed Collins and Edward Collins as of December 31, 2014:

Date Filed	Lien Holder	Property	Original Amount of Lien
3/12/12	St. Augustine Bank	2009 Mercedes SL550	$75,000
6/12/12	Bailey Credit Union	2011 Nissan 370Z	$21,505
7/17/13	Norwood Corporation	Stereo Equipment	$8,500

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF RECORDS
DUN & BRADSTREET
DATE: APRIL 17, 2015

Records of Dun & Bradstreet reflect the following information about Collins Marine Corporation as of December 31, 2013:

	2011	2012	2013
Sales	$302,000	$257,000	$193,000
Total assets	$157,000	$146,000	$118,000
Total liabilities	$104,000	$161,000	$183,000
Net income	$41,000	-$13,000	-$63,000

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
SUBJECT: REVIEW OF FINANCIAL CONDITION OF LINDA REED COLLINS AND EDWARD J. COLLINS FROM PUBLIC RECORDS
DATE: APRIL 18, 2015

A review of the financial condition of Linda Reed Collins and Edward Collins, assembled from public records, reflects the following for the year of 2014:

Income (net):			
Linda Reed Collins	$35,400		
Edward J. Collins		_____	
Total income:			$35,400
Expenses:			
House payments		16,524	
Automobile payments			
'09 Mercedes		28,332	
'11 Nissan		9,444	
Stereo equipment		5,532	
Food (estimated)		4,800	
Utilities (estimated)		2,400	
Total expenses:			67,032
Unexplained income:			$31,632

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)

FROM: LOREN D. BRIDGES, CFE
TONYA VINCENT, CFE
SUBJECT: INTERVIEW OF JAMES R. NAGEL
DATE: APRIL 19, 2015

James R. Nagel, sales representative, Orion Corporation, was interviewed at his office, Room 5214, 2600 Industrial Drive, St. Augustine, Florida. After being advised of the identity of the interviewers and of the nature of the inquiry, Mr. Nagel voluntarily provided the following information.

He has been a salesperson for Orion since October 2005. He sells stationery and paper stock to a variety of business enterprises, including Bailey Books, Incorporated. Bailey is not his largest account.

Mr. Nagel acknowledges that he knows Linda Reed Collins. He says their relationship is purely professional, and he has never socialized with her. He emphatically denies any improprieties of any kind, and says he has never offered any gratuities or kickbacks to Ms. Collins.

Mr. Nagel claims the prices he charges Bailey are competitive, and that if Bailey is paying higher prices, it is because they are getting better products. He was presented with two invoices, dated 11/16/14 and 12/5/14, which reflect the payments for products that were not received. Nagel claims he does not know anything about any missing products, and that Bailey's records were in error. He denies asking for payment in advance to help the cash flow of Orion Corporation.

Mr. Nagel denied our request to review Orion's books and records pertaining to the 11/16/14 and 12/5/14 invoices, saying the information was "none of your business" and "proprietary." He refused to answer any further questions without his legal counsel being present.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
TONYA VINCENT, CFE
SUBJECT: INTERVIEW OF OWEN STETFORD
DATE: APRIL 21, 2015

Owen Stetford, chief financial officer, Orion Corporation, was interviewed in his office at 2600 Industrial Drive, St. Augustine, Florida. Clifford Karchmer, Orion's general counsel, also attended the meeting.

We advised Mr. Stetford and Mr. Karchmer of the nature of our inquiry and requested their cooperation. We had earlier asked Mr. Stetford to produce copies of Orion's records pertaining to sales to Bailey Books when we telephoned to set up the interview.

Mr. Stetford said that Orion Corporation was formed in 1979 by his grandfather and that the company is closely held. Mr. Stetford further stated that Orion is committed to the highest level of business integrity, that Bailey Books is a valued customer, and that he is anxious to cooperate as far as permitted by company counsel.

Regarding our request to review Orion's records pertaining to sales to Bailey Books, and in particular the invoices dated November 16 and December 5, 2014, Mr. Stetford said that he would be unable to provide us with access to the original records on the advice of counsel. However, he said he personally reviewed the records and told us that Orion had no record of any receipt of payment for the above invoices, nor any record that such an order had been placed or shipped.

Mr. Stetford further advised, after reviewing our copies of the canceled Bailey Books checks payable to Orion for the above invoices, that Orion does not maintain any corporate accounts at Florida Marine National Bank. Furthermore, the correct corporate name is Orion Corporation, not Orion Paper Company, as the endorsements indicate.

Mr. Stetford emphatically stated that neither he nor any other corporate officer was aware of or condoned any improper activities regarding their sales. He said that he would direct Mr. Nagel to answer any questions regarding sales to Bailey Books Incorporated.

In this regard, we again asked for permission to examine Orion's records, particularly the account receivable records for the period November 2012 through March 2015. Mr. Karchmer said that he would take our request under advisement.

(Page 32)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO: FILE (11-4422)
FROM: LOREN D. BRIDGES, CFE
TONYA VINCENT, CFE
SUBJECT: INTERVIEW OF JAMES R. NAGEL
DATE: MAY 1, 2015

James R. Nagel was interviewed at the office of his attorney, Conrad Vance, of the law firm Vance, Selig and Reisman, Suite 1000, 1601 Harbor Drive, St. Augustine, Florida. Mr. Nagel was presented with copies of the checks endorsed "Orion Paper Company," and asked about the bank account to which they were deposited. After hesitating for several moments, he quietly admitted to conspiring with Linda Reed Collins to have Bailey Books pay the fake invoices. At the conclusion of the interview, Mr. Nagel voluntarily executed the attached statement. The original of this statement has been witnessed by Bridges and Vincent, and is maintained in the evidence file, Room 874, Bailey Books Corporation, 6200 Bayshore, St. Augustine, Florida 32082.

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

St. Augustine, Florida
May 1, 2015

I, James R. Nagel, furnish the following free and voluntary statement to Loren D. Bridges and Tonya Vincent of Bailey Books, Incorporated. No threats or promises of any kind have been used to induce this statement.

Since 2005, I have been a sales representative employed by Orion Corporation. Since 2007, I have been responsible for paper sales to Bailey Books, Incorporated.

In or about January 2013, Linda Reed Collins, manager of purchasing, told me that she would require a "commission" on all sales to Bailey Books by Orion. I advised my boss, Donald L. Marsh, sales manager, of Ms. Collins's demand. Mr. Marsh and I reluctantly agreed to make the payments because we believed that it would otherwise be impossible to make any sales to Bailey Books. No other person at Orion was informed of Ms. Collins's demand.

The payments to Ms. Collins began about February 2013. Ms. Collins told me that she would inflate the prices paid to Orion in order to cover the kickbacks. Thereafter, approximately $51,000 was paid to Ms. Collins by Orion Corporation checks, payable to Market Research, Inc. Ms. Collins told me that Market Research, Inc., was a company she had established. The checks were recorded on Orion's books as consulting fees, and were approved by Mr. Marsh and me.

In about October 2014, Ms. Collins told me that she would approve the payment of invoices to Orion for product that would not have to be delivered. Ms. Collins thereafter authorized the payment of two invoices in the amounts of $102,136 and $95,637, which were paid by Bailey Books, Incorporated, in November and December, 2014. No product was shipped on these invoices. Ms. Collins and I established a bank account in the name of Orion Paper Company at Florida Marine National Bank and equally divided the proceeds of the above-mentioned invoices. Ms. Collins prepared my checks, which were then deposited to my personal checking account at Flagler National Bank in St. Augustine. I spent the proceeds on bills. Neither Mr. Marsh nor any other person at Orion was aware of the above activity.

I make this statement in order to express my regret for having engaged in the aforementioned conduct, and promise to make restitution to the extent possible. I knew my conduct was wrong, but I felt it was justifiable at the time. I will try to pay any losses that have occurred as a result of my activities.

I have read this statement, consisting of this page. I now sign my name below in the presence of the undersigned witnesses because the statement is true and correct to the best of my knowledge.

Witnesses:
Loren D. Bridges_____ *James R. Nagel*_____
Signature

Tonya Vincent_____

Date:
_____

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

Bailey Books, Incorporated

MEMORANDUM

TO:	FILE (11-4422)
FROM:	LOREN D. BRIDGES, CFE
	TONYA VINCENT, CFE
SUBJECT:	INTERVIEW OF LINDA REED COLLINS
DATE:	MAY 1, 2015

Ms. Linda Reed Collins was interviewed on May 1, 2015, by Loren D. Bridges and Tonya Vincent. She voluntarily provided the attached signed statement. The original of this statement has been witnessed by Bridges and Vincent, and is maintained in the evidence file, Room 874, Bailey Books Corporation, 6200 Bayshore, St. Augustine, Florida 32082.

(Page 35)

APPENDIX E

SAMPLE FRAUD EXAMINATION REPORTS

St. Augustine, Florida
May 1, 2015

I, Linda Reed Collins, furnish the following free and voluntary statement to Loren D. Bridges and Tonya Vincent of Bailey Books, Incorporated. No threats or promises of any kind have been used to induce this statement.

I am senior purchasing agent for Bailey Books, Incorporated, and have been employed by Bailey Books since 2010. My job is to oversee the purchase of merchandise and other supplies for Bailey Books, Incorporated. As part of my job, I am to ensure that Bailey Books, Incorporated, receives the highest quality products at the lowest possible cost.

Commencing in approximately February 2013, and continuing through the current time, I have accepted money from James Nagel, sales representative for Orion Corporation, St. Augustine, Florida. Nagel offered me money to ensure that his company received preferential treatment in supplying Bailey Books with stationery and paper products.

On those occasions that I accepted money, I was aware that Bailey Books, Incorporated, was not obtaining the best product at the lowest possible price. The price charged for products delivered during the time I accepted money was substantially higher than market value.

In November and December 2014, I authorized the payment of invoices of $102,136 and $95,637, respectively. These invoices were paid without the receipt of any merchandise. Nagel and I subsequently split the proceeds of these invoices equally between us.

I estimate that I have received in excess of $150,000 in connection with Mr. Nagel. I am not sure that anyone at Orion Corporation knew of our arrangement. No one at Bailey Books had knowledge of, or participated in, my scheme.

I am aware that my conduct is illegal and violated Bailey Books' policies. I participated in this scheme because my husband and I were having severe financial problems due to his business. We used the proceeds of my conduct to pay off several personal and business-related debts that were past due. I am truly sorry for my conduct, and I promise to repay any resulting damages.

I have read this statement consisting of this page. I now sign my name below because this statement is true and correct to the best of my knowledge.

Witnesses:
Loren D. Bridges _____ *Linda Reed Collins* _____
Signature

Tonya Vincent _____

Date:

_____

(Page 36)

FRAUD PREVENTION AND DETERRENCE

TABLE OF CONTENTS

WHITE-COLLAR CRIME (CONT.)

CORPORATE GOVERNANCE

CORPORATE GOVERNANCE (CONT.)

MANAGEMENT'S FRAUD-RELATED RESPONSIBILITIES

MANAGEMENT'S FRAUD-RELATED RESPONSIBILITIES (CONT.)

AUDITORS' FRAUD-RELATED RESPONSIBILITIES

FRAUD PREVENTION PROGRAMS (CONT.)

FRAUD PREVENTION PROGRAMS (CONT.)

FRAUD RISK ASSESSMENT

MENU

FRAUD RISK ASSESSMENT (CONT.)

FRAUD PREVENTION AND DETERRENCE

FRAUD RISK ASSESSMENT (CONT.)

FRAUD RISK MANAGEMENT

ACFE CODE OF PROFESSIONAL ETHICS (CONT.)

CFE CODE OF PROFESSIONAL STANDARDS

UNDERSTANDING CRIMINAL BEHAVIOR

Much of our understanding of criminal behavior can be attributed to B.F. Skinner, described by many as one of the greatest social scientists of the 20th century. Skinner promised that he would revolutionize not just psychology, but all of human society with his theories of behaviorism. According to Skinner, human behavior should be approached scientifically. Instead of worrying over men's souls or quibbling about what makes up the Self, behaviorists would deal with what people actually do. By analyzing people's actions, the behaviorist could then alter or direct any behavior for the greater good of all. Criminal behavior could be modified into productive action, and rearing a family would cease to be a continual game of trial and error—the pitfalls would be replaced by basic behavioral principles.

Skinner's accomplishments might have fallen short of this lofty goal. But while he's not as widely recognized as Sigmund Freud, Skinner's influence permeates many areas, often without being overtly attributed to the methods he proposed in *Walden Two* (1948) and *Science and Human Behavior* (1953). When lawyers argue the mitigating or exonerating circumstances of a client's case, they often use behaviorist ideas. Entire theories of management rest on the assumption that *incentives* and *promotion* are not just the best way to sell something; they are the best way to ensure that employees work properly.

Behavioral Analysis and the Prevention of Fraud

When a detective searches for a suspect's motive, the detective is using behaviorist methods of analysis. The detective assumes that the suspect was stimulated by some arrangement of factors. Many courses in criminology are built around the fundamental premise that crimes are particular sorts of behavior and best understood as the product of operant conditioning. Fraud examiners often use the same methods in approaching a case. When money is missing, the fraud examiner traces the known flow of funds and then asks, "Who had the opportunity and the motive to get at this money?" Even without being conscious of the fact, the fraud examiner is performing a behaviorist analysis on the crime.

Ultimately, the question of fraud and behavior comes down to this—*what can we do about it?* We know that people commit these crimes at an alarming rate. Incidents range from the clerk who skims a few hundred dollars off a business's daily deposits, to multimillion-dollar

scam artists who destroy entire organizations. There's a world of difference between the skimming clerk and the scamming financial executive—so can we even analyze the two people within the same system of fraud?

A fraud examiner working with behaviorist principles knows that the difference between crimes lies in the different behaviors. The man who plays million-dollar games with other people's money is stimulated and reinforced by a distinct set of factors, and so, too, is the clerk who builds a family nest egg from his three-figure thefts. So when a fraud examiner is asked to go beyond crime-solving and to consult on fraud prevention, the job demands a thorough analysis of behavior.

It is important to think of employment as a system of behavior because so much fraud occurs in workplace environments, which highlights the connection between economics and people's actions. For both the crook and the dedicated worker, money exerts a powerful influence, and this is not likely to change. The resourceful employer, then, should consider the best way to establish a positive set of relations between employees and the funds flowing through the company. The more rigorously we understand *how* people behave, the better equipped we are to change *the way* they behave.

Behavioral studies such as those conducted by Skinner show that punishment is the least effective method of changing behavior. According to Skinner, punishing brings a temporary suppression of the behavior, but only with constant supervision and application. In repeated experiments, Skinner found that punishment—either applying a negative stimulus or taking away a positive one—effectively extinguished a subject's behavior, but that the behavior returned when the punishment was discontinued. In other words, the subject would suppress the behavior as long as the punishment was applied directly and continually, but as soon as the punishment was withdrawn for a while, the behavior was attempted again; if there was no punishment following the attempt, the subject began to behave as before.

Reinforcement and Punishment

Reinforcement and punishment of behavior are distinguished by the way that positive and negative forces are applied. A *positive reinforcement* presents a positive stimulus in exchange for the desired response. For example, a parent might say to a child, "You've cleaned your room. Good. Here's the key to the car." The behavior (cleaning) is reinforced by the awarding of the positive stimulus (the car key). In contrast, a *negative reinforcement* withdraws a

negative stimulus in exchange for the response. Continuing the example, the parent might say, "I'll stop hassling you if you clean this room." The negative stimulus (hassling) is withdrawn when the appropriate behavior is performed.

In an act of *punishment*, the polarities, so to speak, are reversed. Faced with an undesired behavior, the punisher applies a negative stimulus. A father, hearing his son use profanity, puts a bar of soap into the boy's mouth. Punishment may also be administered by withdrawing a positive stimulus, such as "Your room is still filthy, so you can't use the car."

The following chart summarizes the applications of each approach:

REINFORCEMENT	*Presents positive stimuli*	*Withdraws negative stimuli*
PUNISHMENT	*Presents negative stimuli*	*Withdraws positive stimuli*

Punishment fights a losing battle in manipulating behavior because it works by providing negative consequences—administering penalties and taking away desirables. Access to the car or the thrill of a racy story doesn't become less attractive for its use in punishment; its power to stimulate is simply squelched. Conversely, reinforcement proceeds to accentuate the positive. Skinner concludes that behavior is most effectively modified by managing and modifying desires through reinforcement; he wants to replace destructive behaviors with productive ones, instead of trying to punish an already existing impulse.

Alternatives to Punishment

Behaviorism points toward a number of alternatives to punishment. Chief among these is to *modify the circumstances* surrounding the act. If an employee is experiencing financial problems, there might be ways a company can help alleviate pressures. For example, the company could offer financial counseling, pay advances, or low-interest loans, thereby alleviating financial difficulties without the employee having to resort to fraud. In other instances, employees engage in fraud because they feel underpaid or unappreciated.

Emotions, according to Skinner, are a predisposition for people's actions. Anger is not a behavior, but a state of being that predisposes people to do things like yell or fight. Anger is a part of a person's response, to the extent that an angry man is more likely to get in a shouting match with his friends. And since the emotional associations of any event are

important factors in conditioning behavior, the associations can be manipulated in conditioning the behavior. That's why advertisers use cute babies to sell toilet paper—the image associates the toilet paper with the emotions evoked by the baby. A company portrays its founder as a father figure for a similar reason. When managers are faced with disgruntled employees, they can modify these emotional circumstances, not just with "image" work, but with adequate compensation and recognition of workers' accomplishments. Incentive programs and task-related bonuses follow this principle, assuming that employees who feel challenged and rewarded by their jobs will produce more work at a higher quality and are less likely to violate the law.

Another non-punitive approach drives the undesirable behavior into extinction by preventing the expected response. This is a specialized version of modifying the circumstances. Business managers perform an extinction strategy by implementing a system of internal controls. In requiring several signatures for a transaction, for example, a bank's procedures prevent any one employee from gaining access to money. This approach doesn't involve reinforcements or punitive measures; it simply modifies the structure in which acts take place. The perception of internal controls provides a particularly strong deterrent to fraud because it obstructs the operant behavior that has, heretofore, been linked with positive reinforcement. We prevent the act by blocking the expected response. Criminal behavior is discouraged because crime doesn't pay.

A related strategy overcomes improper behavior by encouraging the behavior's "opposite." Skinner says that we can *condition incompatible behavior* that interferes with the person's usual acts. Instead of punishing a child's emotional tantrums, for example, the behaviorist rewards the child for controlling emotional outbursts; we drive the tantrums into extinction by not responding, thereby reinforcing the stoical behavior. A destructive behavior is offset by an incompatible productive one. Since fraud involves dishonesty, secrecy, and antagonistic behaviors, the astute manager finds ways to reward the opposite behaviors—honesty, openness, and cooperation.

Of course, it's easier to list these strategies in a few paragraphs than it is to implement them. Even the most seemingly simple acts can become tangled as people and circumstances interact. A perfectly sound theoretical reinforcement—an employee incentive program, perhaps—might be viewed with suspicion by disgruntled workers. Behavioral modification is never easy, Skinner says; reinforcements "must be sensitive and complex" because people's lives are complicated and their behaviors sensitized. For example, people in groups often

interact in alarming and unstable ways. Skinner demonstrates this tendency with the example of a whipping-boy game played by eighteenth-century sailors. The sailors tied up a group of young boys in a straight line, restraining each boy's left hand and placing a whip in the right hand. The first boy in line was given a light blow on the back and told to do the same to the person immediately in front of him. Each boy hit the next in line, and each one was hit in turn. As Skinner reports, "It was clearly in the interest of the group that all blows be gentle, [but] the inevitable result was a furious lashing."[1] Each boy in the line hit a little harder than he had been hit himself; after a few cycles, the last blows would, in fact, be furious (especially since each swing was preceded by pain, creating an emotional disposition of anger and anxiety). Whipping sessions aren't a likely happening in most companies, but people often exhibit a similar inclination toward catalyzed reactions: Whispering sessions gradually evolve into full-blown discussions that echo into the hallways; minor financial indiscretions grow into large-scale larceny.

Ideally, behavioral managers could anticipate this catalyzing and redirect the energies, but what if that is not an option? Though the dollar amounts (and the audacity) of some white-collar crimes boggle the average observer's mind, the crime remains an act of behavior. The perpetrator might be described as "obsessive" and "megalomaniacal," but he is still behaving in a network of actions, with his behavior subject to operant conditioning.

The monetary amounts are, in fact, misleading. Once the stakes reach a certain level, it's not even plausible to look for explanations involving a lack of respect or appreciation. High-dollar criminals describe their machinations as a "kick" or thrill; they feel like they're playing a game, and it's the game of their lives. Behaviorists agree. Money is a "generalized reinforcer," directly linked with many positive factors and often taking on a symbolic power of its own, thereby yielding a condition of strength. Skinner says, "We are automatically reinforced, apart from any particular deprivation, when we successfully control the physical world."[2] So, we need not be starving in order to act, especially with the sense of control—symbolic and literal—gained by acquiring money. Game-playing exerts something similar on its participants; someone who manipulates a chessboard or a deck of cards successfully gains a sense of strength over external events. We can play the game "for its own sake" because it yields the impression of strength. Imagine, then, the behavioral stroke that happens when the game's power is combined with the power of money as a generalized reinforcer, and

[1] B. F. Skinner, *Science and Human Behavior* (New York: Macmillan Publishing, 1953), 309.
[2] Ibid., 77.

both of these factors are played out with real people and settings. The dealmaker is racing through a thicket of reinforcements, and the greater the risk—financial, legal, or personal—the greater the thrill. The stimulus isn't the money as a thing in itself, any more than money for its own sake prompts the miser. In either case, the condition of strength (we might even call it "power") feeds the behaving person; money just happens to be the reinforcer *par excellence* of our culture.

Dealing with high-stakes criminals will remain difficult, despite our understanding of their behavior. Not just because the amounts of money and the networks of action are so complex, but because the conditioning is so intense. How, for example, can you replace the kick of scoring a $35-million-dollar take in a three-day scam? Can a career con be prompted to give up the deceitful practices that have marked his experience? Finding genuine and specific answers might be delayed for some time, but they will likely follow the same pattern we've discussed with other crimes, such as:

- Modifying the circumstances of the behavior by, for example, making legitimate businesses a more opportune place for daring and innovative techniques
- Extinguishing the criminal behavior by preventing its success using regulation, controls, and supervision
- Encouraging behaviors incompatible with criminal activity via educational practices and the demonstration of "values" that call the criminal lifestyle, however flashy, into question

The specific measures will be particular to the crime. The actions dictate the response. But whether we're dealing with a working mother's credit card fraud, or Bernie Madoff's palatial schemes, our methods can be behavioral. Fraud examiners might never eradicate crime completely, but by approaching criminal acts scientifically, we can become more successful in anticipating and preventing the acts.

Applying Behavioral Analysis to Fraud Prevention

To successfully recognize, detect, and prevent fraud, the fraud examiner has to take into account as many variables as possible, and has to learn a great deal about how human beings—as individuals and in groups—behave.

All the efforts of behavioral engineering notwithstanding, the question of behavior finally rests with the person who behaves. In *Walden Two*, the founder of Skinner's utopian community admits that there is only so much that can be done by cultural design:

> *You can't foresee all future circumstances, and you can't specify adequate future conduct. You don't know what will be required. Instead, you have to set up certain behavioral processes which will lead the individual to design his own "good" conduct when the time comes. We call that sort of thing "self-control."*[3]

No substitute exists for the conscious individual making a choice to act. And no science can predict or shape behavior with pure accuracy. There are just too many factors at work in the network of actions. However, self-control is a behavior that is guided by conditioning in the same way any other act would be.

It does little good, for example, to tell an alcoholic, "Stop drinking; control yourself." The command alone has little force, even if the alcoholic wants to stop drinking. Family members can suggest that the man simply throw away his bottles, but "the principal problem," Skinner interjects, "is to get him to do it."[4] Family members can, however, help condition the alcoholic's self-control by registering disapproval of drinking, reinforcing the man's successful resistance to drink, and encouraging the man to do things incompatible with a drinking life. They can't follow the man through every step of his life; he has to resist the impulse to sneak a sip on his own. But the behavior of resistance is strengthened by his family members' intervention. "Self-control" as a behavior is shaped by "variables in the environment and the history of the individual."[5]

Understanding why people do certain things allows us to go beyond a simplistic insistence that criminals "control themselves." We will instead have to consider how this control can be conditioned, preventing the behavior directly when possible, but ultimately relying on each individual having adequately absorbed the principles of self-control.

Why People Obey the Law

Now that we have a general understanding of at least some of the reasons why humans behave the way they do, let us turn our discussion to why people obey (and contrarily break) the law. In his book *Why People Obey the Law*, Tom Tyler studies the two principal types of law-abiding people.[6]

---

[3] B. F. Skinner, *Walden Two* (Indianapolis, IN: Hackett Publishing Company, 1948), 96.
[4] B. F. Skinner, *Science and Human Behavior* (New York: Macmillan Publishing, 1953), 240.
[5] Ibid.
[6] Tom R. Tyler, *Why People Obey the Law* (New Haven: Yale University Press, 1990).

Obviously, some people choose to obey the law, while others choose to break it. Many otherwise law-abiding members of society evade taxes, occasionally use a controlled substance, commit fraud, or even drive under the influence of alcohol. According to studies by Tyler, the instrumental and the normative perspectives attempt to explain why some follow the law to the letter while others obey selectively.

Instrumental Perspective

According to the instrumental perspective, people weigh the pros and cons of compliance with the law and act accordingly. In other words, they choose to obey the law because they fear punishment for noncompliance.

A person exemplifying the instrumental perspective might exceed the speed limit, thinking that the benefit of saved time outweighs the risk of the potential speeding ticket. These types of individuals are unlikely to rob a bank, though, considering that success is doubtful and the penalty is steep.

Normative Perspective

The focus of the normative perspective is what one considers just and moral. When people believe compliance is their moral obligation, commitment to the law is voluntary, regardless of fear of punishment.

People of this belief might indulge in illegal drugs but refrain from stealing—one being morally acceptable in their view and the other not. Others might obey all laws out of the belief that the authorities are just. In any case, compliance is unforced and voluntary.

Naturally, the authorities prefer voluntary compliance. From their point of view, the normative is preferable to the instrumental perspective since the former does not require enforcement. If the public already believes in the government's moral right to govern, the authorities' job is made much easier.

Morality, however, can work against the government, as it did with the U.S. public's moral indignation over the Vietnam conflict. Those who viewed the government's authority as legitimate supported the war, regardless of their own views as to its necessity. Others considered the ongoing struggle useless and wrong and opposed it.

Another significant difference between the instrumental and the normative perspectives is whether one focuses on procedures rather than results. Those adhering to the normative point of view will, for example, be more concerned with being treated justly in court rather than with winning or losing their case. They will contentedly await judgment if dealt with fairly. People of this opinion are interested in neutrality, lack of bias, honesty, politeness, and respect for one's rights. The "due process," then, is most effective in promoting compliance to those of this view. The instrumentalist, on the other hand, focuses on the outcome of his case and is less concerned with procedures. In his mind, a procedure is fair if it is favorable.

Legitimacy and Compliance

Legitimacy

Legitimacy is regarded as the essential ingredient in what gives governments and leaders authority. The idea is that if the authorities have legitimacy, the public will obey the law.

By definition, effective leadership must produce compliance with a leader's decisions. However, when new legislation or policy is introduced, public support and compliance do not always occur. Court decisions or legislative decrees do not necessarily produce general public acceptance of or adherence to policy. Likewise, if a company introduces a new policy that no employee may take a gift (no matter how small) from a potential vendor, many employees will continue to take small gifts anyway.

Altering citizens' behavior by manipulating access to valued resources or threatening to impose sanctions is known as *social control*. Once again, the concept is that reward and punishment are what cause people to obey the law. People maximize their personal gain and comply based on deterrence. Of course, life is more complicated than reward and punishment. Otherwise, the job of law enforcement would be easy. But social control appeals to authorities. The public understands deterrence, rewards, and punishment. In contrast, emphasizing the normative approach places power not in authorities, but in the people whose voluntary compliance is sought.

In studying general compliance with the law, sociologists have found that the instrumental perspective does not fully explain why people obey the law. Citizens choose to obey the law when the chances of being caught violating it are virtually zero, as when one might come upon a stop sign in a deserted street. Almost all citizens pay their income taxes in a voluntary system, even though the chances of being caught shaving taxes owed are small. Yet some

citizens break the law when it is risky to do so, as when they buy illegal drugs or embezzle thousands of dollars from their company.

In a democracy, the legal system cannot function if it can influence people only by manipulating rewards and costs. The resources required to enforce such a regime are too high. Deterrence is expensive to enforce and does not guarantee an adequate level of obedience. Drunk driving is a good example. Studies show that an extremely high investment of resources is needed to convince people that the likelihood of being caught and punished for driving drunk is high. Public campaigns against drunk driving tend to temporarily reduce the number of DUIs or DWIs. As long as citizens think the chances of being caught are rising, the incidences of drunk driving remain lower. However, as soon as public perception of increased vigilance against drunk driving lessens, the number of arrests goes up again. Likewise, as is discussed later in the "Fraud Prevention Programs" chapter, increasing the perception of detection is a powerful anti-fraud program. If an employee thinks that his company is not paying attention to occupational fraud, then some employees are more likely to try to get away with it.

Consider the use of marijuana, an illegal yet still popular drug in many countries. If the reason people abstain from using this drug is that they believe in complying with the law, then obviously the authorities have legitimacy in their eyes. However, if they forgo marijuana use because it violates their moral values, then it is their convictions that are the deciding factor. If fear of legal punishment stops them, then deterrence carries greater weight with them. And if they refrain out of fear of social ostracism, then the social group's influence prevails.

A person's own normative values have the final say about appropriate behavior. Unlike the reward and punishment approach, one's own values are what produce compliance or noncompliance with the law in the end. Psychologists refer to this as "internalized obligations," for which citizens take personal responsibility.

Voluntary Compliance

Voluntary compliance matters only to the extent to which it produces obedience that goes beyond self-interest, measured by most of us by reward and punishment. A normative speeder, for instance, will accept being a few minutes late to his appointment in order to obey the speed limit, thus making the roads safer for everyone. A normative employee will accept a salary freeze and not steal from the company to make up for the raise he was

promised. In other words, these people will act against their own best interests if they feel compliance with the rule is of greater moral import.

Of course, government authorities recognize that without the good will of the public, they could not function. Their aim must be to maximize compliance and minimize hostility toward laws, while gaining legitimacy in the eyes of the public. Any leader who wants to effectively govern must have legitimacy with his subordinates. The same is true for employers, managers, teachers, and army sergeants. Otherwise, compliance will not occur.

Due to its significant social impact, social scientists and politicians have found legitimacy to be an issue of major concern. It is seen as a reservoir of loyalty from which leaders can draw. Opinion polls on the public's attitude toward the law and the government are really about public confidence in the government's legitimacy. If the public does not have confidence in the legal system, obedience to laws is unlikely.

Studies show that both children and adults feel a strong obligation to obey the law. Whether we can attribute this to their normative values or the legitimacy of the authorities is the real question. Naturally, those who view the authorities as legitimate are more likely to comply. This leads to the conclusion that normative support of the system results in compliant behavior.

Measuring Legitimacy and Compliance

Tyler conducted a study (called the Chicago Study) to test the concept that if authorities have legitimacy, the public will obey the law. The study focused on six laws with which people deal on a daily basis: disturbing the peace, littering, driving while intoxicated, speeding, shoplifting, and parking illegally. Participants were asked how often they had broken these laws in the past year. Most admitted to parking illegally (51 percent) and speeding (62 percent), but very few admitted to shoplifting (3 percent). Twenty-seven percent confessed to disturbing the peace, 25 percent to littering, and 19 percent admitted to having driven while under the influence.

The second wave of interviews, in which participants were asked about a shorter time frame, produced similar results. To measure fear of punishment, respondents were asked how likely they thought it was that they would be arrested or issued a citation if they violated these six laws. Eighty-three percent thought it was likely that they would be caught driving drunk; 78

percent thought the same for parking violations and shoplifting; 72 percent for speeding; 35 percent for disturbing the peace; and 31 percent for littering.

Participants were then gauged for peer approval. For shoplifting, 89 percent said that they thought that the five adults they know best would disapprove. Eighty-six percent said the same for drunk driving, as did 51 percent for littering, 52 percent for speeding, 44 percent for illegal parking, and 53 percent for disturbing the peace.

The next question was designed to measure respondents' morality. They were asked whether each offense was "wrong." Almost every one of the participants felt that any violations of the six laws were wrong. Speeding came out as the least immoral and shoplifting the most, with 99 percent of participants considering it morally objectionable.

One sees that citizens seem to view the breaking of laws as a violation of their personal morality. Interestingly, most believe the chances of getting caught are high. And since peer disapproval levels are relatively light, one can gather that the social group is the source of the least amount of pressure to obey laws.

More than four out of five participants felt a person should obey the law "even if it goes against what they think is right." Almost as many respondents felt that disobeying the law is seldom justified and that obedience and respect for authority are the most important virtues children should learn.

The study did show that legitimacy is related to compliance. Participants who attributed greater legitimacy to authorities were more likely to obey the law, for instance. This does not prove a causal relationship, though. The results of the study were analyzed to account for demographic and sociological factors. This "regression analysis" suggests that legitimacy has a significant effect on compliance, regardless of the other factors.

Certainly, legitimacy's impact on a person is influenced by his personal experiences with police and courts. A person who feels mistreated by the authorities is certainly less likely to have confidence in their legitimacy and, therefore, is less likely to obey laws. In such cases, peer approval seems to take on greater importance in those people's thinking. One more interesting result was that those participants who considered themselves politically liberal were more likely than those who regarded themselves as moderate to base compliant behavior on feelings of legitimacy.

Implications of the Chicago Study

Authorities do not take compliance with the law for granted. They often find that occasional noncompliance must be tolerated. Sometimes noncompliance is so widespread that it casts doubt upon the effectiveness and validity of the law itself. Prohibition, for example, was widely and often openly violated before its repeal. The results of the Chicago Study suggest that normative values are more influential upon compliance than the reward and punishment approach. This is consistent with Skinner's behavioral theories discussed previously.

Again, the Chicago Study shows that people have a high level of normative commitment to abide by the law. Most participants felt that breaking the law was morally wrong and that laws should be obeyed even when one does not agree with them. Authorities who can tap into and encourage those views will inspire compliance. Similarly, employees who have a strong sense of loyalty to their employer will not violate company policies because such acts would be a betrayal to the company.

THE PSYCHOLOGICAL VARIABLES

The Chicago Study was designed to gauge the gap between citizens' concerns for favorable outcomes and procedural fairness. It also measures the extent to which fairness influences reactions to experience. The experience in question is of the everyday, average-citizen variety—the type of encounter most of us have with authorities over relatively minor matters. Participants reported calling the police for a number of reasons: accidents, disturbances, suspicious activities, and crimes against property or violent crimes. The majority of callers felt it was important for the police to solve their problem, whether it was serious or not.

Police response time was satisfactory to most respondents. Only 15 percent felt that the police did not respond quickly enough. Nearly 70 percent knew what actions the police had taken to solve the problem, and almost two-thirds of those said that the police settled the situation. The 43 percent who said that the police failed to solve their problem admitted that the police did everything they could. All in all, 71 percent said they were satisfied with the outcome of their call. Most respondents also felt that they were treated quite well by the police. Eighty-six percent expressed overall satisfaction with their politeness, concern for their rights, propriety, attentiveness, honesty, and willingness to consider their opinions.

Respondents who were stopped by the police had less magnanimous feelings toward them. Still, 73 percent of those who received tickets for minor offenses considered the outcome fair, acknowledging that the ticket was deserved.

Satisfaction levels of participants who had to go to court were similarly high: 80 percent considered their treatment fair. However, 36 percent stated that they believed the judge could have reached a better outcome. Overall, though, participants were content with these elements of our justice system.

LEGITIMACY AND EXPERIENCE

Most people will accept unfavorable rulings if they believe they were dealt with fairly. Thus, fair procedures can cushion the blow of an outcome that is to one's disadvantage, without damaging the authorities' legitimacy. Of course, fair procedures can only go so far. If fair procedures consistently produce unfavorable results, the fairness of the procedures will come into question.

People typically place importance on procedure for several reasons, the first of which is simplicity. Often, the result itself is difficult to classify as fair or unfair. People, therefore, focus on the steps that lead up to the outcome. Another reason such emphasis is placed on procedures is that, with as much religious and ethnic diversity as there is around the world, people do not always concur on what is fair. Although most people might not necessarily agree upon the outcome, they are usually of one mind as to the justice of the procedures.

The procedural aspects of the law and how the public perceives them must be of great importance to authorities. Policymakers must have a good idea of what the public considers fair. If the public perceives a court's legal actions as just, they will support the outcome although it might not be to their advantage. For example, in jurisdictions that offer plea bargaining, the practice of negotiating a deal with a criminal defendant is often justified based on outcome. But if the inconsistency in plea agreements is seen as unfair, support for the legal system will weaken.

The same is true in the corporate environment. Employees will often accept unpopular company policies if the employees feel that the policy is applied "fairly." For instance, employees might be upset that the company provides only three paid sick days, but if the rule is applied to all employees in an equal manner, most employees will live with the policy. However, if some employees are allowed additional sick days and others are not, employees

begin to resent the policy and the company. In other words, these employees feel they are being treated unfairly.

THE MEANING OF PROCEDURAL JUSTICE

An important issue left unaddressed until now is how people decide which procedures are fair and which are not. Previous efforts to study this question have focused on control. Two areas of control with which people are generally concerned are *decision control* (control over the actual decisions made) and *process control* (control over the opportunity to state one's case).

To better illustrate, let us take the example of an attorney representing a client in court. While the client surrenders control of the case to his attorney, he might still seek to maintain as much control as he can through control of the process. According to the instrumental perspective, he will value the opportunity to testify only insofar as it helps to achieve a beneficial outcome to his case. Studies show, however, that most of us appreciate the chance to air our views, regardless of whether it influences the outcome or not. From this, one can conclude that process control has an independent impact on how one perceives fairness and whether one is satisfied with the outcome (one's satisfaction with the outcome and one's opinion of fair procedures depends largely on one's degree of control).

Again, one must ask what criteria people use to decide whether a procedure is fair. G. S. Leventhal proposed six standards for evaluating the fairness of a procedure:[7]

- Representativeness
- Consistency
- Suppression of bias
- Accuracy
- Correctability
- Ethicality

Representativeness relates to those parties whose concerns are affected throughout the allocation process. *Consistency* refers to the uniform and unbiased treatment of all of the affected parties. *Suppression of bias* guarantees that those involved with the outcome have no personal, vested interest in the case. This also prohibits a participant's reliance on previously

[7] G. S. Leventhal , "What Should Be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships." In K. Gergen, M. Greenberg, and R. Willis, eds., *Social Exchanges: Advances in Theory and Research* (New York: Plenum, 1980), 27–55.

formed opinions rather than just the evidence at hand, as when a juror convicts because he believes most defendants are guilty. *Accuracy* refers to objective high quality. *Correctability* involves the checks and balances provided in the system, which allow unfair decisions to be corrected, such as the appeals process. *Ethicality*, of course, involves the degree to which procedures meet generally held ethical standards of fairness and morality. Torture, for instance, is a violation of ethicality, as it is a breach of basic moral codes.

Studies measuring the importance of Leventhal's six criteria show that people place the most importance on consistency. Accuracy, representativeness, and suppressing bias are also highly valued.

Based on Tyler's Chicago Study, it appears likely that, in encounters with the police, people are more concerned with fairness than with the policeman's adherence to formal issues of rights (i.e., ethicality). In the courtroom, however, ethical standards and rights receive greater emphasis.

People's views on procedural fairness are affected by two factors: background characteristics and prior views. Race, education, income, sex, age, and political views are the most important background characteristics. Those who are liberal and better educated will place the most emphasis on ethicality when deciding if a procedure is just. Minorities are more likely to focus on consistency and suppression of bias, though. Prior views, formed perhaps from past experiences, carry more weight than background characteristics. Any background characteristic is certain to be overridden by one's prior views on a subject.

INFLUENCE OF CONTROL ON THE MEANING OF PROCEDURAL JUSTICE

The Chicago Study assessed process control by questioning respondents about how much opportunity they had to state their case or present their problem. Decision control was measured by asking how much influence participants had over the determinations made by the third party in control. Most participants felt they had a high (43 percent) to moderate (20 percent) level of process control. In contrast, a number of participants felt they had little decision control (about half said "not much at all").

The Chicago Study thus indicates that process control judgments are the deciding factor when assessing procedural justice in terms of control. Process control judgments are also important in assessing how experience affects people's evaluation of procedural justice. Consequently, respondents are more concerned with their opportunities to speak out rather

than their influence over the outcome. The belief of citizens that their views are being weighed and considered by the authorities and that the authorities are dealing fairly with them reinforces their belief in their own process and decision control.

In the employment context, the Chicago Study tends to support the idea that employees should be involved in the development of policies and procedures. Instead of just distributing a fraud policy or an ethics policy, send out a questionnaire asking employees for their ideas on how fraud and corruption can be prevented in the company. If employees feel they have some control over the rules, they will be more likely to obey and follow them.

Theories of Crime Causation

Understanding human behavior and why people obey the law helps explain some of the reasons people commit fraud. However, there have been a number of theorists who have attempted to explain specifically why people commit crimes. In more sophisticated sciences, such as chemistry and physics, theories build on one another as new facts emerge from studies prompted by the reigning theories. In criminology (as in virtually all the social sciences), theories compete with one another for acceptance, with none of them adequately satisfying either practitioners or scholars in the field.

The reason for this jumble of interpretations of criminal activity largely lies in the fact that human beings, unlike inanimate objects, think for themselves. You can push a rock in a certain direction and it will (all other things being equal) move in that direction. But you cannot predict as simple a matter as the direction in which a human being might decide to proceed when confronted with a choice. Perhaps you can guess that he will go to the right because you know that this is the direction in which the store he wants to go to lies. But any human being, for reasons that satisfy him, can decide on any given day that he prefers to go to the left, perhaps just to saunter around or to get extra exercise, or for no particular reason that seems evident to him or to others. Imagine how much more difficult it is to try to predict very complicated human behaviors, such as criminal acts.

The following sections summarize some of the better-known criminological theories, both past and present.

Classical Criminology

Classical criminology, based on the philosophical principle of *utilitarianism*, has its roots in the belief that human beings are rational and calculating creatures and, therefore, do things in order to avoid pain and produce pleasure. Some of the components of classical criminological theory are:

- People have free will, which they can use to elect to engage in either criminal or noncriminal behavior.
- Criminal behavior will be more attractive if the gains are estimated to be greater than the losses.
- The more certain, severe, and swift the reaction to crime, the more likely it is that the penalties will control the behavior.

Two theorists' names are most frequently associated with classical criminology: the Italian Cesare Beccaria and the Englishman Jeremy Bentham. (Bentham, marvelously eccentric, willed that his body be preserved and placed in the entryway to the University of London and brought to the table when the faculty meets. His wishes were carried out; the body can still be seen today by anyone visiting the school.)

The policy implications of classical criminological thought, which are prominent today in theories grouped under the heading of "rational choice," are that penalties should be established that make the anticipated results of criminal behavior less appealing than the prospects of the losses, such as the loss of freedom. The theory also has a benevolent component in that it suggests that penalties that are too severe serve no purpose, since they are needlessly excessive for the deterrence they seek to achieve.

Utilitarianism remains a much-favored approach to crime, with its assumption that offenders will calculate potential gains and losses before they decide to disobey the law. Corporate sentencing guidelines, for example, are based almost totally on the idea of classical criminology, mandating that monetary penalties be calculated at a level that will induce companies to conclude that breaking the law is not fiscally appealing.

There are several major difficulties inherent in the theory, though. The first is that many people do not stop and add up the gains and losses of lawbreaking before they engage in it. Second, the impact of penalties can be very different for different people; the thought of a week in prison might be awful to one person, but a piece of cake to another. Third, it is very

difficult to know whether the penalty will, in fact, result from the behavior; most offenders optimistically assume that they will not be caught.

Routine Activities Theory

Routine activities theory, a variation of classical theory, holds that both the motivation to commit crime and the supply of offenders is constant. There will always be a certain number of people, motivated by greed, lust, and other forces, who are inclined toward lawbreaking. The determining factor, particularly in predatory crimes, such as those involving violence and theft, are the activities of potential victims. There are three important elements that influence crime:

- The availability of suitable targets, such as companies and individuals
- The absence of capable guardians, such as auditors and security personnel
- The presence of motivated offenders, such as unhappy or financially challenged employees

Biological Theories

Biological theories maintain that criminal behavior is not the result of choice (the calculation of benefits and potential losses), but rather is caused by the physical traits of those who commit crime. The foundations of biological theory were laid by Cesare Lombroso, an Italian doctor, who insisted that there were born criminals—people who were atavistic, or a throwback to more primitive human types. Lombroso spent his career measuring the bodies of offenders and concluded that they were marked by a high degree of asymmetry, with such things as sloping foreheads and other "anomalies." Later critics would point out that Lombroso used no control group—that is, he did not measure people who were not criminals. If he had done so, he would have found that they shared equally in those kinds of traits that Lombroso presumed were indicative of criminal propensities.

Biological theory continues to evolve, with theorists seeking to locate genetic distinctions between those who break the law and those who obey it. In their book, *The Bell Curve*, Richard Herrnstein and Charles Murray argued that low intelligence and crime are intimately connected, and that low intelligence (as measured by I.Q. scores) is genetically transmitted. Some scholars in the field savaged the Herrnstein-Murray position, but it received a good deal of media attention.

Biological theorists now take a much less deterministic position than Lombroso. They will point to this or that human characteristic and say that it is apt to produce illegal acts, given

certain environmental circumstances. Put another way, they report that they have found a large number of offenders with a biological trait, but that there are many more that have the trait who never get into any trouble with the law.

Psychological Theories

Theories rooted in psychology are based on the view that criminal behavior is the product of mental processes. The psychoanalytical ideas of Sigmund Freud focus on early childhood development and on unconscious motivations—that is, motivations of which the offender himself is not aware. Freud identified a three-part structure to human personality: the *id* (the drive for food, sex, and other life-sustaining things), the *superego* (the conscience that develops when learned values become incorporated into a person's behavior), and the *ego* (the "I," or the product of the interaction between what a person wants and what his conscience will allow him to do to achieve what he wants).

Cognitive and Personality Theories

Cognitive theories stress inadequate moral and intellectual development as lying at the root of criminal acts. There are also *personality theories*, which illustrate the belief that traits such as extroversion are responsible for a significant amount of crime.

Integrated Theories

Integrated theories draw from choice theory, biological theory, and psychological theory. One such argument is put forward by James Q. Wilson and Richard J. Herrnstein in their book *Crime and Human Nature*. Wilson and Herrnstein maintain that, while criminal activity is a choice, this choice is heavily influenced by biological and psychological factors. They also explore social factors. The factors include family life, schools, and gang membership.

Conditioning Theory

H. J. Eysenck, working with what he calls *conditioning theory*, argues that the failure of a person to incorporate satisfactorily the rules of society represents the major explanation for subsequent criminal behavior. Eysenck maintains that extroverted persons, both normal and neurotic, are more difficult to condition—that is, to train—than introverted persons, and that extroverts, therefore, get into more trouble than introverts.

Another psychological theme is that frustration is the precursor of aggression. The theory suggests that the expression of aggression, such as a fraud perpetrator "getting back" at his

employer, will alleviate the frustration and allow the organism to return to a more satisfactory state.

Social Structure Theories

These theories concentrate on the kinds of societies that generate particular levels of crime. Why is the crime rate in Japan so much lower than in the United States? Why do many Central American countries typically have high rates of homicide while Hong Kong's homicide rate is notably low? There are various kinds of sociological theories, all based on similar premises but with differing emphases.

As a group, social structure theories suggest that forces operating in the lower-class areas of the environment push many of their residents into criminal behavior. Social structure theorists challenge those who would suggest that crime is an expression of psychological imbalance, biological traits, personal choice, etc. They argue that people living in equivalent social environments seem to behave in a similar, predictable fashion.

Theory of Anomie

Strain theories are a branch of the social structure theory. Strain theorists view crime as a direct result of the frustration and anger people experience over their inability to achieve the social and financial success they desire. The best-known strain theory is Robert Merton's *theory of anomie*. Robert Merton, a Columbia University sociologist, maintained that the discrepancy between what people are indoctrinated into desiring and the ways that are available to them to achieve such ends is the cornerstone for explanation of criminal behavior.

Merton's theory of anomie (that is, normlessness) was derived from the work of Emile Durkheim, a French sociologist who adopted the term in his effort to explain suicide rates among different social groups. For Merton, anomie in the United States was characterized by an almost overpowering emphasis on the acquisition of things and on the fact that social status and importance is usually measured in terms of money.

People can obtain money and material goods, Merton noted, by conforming—that is, by working at jobs and engaging in other legal enterprises that pay off. They can also withdraw from the fray, saying that they will not be driven by a desire for goods, but will opt out of the game that dominates society. The most withdrawn often tend to be those who employ illegal drugs to provide their satisfactions. Then there are the *innovators*—those who refuse to

play by the accepted rules of the game, but turn to outlawed methods to accomplish what society has told them that they must achieve to be acceptable members.

Social Process Theories

Not all sociologists believe that a person's social structure alone controls the direction of his values, attitudes, and behavior. After all, most people who reside in even the most deteriorated urban areas are law-abiding citizens. *Social process theories* hold that criminality is a function of individual socialization and the social-psychological interactions people have with the various organizations, institutions, and processes of society.

Though they differ in many respects, the various social process theories all share one basic concept: All people, regardless of their race, class, or gender, have the potential to become criminals.

Social Learning Theories

Social learning theories hold that criminal behavior is a function of the way people absorb information, viewpoints, and motivations from others, most notably from those with whom they are close, such as members of their peer group. Social learning theorists believe that all people have the potential to commit crime if they are exposed to certain kinds of circumstances. All people raised in France by French parents learn to speak that language; Poles learn to speak Polish. So, too, will a person raised with attitudes that favor criminal acts respond by committing such acts, and the person raised and living in an environment where criminal activity would be unthinkable will avoid crime; crime might not even occur to him as a solution to whatever problem is confronting him.

Theory of Differential Association

The theory of differential association is undoubtedly the best-known among all explanations offered in the United States to account for crime, though it, too, has been widely criticized on the grounds that it is just about impossible to test.

The theory first appeared as a systematic formulation in 1939 in the third edition of Edwin H. Sutherland's *Principles of Criminology*. Later, Sutherland would make his best-known contribution to criminology by coining the phrase *white-collar crime* and writing a monograph on the subject. Sutherland was particularly interested in fraud committed by the elite upper-world business executive, either against shareholders or the public. Sutherland said:

> *General Motors does not have an inferiority complex, United States Steel does not suffer from an unresolved Oedipus problem, and the DuPonts do not desire to return to the womb. The assumption that an offender may have such pathological distortion of the intellect or the emotions seems to me absurd, and if it is absurd regarding the crimes of businessmen, it is equally absurd regarding the crimes of persons in the economic lower classes.*[8]

The theory of differential association begins by asserting that criminal behavior is learned. Explicating that idea, Sutherland specifies as a second point that criminal behavior is learned in interaction with other persons in a process of communication. If individuals acquiring criminal habits or propensities were exposed to situations, circumstances, and interactions totally of a criminal nature, it would be relatively easy to comprehend how this process of communication operates. In view of the enormous variation in standards and personalities to which any individual in our society is exposed, it becomes exceedingly difficult to discern those critical elements that induce criminal behavior without the intervention of some additional principle.

Sutherland's third point is that criminal behavior is acquired through participation within intimate personal groups. This particular stress suggests that the roots of crime must be sought in the socializing experiences of the individual. Unfortunately, the process of socialization is far from being adequately understood. Sutherland's fourth point indicates that the criminal learning process includes not only techniques of committing crime, but also the shaping of motives, drives, rationalizations, and attitudes. Crime techniques often involve a high degree of skill; picking pockets (and not getting caught) demands considerable adroitness, and being a successful prostitute demands knowing how to hustle customers, collect money, buy police protection, and deal with a drunken or violent john.

Fifth, Sutherland narrows his focus by indicating the kinds of pressures that move the learning process in the direction of acceptance of illegal pursuits. Careful to keep within the legal definitions of behavior, Sutherland stipulates that the specific direction of motives and drives is learned from definitions of the legal codes as favorable or unfavorable.

And sixth, he sets out his core point by establishing the principle of "differential association." According to this postulate, a person becomes a criminal because of an excess

[8] Gilbert Geis, *On White-collar Crime* (Lexington: Lexington Books, 1982).

of definitions favorable to violation of the law over definitions unfavorable to violation of the law. Then, as a means of demonstrating with greater clarity the character of associations that have a subsequent effect on behavior, Sutherland states his seventh point—that differential association may vary in frequency, duration, priority, and intensity. But there is no suggestion regarding which of these elements is apt to be more important than the others. Frequent contacts might promote feelings of boredom and indifference; one intense experience might overwhelm all prior learning, or it might not. The axiom hardly helps us much in unraveling the causal contents of crime.

Sutherland's eighth point concerns the nature of learning and, again, is primarily a didactic statement of common behavioral science understanding rather than a contribution that moves the theory very far forward: Learning criminal and delinquent behavior, Sutherland asserts, involves all the mechanisms that are involved in any other learning. The key problem is not that Sutherland is wrong; it is that he casts into the spotlight a theoretical problem that has plagued students of human behavior since time immemorial. If crime is to be understood as learned like anything else—say, basketball skills, cooking, patriotism, and flirting—then any theory that can unravel its ingredients will, at the same time, have to set before us an understanding of all human action. Sutherland's propositions can hardly pretend to approach so stunning an intellectual achievement and, in this respect, can be regarded as extraordinarily overambitious or, perhaps, simplistic.

As his next to last proposition, Sutherland stresses that learning differs from pure imitation. His last point is a worthwhile reminder that, while criminal behavior is an expression of general needs and values, it is not explained by these general needs and values because noncriminal behavior is an expression of the same needs and values. This injunction indicates that the generalizations sometimes employed to account for crime—such as the view that people steal because they crave esteem or are greedy, or kill because they are unhappy—have little scientific merit. People, both criminals and noncriminals, are motivated by much the same needs and values. They become or do not become criminals on the basis of their unique responses to common drives for prestige, happiness, success, power, wealth, and numerous other human aspirations. An individual might feel a pressing need for money and take an extra weekend job pumping gas; alternatively, he might try to borrow from a friend or shrug his shoulders and figure that, this time, he'll do without. Another person, feeling the same need, might hold up a fast food outlet.

Social Control Theory

Travis Hirschi, in his book, *Causes of Delinquency*, first articulated the *social control theory*. A particularly important reason for the current dominance of control theory as the interpretative scheme for understanding crime and delinquency is that, unlike theories such as differential association, it offers a considerable number of testable propositions. Such propositions take the form of if-then statements: If something exists or is done, then it foretells that something will follow. Such formulations allow for experimental testing and rebuttal.

Control theory takes its cue from a classic of sociology, Emile Durkheim's *Suicide*, in which the French theoretician wrote:

> *The more weakened the groups to which [the individual belongs], the less he depends on them, the more he consequently depends on himself and recognizes no other rules of conduct than what are founded on his private interests.*[9]

Essentially, control theory argues that the institutions of the social system train and press those with whom they are in contact into patterns of conformity. Schools train for adjustment in society, peers press the ethos of success and conventional behavior, and parents strive to inculcate law-abiding habits in their youngsters—even, Hirschi stresses, parents who themselves sometimes violate the rules. The theory rests on the thesis that, to the extent that a person fails to become attached to the variety of control agencies of the society, his chances of violating the law are increased. This doctrine edges very close to being self-evident in its insistence that close affiliation with law-abiding people, groups, and organizations is predictive of law-abiding behavior; however, it is notably rich with subordinate statements, some of them far from obvious.

Four aspects of affiliation are addressed by the theory:

- Attachment
- Commitment
- Involvement
- Belief

[9] Emile Durkheim, *Suicide: A Study in Sociology,* translated by John A. Spaulding and George Simpson (New York: The Free Press, 1951), 209.

Attachment refers primarily to affection-type ties with people such as parents, teachers, and peers. *Commitment* refers to cost factors involved in criminal activity. People are committed to conventional behavior and probably have invested something—fiscally and emotionally—in their ultimate success—an investment that they are wary of risking by means of a criminal act. Commitment might involve things such as obtaining a better job or seeing one's children succeed. *Involvement* concerns matters such as time spent on the job—that is, participation in activities related to future goals and objectives. *Belief* refers to a conviction about the legitimacy of conventional values, such as the law in general and criminal justice prescriptions in particular.

Hirschi insists that there is no important relationship between social class and delinquency and crime; thus, a person in any class—lower, middle, or upper—who defaults on liaisons with the important formative agencies in our society will be more apt to find himself on a path that ends in crime. Among the important considerations is that control theory "assumes the bond of affection for conventional persons is a major deterrent to crime. The stronger this bond, the more likely the person is to take it into account when and if he contemplates a criminal act."[10] What essentially happens, the theory suggests, is that people confronted with the possibility of violating a law are likely to ask themselves questions such as, "What will my spouse—or my mother and father—think if they find out?" To the extent that individuals believe that other people whose opinions are important to them will be disappointed or ashamed, and to the extent that they care deeply that these people will feel this way, they will be deterred from committing a criminal act.

Differential Reinforcement Theory

Differential reinforcement theory is another attempt to explain crime as a type of learned behavior. It is a revision of Sutherland's work that incorporates elements of psychological learning theory popularized by B. F. Skinner and the social learning theory discussed previously. The theory was summarized by Ronald Akers in his 1977 work, *Deviant Behavior: A Social Learning Approach*.

According to these behavioral theorists, people learn social behavior by *operant conditioning*—behavior controlled by stimuli that follow the behavior. Behavior is reinforced when positive rewards are gained or punishment is avoided (negative reinforcement). It is weakened by negative stimuli (punishment) and loss of reward (negative punishment). Whether deviant or

[10] Travis Hirschi, *Causes of Delinquency* (Piscataway, NJ: Transaction Publishers, 2002), 83.

criminal behavior is begun or persists depends on the degree to which it has been rewarded or punished, as well as the rewards or punishments attached to its alternatives. This is the theory of differential reinforcement.

WHITE-COLLAR CRIME

What Is White-Collar Crime?

Since the term was first used, there have been constant disputes regarding what is (or should be) the definition of *white-collar crime.* The designation was coined by Edwin H. Sutherland in December 1939 during his presidential address in Philadelphia to the American Sociological Society. Ten years later, Sutherland published *White Collar Crime,* in which he offered an arguable, vague definition of the concept in a footnote: White-collar crime was said to be "Crime in the upper, white-collar class, which is composed of respectable, or at least respected, business, and professional men." These crimes were confined to acts performed by white-collar persons in occupational roles, thereby excluding "most of their cases of murder, adultery, and intoxication, since these are not customarily a part of their occupational procedures."[1]

A few pages after this definitional foray, Sutherland illustrated white-collar crime through examples of thefts by chain-store employees and overcharges by garage mechanics and watch repairers. There was little consistency between his definition and his illustrations of what might fall within it.

Nonetheless, the term *white-collar crime* has been widely incorporated into popular and scholarly language throughout the world, though the designation *economic crime* is sometimes used as well. The difficulty with *economic crime* is that so many illegal acts, including murder, are often committed in order to achieve economic gain. The United Nations, for its part, adopted the phrase *abuse of power* for those behaviors that correspond to white-collar crimes as defined by Sutherland. In addition, other designations, such as *upperworld crime*, *crimes by the powerful*, *avocational crime*, *crime in the suites*, and *organizational crime*, have been employed to designate more or less the same phenomena as white-collar crime.

A major difficulty with the concept as formulated by Sutherland is that he is designating an offense category that has no equivalent in the law. Certain statutory offenses can be identified as those that, by and large, will be committed by persons in the elite classes—offenses such as antitrust violations and insider trading—but what is to be done definitionally with, say, the proofreader, who is paid little more than minimum wage and learns from information that he is working on of a merger between the company and one of

[1]Edwin H. Sutherland, *White Collar Crime* (New York: Dryden Press, 1949), 9.

its strong competitors? He buys stock and reaps a considerable profit, but is then caught and prosecuted as an inside trader. Is this person to be regarded as a white-collar criminal?

The *Dictionary of Criminal Justice Data Terminology*, published by the U.S. Federal Bureau of Justice Statistics, defines *white-collar crime* as:

> *Nonviolent crime for financial gain committed by means of deception by persons whose occupational status is entrepreneurial, professional, or semi-professional and utilizing their special occupational skills and opportunities; also nonviolent crime for financial gain utilizing deception and committed by anyone having special technical and professional knowledge of business and government, irrespective of the person's occupation.*[2]

This definition certainly catches in its net a wide array of wrongdoers. But critics fault it for its explicit omission of violent offenses. What about a doctor who knowingly performs unnecessary surgery in order to collect a large fee and ends up causing the patient to die? Or how about the numerous deaths and injuries from toxic wastes, polluted air, and violations of health and safety regulations? Are such results not the product of white-collar crime?

Though there is no formal consensus within the scholarly community, another definition of *white-collar crime* proposed by Albert J. Reiss, Jr., and Albert Biderman is more all-encompassing:

> *White-collar crime violations are those violations of law … that involve the use of a violator's position of economic power, influence, or trust in the legitimate economic or political institutional order for the purpose of illegal gain, or to commit an illegal act for personal or organizational gain.*[3]

Opportunity is an important ingredient of white-collar crime. An unemployed youth needing funds might turn to armed robbery or burglary. He is in no position to violate the antitrust laws, though doing so might well provide him with a great deal more funds and lesser likelihood of being caught. The bank president or the company chief executive, for their part, can deal with a personal cash shortage through a variety of illegal tactics that are tied to

---

[2] U.S. Department of Justice, Bureau of Justice Statistics, *Dictionary of Criminal Justice Data Terminology* (Washington, DC: National Institute of Justice, U.S. Department of Justice, 1981), 215.

[3] Albert J. Reiss, Jr., and Albert Biderman, *Data Sources on White-Collar Law-Breaking* (Washington, DC: National Institute of Justice, U.S. Department of Justice, 1980).

their business position. Criminals will often commit offenses in ways with which they are most familiar, can most easily accomplish, and have the lowest likelihood of dire consequences. An often-unheralded bonus of social status is access to opportunities for less dirty, "more decent" kinds of crime.

Crimes of the Middle Classes—A Look at White-Collar Crime

Many surveys on the public perception of white-collar crime provide essentially the same result—that the public, as a whole, regards white-collar offenses as serious matters. The difficulty with such surveys, however, is that they fail to convey in any effective manner the complexity of the white-collar offenses and the status of the offenders. It is one thing for a respondent to say that he regards toxic waste offenses that produce death as very serious violations, but quite another for that person to regard the corporate executive responsible for such matters as an "evil" person. Because of this, white-collar offenders receive much less severe penalties than the street people who commit the offenses that the public generally regards to be as serious as theirs.

The debate over just what constitutes a white-collar crime, and what drives the white-collar criminal, has been raging ever since Sutherland's seminal work. The authors of *Crimes of the Middle Classes* offer a contribution that, for the most part, avoids theory-building, offering instead a statistical report of offenders convicted in federal court.[4]

Using U.S. federal court records, and an unprecedented access to probation officers' presentencing investigation reports (PSIs), the authors determined that most people convicted of white-collar crimes are not upper class; that social status has only an indirect significance; and that, once a conviction is attained, higher status often means a stiffer sentence. White-collar crime does have a unique place in criminology, but the split is not between an underworld of the desperate poor and an elite universe of high-stakes shysters. White-collar crime has some relation to both of these mythological worlds, but is largely the province of the middle classes, where organizational position is more important than pedigree and personal situations are more forceful than sociological trends.

[4] David Weisburd et al., *Crimes of the Middle Classes. White-Collar Offenders in the Federal Courts* (New Haven: Yale University Press, 1991).

Profiles of Offenders

The wide array of crimes called "white collar"—from antitrust and securities violations to bank embezzlement and credit fraud—makes assembling a profile of the typical offender difficult, but not impossible. Most defendants are white males, with a moderate social status. They are slightly more likely than the general population to have a high school diploma (78 percent versus 69 percent) or a college degree (24.7 percent versus 19 percent for the general public). The majority, then, are not highly educated and, in at least one category, owning one's home, the offenders fall behind the average citizen: While 55 percent of Americans own their homes, only 45.3 percent of the offenders do. Social status is a factor in white-collar criminality, but, as the authors point out, "The position conferred by status, rather than status itself, empowers the offender."[5] So, a corporate manager who was promoted from inside the company with only a ninth-grade education and who doesn't own his home is not as atypical an offender as might be supposed. The key is that, by his position in his company, he has the opportunity and means to commit a crime.

Cressey Study

In his 1953 study of embezzlers, Donald R. Cressey found that most of those he examined "had lived beyond their means for some time before deciding to embezzle."[6] *Crimes of the Middle Classes* extends this statement more generally, remarking, "The most interesting fact about the white-collar offenders' aggregate financial status is not the value of their assets but the extent of their liabilities." Offenders often "have the material goods associated with successful people, but may barely be holding their financial selves together."[7] These people have assembled a structure of respectability, but it is often built on a foundation of debt. The Cressey Study is discussed in more detail later in this chapter, in the section on "Occupational Fraud."

Effect of Status

What is loosely called "class" or "social status" does have an effect on crimes. For example, one defendant used his position as chairman of a local bank board to set up loans for his ailing wood chip company. The loans would never have been approved without the chairman's influence, and he never reported them in his proxy statement to the bank's shareholders. Ultimately, the bank lost close to $6 million. In this case, the chairman's class standing made a difference. His ruse squares with the documented knowledge that officers

[5] Ibid., p. 61.
[6] Ibid., p. 65.
[7] Ibid., p. 65.

and managers commit the business crimes with the widest impact (in terms of dollar amounts and victimization), while owners and workers generally commit narrower schemes.

Organizational Opportunity

Of all factors, organizational opportunity remains the determinant aspect of white-collar crime. Against Sutherland's emphasis on an elite group running high-class sting operations, *Crimes of the Middle Classes* shows that organization and complexity make a larger difference than the offender's social status. In a fascinating case, a church group used its daycare center to defraud the federal government of approximately $1 million. Their arrangement with the U.S. Department of Agriculture required the daycare's administrators to submit monthly vouchers reporting the number of meals they had served and the cost of food and labor. When auditors descended upon the scam, they found that, for about $79,000 in actual expenses, the administrators had submitted almost $1 million in food costs, and $400,000 for labor. Teachers said they sometimes brought food to the center themselves because the children weren't being fed properly. There were also reports that "morning snacks were never served unless the government inspectors were expected, that the same children were run through serving lines twice when inspectors were present, and that some children were bused in from other daycare centers on inspection days."[8] The example shows, according to the authors, that a criminal's position in an organization and his ability to organize the scam have far more bearing on the crime than social status or class alone.

The Middle Class

People of moderate social standing are, in fact, more likely than members of the upper class to commit highly organized crimes from within a corporate structure. Some offenders do fit the stereotype of "respectability and high social status" in white-collar crime, but most of them are solidly middle class. According to *Crimes of the Middle Classes*, "they appear to represent the very broad middle of the society, much above the poverty line but for the most part far from elite social status … the offenders are mostly commonplace, not unlike the average [citizen] in most respects, though perhaps more often with personal lives that are in some state of disarray. The single quality that distinguishes them from other[s] is that they have been convicted of a federal crime."[9]

[8] Ibid., p. 94.
[9] Ibid., p. 73.

Methodology

All the conclusions in the *Crimes of the Middle Classes* are qualified. The authors and researchers drew from the federal court records of seven districts in the United States and obtained access to the pre-sentencing reports (PSIs) prepared by probation officers. PSIs had never been available to researchers before, and the close reading of these documents formed a central part of the project. Admittedly, the crimes and specific cases studied were selected, not drawn from a random sample. Eight crimes were targeted as "white collar": securities violations, antitrust suits, bribery and influence-peddling, embezzlement, mail or wire fraud, tax fraud, false claims and statements (in official documents), and credit fraud. Certain violations—such as charges against organized crime and breaking importation laws—were excluded, judged to lie outside the parameters of what most people think of as white-collar activity.

Even within their eight categories, the authors didn't examine every single case, deciding to focus on no more than 30 cases within each category in order to facilitate the close reading of PSIs. They warn that their findings were taken from studying people actually convicted, so the results don't take into account how often charges are actually filed and followed up by prosecution. By dealing with the convicted, they focused on the treatment of people already inside the federal system.

Finally, the long-range nature of the project meant that the study's sample years (1976–1978) were considerably past before the findings were published and, during the interim, several notable legal developments had occurred. The U.S. Federal Sentencing Guidelines that were handed down in 1984 and adopted in 1987 made some material that judges previously considered at their discretion (like the dollar amount of a crime) a *mandatory* element of sentencing. At the same time, the U.S. Sentencing Act systematically *excluded* judgments based on a defendant's "moral character," which had previously been a standard in assessments.

With these qualifications in mind, it remains useful to consider the findings of the research presented in *Crimes of the Middle Classes*. The following chart summarizes the ranking of offenders by social status and in respect to certain demographic features.

Offenders Ranked by Status, with Selected Demographic Information

High • *Antitrust* • *Securities*	These offenders committed the crimes with the largest dollar impact and the widest geographic scope. They are overwhelmingly white (over 99%) and male (99.1% for antitrust, 97.8% for securities). The groups are equally likely to hold a college degree (40.9% in either case), and their frauds were usually occupational in nature. There are revealing contrasts when these two types of offenders are compared: **(1)** Almost 97% of antitrust offenders had been steadily employed in the years preceding their crime, while only about 60% of the securities offenders had continually held a job. **(2)** The antitrusters had a median ratio of assets to liabilities of $200,000 (assets) to $40,000 (liabilities); the securities offenders medianly held $57,500 in assets with $54,000 in liabilities. **(3)** Antitrust violators were more likely to own their own homes (73.5% vs. 58.2%) and to be married (95.7% vs. 80.7%) than securities offenders.
Middle • *Tax fraud* • *Bribery*	These offenders are mainly white males, around 45 years old. Their crimes are not usually occupational—just 15% for tax fraud and less than 18% for bribery. Roughly 57% of offenders owned their own homes, and about 28% held a college degree. Their median assets ranged from $45,000–$49,500; median liabilities were between $19,000 and $23,500. The authors remark that, although tax fraud is a typical white-collar crime, "two-thirds of the tax offenders work in the manufacturing or nonprofessional service sectors."
Low • *Credit fraud* • *Mail fraud* • *False claims*	This group was not as likely to be white—71.5% for credit fraud, 76.8% for mail fraud, 61.8% for false claims—or male—84.8% for credit fraud, 82.1% for mail fraud, 84.7% for false claims. They were generally younger than the other category offenders (less than 40 years old); less likely to be married (about 50%); and less likely to own their own home (roughly 34–45% across the three crime types). Their net worth, as per the ratio of assets to liabilities, was remarkably low: $7,000/$7,000 for credit fraud; $2,000/$3,500 for mail fraud; $4,000/$5,000 for false claims.

Outside Hierarchy • *Bank embezzlement*	These offenders were placed outside the rankings because they were dramatically younger (a mean age of 31) and more likely to be female (44.8% female/55.2% male) than the other groups. While nearly 25% of the low-status group was unemployed at the time of their crime, only 3% of embezzlers were without a job (just slightly above the 2.8% rate for high-status offenders). They are the group least likely to have a college degree (12.9%) or to own their own home (28.4%). Their median net worth was $2,000 in assets with $3,000 in liabilities. Male embezzlers were usually managers of a local banking operation, while females were most often tellers or clerical workers.

However difficult it might prove to be to sort out the demography of *Crimes of the Middle Classes*, the strength of the analysis lies in its tracing of the path of criminals through the federal system. Following their core group from offense to conviction, the authors report on general trends in the treatment and sentencing of white-collar criminals. The most surprising conclusion states that once convicted, people of higher social status are more likely than similar offenders to receive prison time and to be fined.

Cooperating Defendants

Some standard assumptions still apply. For example, informing on one's cohorts does help. *Crimes of the Middle Classes* found that more than 42 percent of cooperating defendants were charged with a single violation, while only 30 percent of uncooperative defendants were so lucky. Also, white-collar defendants receive bail rather easily: Just one person in eight spends any time incarcerated before trial and, for the generally high-status antitrust defendants, the figure is fewer than one in twenty. By comparison, in a control group of "common criminals" (i.e., people convicted of the "nonviolent economic crimes" of postal theft or postal fraud), at least one-third of the defendants spent time in jail before going to trial.

Pleas by White-Collar Defendants

White-collar defendants are more likely to insist on a trial than other offenders. In at least 90 percent of federal cases, defendants will plead guilty, avoiding the expense and effort of a trial. But, over 18 percent of defendants in the *Crimes of the Middle Classes* sample (as opposed to the usual 10 percent) pleaded not guilty. In cases like bank embezzlement, usually "simple cases with clear evidence," plea bargains are easily negotiated and "prosecutors may actively

seek guilty pleas."[10] The decision on how to plead varies with the offender as much as the offense. For example, female bank tellers were especially prone to plead guilty, while many of the male embezzlers—generally "higher-level officials involved in more complex crimes"—proceeded to trial. Of all white-collar defendants, securities offenders are the ones most likely to insist on their day in court. Evidently, both the government and the defendants in these cases feel more strongly about their chances to win.

Judgments

Judgments against white-collar defendants often involve an assessment of personal suffering. It is widely held that, when convicted of a crime, these people suffer a greater blow personally and professionally than street criminals. Many observers think this suffering should be acknowledged in assessing a sentence. One federal judge is quoted as saying:

> *The white-collar criminal by virtue of his conviction has suffered a loss of position, usually loss of employment, sometimes status in his profession, other times the ability to ever find employment in anything requiring a fidelity bond or what have you. Whereas the common street criminal hasn't had a career loss of a similar nature; indeed, in some areas the conviction of a crime is some sort of a badge of maturity.*[11]

Personal Suffering

Examining PSIs, the authors found that, in about 65 percent of the cases overall, personal suffering was said to have played an overwhelming role in the defendant's case. Securities offenders and embezzlers topped the list with 70 and 87 percent of these people (respectively) reporting some hardship. Of course, the reports involved statements by the defendants or their families, which could be self-serving.

In actually looking at objective material—such as the loss of employment, marital separations and divorce, or mental health problems—the authors found the results "ambiguous." Credit fraud perpetrators, for example, seldom reported any suffering, but they had a 20 percent divorce rate during the time of their prosecution, the highest in the study. And there were often large gaps between different types of crimes. Compared to the securities offenders, with a 70 percent rate of suffering, only about 24 percent of antitrust offenders had similar complaints. The discrepancy might lie in how different crimes are viewed. "Antitrust violators, who steal *for* their companies and actually provide the services

[10] Ibid., p. 114.
[11] Ibid., 116.

they say they do," aren't seen as harshly as "those who steal *from* their companies."[12] Securities offenders are stigmatized "because their crimes are often against their own clients," while bank embezzlers (with over 87 percent reported suffering) are judged with particular strictness "because they steal from their employers."[13]

In summary, the authors believe that the extra-legal suffering of white-collar defendants has some validity, but it's not always possible to be sure that prosecution alone caused the hardship. The contradictory images of these criminals as both exceptionally privileged and especially harassed "overstate their real experience in the legal system." Neither factor is as great as the standard rhetoric might suggest.

Imprisonment

Crimes of the Middle Classes does find that the highest status group—antitrust violators—were the least likely to receive prison time (about one in five) and to draw the shortest sentence (1.8 months). Securities fraud led the group, with over 67 percent doing time, followed by tax fraud (58.9 percent) and mail fraud (55.1 percent). But in considering all offenders in all groups, the authors discovered that the higher an individual's status, the more likely the person was to be imprisoned: "All else being equal, doctors will have about a 30 percent greater likelihood of being imprisoned [for a white-collar crime] than truck drivers and almost a 13 percent greater likelihood than managers."[14] Judges seem to find people of higher prestige more at fault or, in other words, more blameworthy, in the commission of their crimes.

More often than prison, the punishment of choice for white-collar criminals is the imposition of fines. Whereas six percent of the "common criminals" in the survey received fines, all of the antitrust violators did; embezzlers were the least likely group to be fined, but even so, their 15 percent rate far exceeded the norm. For fines as well as imprisonment, higher status usually meant a higher penalty. Analysis showed that "white defendants, those with more impeccable records, and those who have higher class positions are more likely to be fined."[15] But while the decision to fine seems based on status, the actual levies are often comparatively low. For antitrust suits, the mean fine was $9,808; for embezzlement, it was just $1,397. Even well-off offenders got off light: a man convicted of fixing the price of

[12] Ibid., 124.
[13] Ibid., 125.
[14] Ibid., 143.
[15] Ibid., 157.

candy bars, with a net worth exceeding $190,000, was fined $3,500; another defendant, whose net worth approached $1.4 million, was fined $5,000 for credit fraud. Only 4 percent of offenders were ever given the statute's maximum penalty.

Obviously, most white-collar crimes don't even approach the billion-dollar levels of the stereotype. An accurate picture actually looks rather mundane. "For every truly complicated and rarified offense," according to Wheeler and his colleagues, "there are many others that are simple and could be carried out by almost anyone who can read, write, and give an outward appearance of stability."[16] More than anything else—more than status, or class position, or heritage—the white-collar criminal needs an opportunity and some sort of organization.

Contributing Factors

The authors posit several factors that have contributed to the rising problem of economic crime:

- The economy increasingly runs on credit, which often means rising personal debt. The offenders in the sample often showed serious discrepancies "between their resources and their commitments."[17]
- New information technologies mean that the opportunity for wrongdoing is growing, and many of the techniques are not widely comprehended by businesses or individuals.
- Government programs distributing large amounts of money make an enticing target for defalcations.
- The importance of credentials in a professionalized society may influence individuals "to inflate the credentials, or to make them up when they do not exist."[18] This tendency involves everything from cheating on school entrance exams to falsifying credit applications.
- Most broadly, the authors observe an overarching culture based on affluence and ever-higher levels of success. Television, and advertising in general, promise that no one has to settle for second best, prompting those who find themselves running behind to make an attempt to conceal the difference, crossing ethical and sometimes legal lines.

[16] Ibid., 171.
[17] Ibid., 183.
[18] Ibid.

Conclusion

Curbing this pernicious trend will not be easy, but there are ways. Since organizational opportunity determines so much criminal activity, the foremost deterrent is to pay heightened attention to "where the money is and how it flows" within any group. Obviously, most businesses have some system of financial control, but the authors say that "organizational intelligence" is often less than stellar. Offenders are not usually "the highly sophisticated swindlers" from the mass media, just "average people in a financial jam who see a way out through fraud."[19]

Furthermore, like many analysts these days, the *Crimes of the Middle Classes* team believes it is far too easy to acquire money and goods on credit. Tightening the restrictions on credit cards and loans would directly address the role that debt plays in many schemes.

Finally, these authors center the problem of white-collar crime on values. As long as the places where citizens learn their priorities—schools, families, neighborhoods, mass media—emphasize high-pressure risk-taking and material affluence over "honesty and moral integrity," many people will go for the gold, even if they have to steal it. It will never be easy, they acknowledge, to balance a market-based economy, which requires competition, with an equal insistence on forthrightness and fair play.

Organizational Crime

Most criminologists have adopted the distinction first made by Marshall B. Clinard (a recipient of the ACFE's Cressey Award) and Richard Quinney between *occupational crime* and *organizational crime*. Organizational crime is that which is committed by businesses, particularly corporations, and the government. Occupational crime involves legal offenses committed by individuals in the course of their occupation. An antitrust offense would be an organizational crime; accepting or offering bribes is an occupational offense.

Organizational crime occurs in the context of complex relationships and expectations among boards of directors, executives, and managers on the one hand, and among parent corporations, corporate divisions, and subsidiaries on the other. White-collar crime is distinguished from lower socioeconomic crimes in terms of the structure of the violation

[19] Ibid., 190.

and the fact that administrative and civil penalties are more likely to be used as punishment than are criminal penalties.

While corporations cannot be jailed, they may be confined. Most corporate lawbreakers are handled by government regulatory agencies. Enforcement measures might include warning letters, consent agreements or decrees not to repeat the violation; orders of regulatory agencies to compel compliance, seizure, or recall of goods; administrative or civil monetary penalties; and court injunctions to refrain from further violations.

Corporate crime is certainly not limited to North America, although it has many high-profile cases. Clinard and Yeager say it appears to be extensive in Europe, Japan, Australia, and other areas. For example, French multinationals might transfer profits from one subsidiary to another located in a country that has a more lenient tax system or presents a tax haven, or they might falsify their bookkeeping to avoid payment of industrial and commercial taxes. In Japan, the Diet (legislature) passed a law for the punishment of crimes "relating to environmental pollution that adversely affects the health of persons." Under this law, intentional or negligent emission of a substance that causes danger to human life or health by industries is to be punished with imprisonment or fines. Additionally, the Swiss banking system has often been accused of offering a hiding place for stolen or looted money, providing a screen for stock manipulations and shady promoters, and helping tax evaders to conceal both income and assets. Deposits in Swiss banks are often laundered to obscure their illegal origins, and then the money is made legal through new commercial transactions and is therefore concealed from tax authorities.

Corporate Organization and Criminal Behavior

Corporate offenses take place in a context of complex relationships and expectations in an organizational setting. It is often difficult to distinguish which corporate participants ought to be held personally responsible for the wrongdoing. Many offenses are the result of myriad decisions that are made by different individuals and passed through a chain of command. Not uncommonly, when corporate acts are contrary to the law, upper-level executives take pains to avoid learning what is going on to avoid responsibility if a scheme is uncovered. In some corporations, there is one well-paid executive who is only half in jest referred to as the "vice president in charge of going to jail."

In most jurisdictions, the law largely treats corporations as people. They make more inviting prosecutory targets than individuals, most notably because they have deeper pockets and can

be heavily fined to repay losses that have been inflicted on individuals or on the society in general.

Government regulatory agencies oversee corporate performance in areas assigned to them by legislation. Typically, the lawmakers enact a statute that is deliberately vague, allowing the enforcement agency to develop its own enforcement guidelines within the boundaries of the legislatorial authorization. The agencies will sometimes seek to expand the reach of the law by selecting notably egregious cases for litigation and appeal, thereby anticipating a favorable ruling on what is fundamentally a somewhat novel interpretation of their mandate.

The Image of the Corporation

Large corporations have contributed significantly to industrial and commercial development throughout the world. Their size and resources enable them to organize and coordinate production and distribution. The capital resources of a large corporation provide it with the ability to develop, adopt, and alter technology on a mammoth scale. A considerable portion of the population has been accorded a high standard of living because of corporate activity.

At the same time, large corporations have the power to influence the manner in which laws are written and to commit acts that can inflict serious harm upon the population. They can hire lobbyists and lawyers who manipulate definitions of wrongdoing in the corporations' interests.

The largeness and remoteness of the corporation from most of the population is part of the reason that many individuals traditionally have a love-hate attitude toward such organizations. They admire and desire corporations' products, but are uneasy about their power—a power that tends to be used single-mindedly in the pursuit of profits. Thomas Hobbes, a 17th century English political philosopher, was particularly scornful of corporations, comparing them to ascarides—worms that eat at the entrails of what Hobbes called "natural man."[20] Centuries later, Robert Heilbroner, an economist, would criticize "the corporation with its wealth-seeking, its dehumanizing calculus of plus and minus, its careful inculcation of impulses and goals that should at most be tolerated."[21]

[20] Thomas Hobbes, *Leviathan* (London: Andrew Crooke, 1651).
[21] Robert Heilbroner, *In the Name of Profit* (New York: Doubleday, 1973), 223.

Clinard and Yeager

In a comprehensive study of corporate law-breaking, Marshall Clinard (a recipient of the ACFE's Donald Cressey Award) and Peter Yeager examined, over a two-year period, the records of 562 companies (477 of which were on the *Fortune 500* list) and found that 1,553 white-collar crime cases had been filed against them. Some 60 percent of the firms had at least one case against them; for those companies, the average number of violations was 4.4. The oil, pharmaceutical, and motor vehicle industries were the most likely to be charged for wrongdoing, a matter that might be a function of enforcement priorities or a true reflection of their activities.

The costs of corporate crimes not only include financial losses, but also injuries, deaths, and health hazards. Such crimes destroy public confidence in businesses and hurt the image of corporations. Clinard and Yeager say price-fixing offenses victimize the consumer and government, while income tax crimes deprive the government and those dependent on it of needed revenue.

Clinard and Yeager believe that corporate violations are increasingly difficult to discover, investigate, or prosecute successfully because of their growing complexity and intricacy. This is particularly true, they believe, of antitrust cases, foreign payoffs, computer fraud, and illegal political contributions. In the last category, some corporations pay bonuses to their executives, with the understanding that part of that reward will be turned over to the coffers of a candidate that the corporation favors.[22]

Criminal activities involving corporations are often rooted in organizational subcultures and values and are developed over time. While individuals still carry out the criminal enterprise, their attitudes and characteristics are of little importance, as an organization will replace those employees unwilling to participate in a criminal activity. A particularly comprehensive examination of how matters of life and death become embedded in routine decision making and ultimately can lead to tragedy is provided in a book titled *The Challenger Space Shuttle Disaster* by Diane Vaughan, another Cressey Award winner.[23]

---

[22] Marshall B. Clinard and Peter C. Yeager, *Corporate Crime* (New York: Free Press, 1980).

[23] Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: University of Chicago Press, 1996).

Legal responses have been slow and ineffectual when dealing with economic organizational change. The law has emphasized the role of the individual actor in criminality, but has not examined the role of the organization in crime.

Opportunities for Unlawful Organizational Behavior

Organizational Structure

Complex companies provide a structure that can foster misbehavior. They provide many settings where misconduct is possible. They isolate those settings in departments and in locations around a city, the country, or the world. This isolation, in turn, means that information about what one part of a company is doing might be unknown in another part. All this reduces the risk that misbehavior will be detected and punished. The larger a company grows, the more specialized its subunits tend to become, and this specialization thereby breeds a higher risk of fraud. An internally diversified company might have few employees who fully understand the detailed workings.

Specialized departments in a large firm compete for resources not only with other firms, but with departments in their own firm. The need to outperform both other businesses and internal units can generate sufficient pressure to lead to misconduct. Vaughan notes that departments often have survival concerns that conflict with the larger interests of an organization. When given a chance to make decisions, she writes, lower-level managers will tend to act not in the interest of the firm, but in the interests of their departments.

Specialization also hides illegal activities, especially where a firm's tasks are kept separate and unrelated. Employees cannot garner knowledge about all the particulars of how a firm works. This protects a company from the effects of personnel turnover and leaks of information because no one can offer much more than a piece of the jigsaw puzzle that makes up the company picture. The same secrecy, however, raises the chances for misconduct.

Companies spell out rules in a common language to decide how tasks will be performed and to create common bonds that will facilitate decision making. But a company's ability to coordinate all its activities varies considerably. Vaughan writes that organizational growth naturally leads to a progressive loss of control over departments. Executives cannot hope to keep track of all the units in a huge company and must rely on subordinates to carry out policy. Vaughan states that when the distance between top executives and subordinate units grows to a sufficient level, "authority leakage" results. Such leakage means the company has

become too unwieldy for an executive to enforce rules at all levels. "The organization, in short," Vaughan writes, "can diversify beyond the capability of those at the top to master it."

Such leakage allows subsidiaries, company researchers, accountants, or other departments to engage in misconduct without any assurance that internal controls will check the behavior. In some cases, as with computer crime, detecting misconduct might be beyond the ability of most employees. Conversely, authority leakage and specialization can also lead an organization to comply with societal rules even when the organizational pressures lean toward misconduct.

Does the existence of authority leakage and specialization imply a loss of company control? While a company that cannot steer its employees' behavior might be viewed as irrational or incompetent, the ability to control information flow from top to bottom might not be possible. Research and theory suggest, to the contrary, that information is processed selectively through a company in ways that tend to protect the interests of departments and to promote efficiency.

Sometimes censorship of information promotes a company's interests. In other cases, "need to know" policies or ignorance of rules that are irrelevant to a department leads to inefficiencies. All these tendencies restrict information flow and create opportunities for one unit in a company to act outside the knowledge of other units. Censorship policies might originate in any part of a company and hide matters throughout the organization.

The tiered structure of most organizations obscures personal responsibility and tends to spread it throughout the company. Thus, determining where a decision to engage in misconduct originated can be difficult. *Criminology* author John E. Conklin put it this way: "The delegation of responsibility and unwritten orders keep those at the top of the corporate structure remote from the consequences of their decisions and orders, much as the heads of organized crime families remain 'untouchable' by law."

Criminogenic Organizational Structures

Sociologist Edward Gross asserted that all organizations are inherently criminogenic (that is, prone to committing crime), though not necessarily criminal.[24] Gross makes this assertion because of the reliance on "the bottom line." Without necessarily meaning to, organizations

[24] Edward Gross, "Organizational Structure and Organizational Crime," in *White-Collar Crime: Theory and Research,* Gilbert Geis and Ezra Stotland, eds. (Beverly Hills: Sage, 1980), 53–76.

can invite fraud as a means of obtaining goals. Economist Oliver Williamson noted that, because of a department's concern with reaching its goals, managers might well tend to maximize their department's own interests to the detriment of the organization.

Organizations can also be criminogenic because they encourage loyalty. According to Diane Vaughan, the reasons are that:

- The organization tends to recruit and attract similar individuals.
- Rewards are given out to those who display characteristics of the "company man."
- Long-term loyalty is encouraged through company retirement and benefits.
- Loyalty is encouraged through social interaction, such as company parties and social functions.
- Frequent transfers and long working hours encourage isolation from other groups.
- Specialized job skills can discourage personnel from seeking employment elsewhere.[25]

This, in turn, causes company personnel to sometimes perceive that the organization might be worth committing crime to maintain and further its goals. The use of formal and informal rewards and punishments, plus social activities and pressures to participate, link an employee's needs and goals to the company's success. Society places value on the reputation of the company for which one works, reinforcing the link between an individual and corporate goals. When a company achieves its goals, its employees prosper. In short, the interests of an organization and its employees coincide, and that situation might set the stage for unlawful conduct by individuals on the organization's behalf.

Vaughan writes that organizational processes create "an internal moral and intellectual world" that causes individuals to identify with organizational goals. Company survival comes to mean individual survival and, when resources become scarce, the incentive to misbehave increases. Of course, not all agents will act unlawfully on a company's behalf, and how any employee behaves will be linked to factors that might not be related to the world of the organization.

When the structural pressure to commit fraud exists, a firm often cannot unite its agents in such activities. At least three factors prevent such unity. First, the pressure to commit fraud might not affect departments in a company equally. A sales department that must meet certain goals to generate profits will feel different competitive pressure than a product

[25] Diane Vaughan, "Transaction Systems and Unlawful Organizational Behavior," *Social Problems* 29 (April 1982), 373–380.

development department in the same company that is running smoothly. Some parts of companies might never experience pressure to cheat, and members of those departments will have no motivation to engage in misconduct on a firm's behalf.

Second, even in high-pressure departments, some employees will not have knowledge of the difficulty of obtaining needed resources. An employee will have no motivation to commit fraud unless he has full information about an organization's goals and how the department can achieve them. In other words, an employee usually needs a high degree of responsibility for a company's success, as well as the ability to bring about those goals, before a chance to engage in misbehavior can occur.

Third, outside societal behavior can produce values that conflict with those learned in an organizational environment. For example, fraternal or professional associations impart their own values to employees that might not coincide with a specific corporate code of honor. When faced with conflicting norms, Vaughan writes, employees will make their choices based on the rewards and punishments they perceive to accompany the alternatives. Where misbehavior is seen as too costly, it will not occur. When an organization provides sufficient rewards to overcome the fear of punishment, misbehavior might occur despite competing norms. The amount of information an employee has will affect the decision on which way to go, as will an individual's financial and social dependence on the firm.

The mere fact that corporate and individual goals are often joined in organizations does not necessarily create a climate for illegal actions. As with any major decision, complexities often enter the picture. Temptations vary not only among departments, but within them. The availability of information and individual risk-reward assessments might generate lawful behavior that resists organizational pressures to violate the law, as well as unlawful behavior in the face of organizational pressures to comply. Put plainly, the likelihood that organizational processes will generate misbehavior is highly variable and cannot currently be measured with any degree of precision.

The findings of many criminologists help explain how individuals become corporate offenders. In describing how employees are taught to make decisions that are correct from a corporation's standpoint, Drucker said a natural tendency exists in every large-scale organization to discourage initiative and encourage conformity. Madden and Margolis say corporations lead new managers through an initiation period designed to weaken their ties

with external groups, including their own families, and encourage a feeling of dependence on and attachment to the corporation.

Geis found that individuals are quite often trained in illegal behavior as part of their occupational roles. Schrager and Short say criminal behavior stems more from the roles an employee is expected to fulfill than from individual pathology. Many executives know their behavior is illegal, but tend to justify their actions as simply common practice in the business world. Clinard and Yeager believed that, in rationalizing their behavior, corporations follow a general tendency to obey laws selectively (i.e., obeying according to situational needs and determined by factors like social class and occupation).

Sutherland demonstrated that corporate executives are insulated from those who might disagree with their beliefs because they associate almost exclusively with people who are pro-business, politically conservative, and generally opposed to government regulation. And Silk and Vogel found that certain beliefs about government intervention in business are used throughout the business world to justify illegal activity by corporations.

A common problem in many large corporations with intricate hierarchical structures tends to be a split between what the upper levels believe is going on below and the actual procedures being carried out. Clinard and Yeager say that the chief executive officer of a corporation is often isolated and, thus, messages transmitted down the line tend to become distorted. Clinard and Yeager found that all levels of the corporation might often agree to perpetuate the lack of full information, for the key to any successful conspiracy to violate the law probably lies in the fact that the higher-ups do not inquire about what is going on and the lower levels do not tell them.

Often, in corporations, no single individual at the highest levels may make a decision alone to market a faulty product or take shortcuts on product testing, Clinard and Yeager say. Instead, decisions are made in small steps at each level, possibly without any awareness of the illegal and potentially dangerous result.

Criminologist Charles McCaghy says profit pressure is "the single most compelling factor behind deviance by industry, whether it be price fixing, the destruction of competition, or the misrepresentation of a product,"[26] such as making a poor-quality product that will wear

[26] C. H. McCaghy, *Deviant Behavior: Crime, Conflict, and Interest Groups* (New York: Macmillan, 1976), 218.

out and need to be replaced. Clinard and Yeager say certain industries, such as the drug and chemical businesses, have such severe competition and strong profit drives due to demands for continual development of new products that they might feel pressured to falsify test data, market new products before their full effects are known, or engage in unethical sales techniques that can have disastrous effects on human beings and the environment.

Corporate Executives and Criminal Liability

Many of the ethical and legal problems of a corporation result from the corporate structure that separates ownership from management. Typical large corporations are administered by a group of salaried managers, with the board of directors exercising little direct power other than hiring or firing the managers; thus, corporate managers have great autonomy over decisions regarding production, investment, pricing, and marketing.

Executives tend to believe that their jobs are at risk if they cannot show a profit to higher management or the board of directors, and, often, they are. Clinard and Yeager hold that if goals for managers are set too high, the employee then confronts a hard choice of risking being thought incompetent or taking unethical or even illegal shortcuts.

According to Clinard and Yeager, corporations often try to protect their executives from liability by agreeing to pay fines, court costs, and attorney's fees with corporate funds; bonuses, raises, or liability insurance might offer protection to officers or directors. Generally, executive compensation and tenure remain untouched. There is much difficulty in criminal prosecution of executives because corporate violations are usually far more complex than conventional crimes. Also, the complexity of the legal proof required allows businessmen to test the limits of the law.

Businessmen might have sought legal advice on loopholes in the law before committing the offense, Clinard and Yeager say, which may be cited as evidence that the executives thought they were in legal compliance. Businessmen can hire highly skilled lawyers who present arguments as to the client's lack of previous convictions or unlikelihood of becoming a repeat offender, as well as being able to cite numerous precedents where businessmen were charged but not imprisoned for similar violations.

Corporate offenders are usually not imprisoned with ordinary criminals, but are usually incarcerated in institutions designed for low-risk inmates with short sentences, presumably

for the corporate offender's own physical safety. Justifications used in arguing against a prison sentence for corporate offenders include:

- Age and poor health
- Personal and family reasons
- Extent of punishment already suffered by virtue of being indicted
- Offense was not immoral
- Defendant has no prior record, is not a threat to society, and has been a prominent citizen active in community affairs
- Incarceration would accomplish nothing (no benefit to society)
- Defendant is repentant
- Victimization of corporate executives solely because of their position

Some corporate offenders are given community service as punishment, such as giving speeches about their offenses to businesses and civic groups, working in programs designed to aid the poor, or helping former ordinary criminal offenders secure job pledges from businesses.

Management Behavior

In their study on business ethics, Brenner and Molander found that superiors are the primary influence in unethical decision making. Therefore, the use of sanctions to accomplish compliance with the law is only one of the various forces operating within a corporation encouraging or opposing violations of law. Similarly, Stone found that the success of law enforcement "ultimately depends upon its consistency with and reinforcement of the organization's rules for advancement and reward, its customs, conventions, and morals." He maintains that if the law is too much at odds with the corporation's "culture," employees will tend to cover up their tracks rather than change their behavior.[27]

Some corporations might also argue that regulation is faulty because most government regulations are incomprehensible and too complex. Conklin found that antitrust laws are seen as inconsistent, hypocritical, poorly defined, and rarely enforced. Therefore, most regulations must be written in detail to cover as many contingencies as possible.

[27] Christopher Stone, *Where the Law Ends: The Social Control of Corporate Behavior* (New York: Harper & Row, 1975).

Silk and Vogel found several other actions used by businesses to rationalize conduct:

- Government regulations are unjustified because the additional costs of regulations and bureaucratic procedures cut heavily into profits.
- Regulation is unnecessary because the matters being regulated are unimportant.
- Although some corporate violations involve large sums of money, the damage is so diffused among a large number of consumers that, individually, there is little loss.
- Violations are caused by economic necessity; they aim to protect the value of stock, to ensure an adequate return for stockholders, and to protect the job security of employees by ensuring the financial stability of the corporation.

John Braithwaite (past recipient of the ACFE Cressey Award for his research in international white-collar crime issues) views white-collar crime as a product of the corporate subculture. In Braithwaite's view, corporations will turn to crime as a result of "blocked opportunities."

Because white-collar crime can exist only in secrecy, deviant subcultures develop (e.g., conspiracy among executives), lines of communication are not allowed to develop, and people operate within spheres of responsibility.

Controlling Organizational Crime

Clinard and Yeager believe corporations that do violate acceptable conduct and those that do not are distinguished by "corporate cultures" or ethical climates, which are the degree to which a corporation has made the choice to be unethical, to disregard the interests of the consumer and the public, and to disobey the laws that regulate its specific industry.

Efforts to control corporate crime follow three approaches: voluntary change in corporate attitudes and structure; strong intervention of the political state to force changes in corporate structure, accompanied by legal measures to deter or punish; or consumer action. Voluntary changes would involve the development of stronger business ethics and certain corporate organizational reforms; government controls might involve federal corporate chartering, deconcentration and divestiture, larger and more effective enforcement staffs, stiffer penalties, wider use of publicity as a sanction, and possibly the nationalization of corporations; and consumer group pressures may be exerted through lobbying, selective buying, boycotts, and the establishment of large consumer cooperatives.

Clinard and Yeager suggest that a wide, comprehensive industrial code of ethics, which many businessmen favor, would be of great help if a businessman refused an unethical request. This would help more clearly define the limits of acceptable or ethical conduct, improve the ethical climate of the industry, and serve to reduce cutthroat practices where competition is intense. Greater stockholder involvement might enable greater corporate compliance with the law, but, in actuality, it is the management staff that runs the company and makes the decisions; the stockholders are primarily concerned with stock growth and dividends.

In some cases, critical information dealing with possible law violations simply fails to reach the board of directors. New board members are usually nominated by the board and routinely approved by stockholders, making boards self-perpetuating. Board members are often drawn from management. Many corporations now employ outside directors and/or representatives of the public interest, much like the practice abroad of naming union representatives to boards. These public members represent the public and consumer concerns, ascertain whether the corporation is complying with the law, assist and maintain corporate public responsibility, help monitor the internal management system to discover faulty workmanship and report it to the board, serve as liaisons with government agencies with respect to legislation or standards, and serve as a hotline to receive information about deviance.

Clinard and Yeager found that mass media publicity about law violations probably represents the most feared consequence of sanctions imposed on a corporation. Publicity can also inform the public about the operation of regulatory controls and can enable people to understand the purposes of the controls. Informal publicity is ordinarily carried as news items from the media, while formal publicity is a requirement that a corporation must, as part of an enforcement action, publish an advertisement or some other statement acknowledging a violation and that corrective measures are being taken.

If illegal behavior consistently resulted in decreased patronage or even consumer boycotts, consumer pressure would be an effective tool in the control of illegal corporate behavior. However, say Clinard and Yeager, it appears to not be very effective. Consumers are often unaware when a corporation's products are unsafe or when it has been violating antitrust laws or polluting the environment. Without organized behavior, a consumer's withdrawal of individual patronage is generally ineffective.

Many corporations settle charges without admitting or denying guilt by consenting to either an administrative or a court-ordered decree banning future violations. In a consent agreement, the corporation reaches an understanding with the government agency not to violate the regulation again. In a decree, the agreement is ratified by the court. A problem with consent orders is that, frequently, no one follows up to find out whether the terms imposed are being met.

Criminal fines and civil and administrative penalties against corporations are forms of monetary penalties. For completion, criminal cases average about one year from indictment to conviction, civil actions about two years, and administrative cases about four months. Criminal action against corporations is difficult to initiate because, generally, government agencies are dependent upon the records of the corporation and its ability or willingness to furnish needed information.

Not all experts agree that monetary penalties are appropriate. Some argue that these sanctions are limited to a person's own worth and, therefore, have limited utility. For example, a $25 million fine to a pauper would have no effect. One novel approach to punishing corporations involves intentional stock dilution. Under this approach, the convicted corporation would issue additional shares of stock to the state equal to the cash value of a fine. The state could then sell the shares, trade them, or keep them for their earnings power.

Some of the criteria considered when deciding to bring criminal action against a corporation are the degree of loss to the public, the duration of the violation, the level of complicity by high corporate managers, the frequency of the violation, evidence of intent to violate, evidence of extortion, the degree of notoriety endangered by the media, precedent in law, a history of serious violations by the corporation, deterrence potential, and the degree of cooperation demonstrated by the corporation.

In many jurisdictions, the rules governing industry often have been initiated by parts of the industry itself. Industries might also attempt to gain influence over agencies by creating a business-oriented atmosphere between regulators and regulates, which can cause the regulators to feel unwarranted confidence in the possibility of voluntary compliance by corporations.

The Enforcement Effort: Preventing and Reducing Fraud

While the issues involved in the enforcement effort provide a context in which to assess the efforts to control white-collar crime, actual techniques of prevention need to be discussed. There are many theories about enforcement, sanctions, and punishments that are a part of controlling white-collar crime.

Enforcement strategies include two main theories: compliance and deterrence.

COMPLIANCE

Compliance is designed to achieve conformity to the law without having to detect, process, or penalize violators. Compliance systems provide economic incentives for voluntary compliance to the laws and use administrative efforts to control violations before they occur. In a compliance system, an offense is often called a "technical violation."

Compliance strategies have been criticized by some criminologists. These experts believe that such strategies have little effect, as sanctions are imposed after the infraction occurs. Since economic penalties are common punishments for violators, these penalties are of little consequence in the case of large, wealthy corporations.

DETERRENCE

As a strategy to control crime, *deterrence* is designed to detect law violations, determine who is responsible, and penalize offenders in order to deter future violations. Deterrence systems try to control the immediate behavior of individuals, not the long-term behaviors targeted by compliance systems.

Deterrence theory assumes that humans are rational in their behavior patterns. Humans seek profit and pleasure while they try to avoid pain. Deterrence assumes that an individual's propensity toward lawbreaking is in inverse proportion to the perceived probability of negative consequences.

INCREASED ENFORCEMENT

Formal levels of current enforcement in white-collar crime are, by all measures, extremely low. One view holds that increased enforcement can only come with a complete and total revision of the criminal justice system. Currently, people have little fear of detection because they know that the police and courts cannot keep up with the pace of criminal offenses. It is not necessary or even desirable to advocate longer prison sentences for offenders because

we do not have the courts and jails to accommodate them. Perhaps a better plan would be to sacrifice the severity of punishment for certainty. Until potential offenders have the perception that they will be caught and punished, we cannot expect a reversal of the crime trend.

Fraud Prevention Programs

Although the government can provide incentives for organizations to prevent fraud, ultimately, it is up to management to institute prevention programs. The "Fraud Prevention Programs" chapter describes methods whereby management can institute policies and procedures to help detect and prevent fraud.

Occupational Fraud

Occupational fraud is committed largely by individuals or small groups of individuals in connection with their occupation. It can include violations of law by businessmen, politicians, labor union leaders, lawyers, doctors, pharmacists, and employees who embezzle money from their employers or steal merchandise and tools.

Gary Green, in honing the white-collar crime concept, uses the term *occupational crime,* which he defines as "any act punishable by law which is committed through opportunity created in the course of an occupation which is legal." Green further delineates occupational crime into four categories:

- Crimes for the benefit of an employing organization (organizational occupational crime)
- Crimes by officials through exercise of their government-based authority (government authority occupational crime)
- Crimes by professionals in their capacity as professionals (professional occupational crime)
- Crimes by individuals as individuals

Some scholars debate whether individuals should be held responsible for crimes committed on behalf of their organizations. Although some direct benefit accrues to the perpetrator, far more benefit accrues to the organization. Regardless of whether the organization is held liable, the fraud is a direct result of some human action or interaction.

Research in Occupational Fraud and Abuse

Edwin H. Sutherland

Relatively little research has been done on the subject of occupational fraud and abuse. Much of the current literature is based upon the early works of Edwin H. Sutherland. As previously discussed in the "Understanding Criminal Behavior" chapter, Sutherland believed that the learning of criminal behavior occurs with other persons in a process of communication. Therefore, he reasoned, criminality cannot occur without the assistance of other people. Sutherland further theorized that the learning of criminal activity usually occurred within intimate personal groups. This explains, in his view, how a dysfunctional parent is more likely to produce dysfunctional offspring. Sutherland believed that the learning process involves two specific areas: the techniques to commit the crime, and the attitudes, drives, rationalizations, and motives of the criminal mind. One can see how Sutherland's differential association theory fits with occupational offenders. Organizations that have dishonest employees will eventually infect a portion of honest ones. It also goes the other way: honest employees will eventually have an influence on some of those who are dishonest.

Donald R. Cressey

During the 1940s at Indiana University, one of Sutherland's brightest students was Donald R. Cressey (1919–1987). While much of Sutherland's research concentrated on upper-world criminality, Cressey took his own studies in a different direction. Working on his Ph.D. in criminology, he decided his dissertation would focus on embezzlers. To serve as a basis for his research, Cressey interviewed about 200 people who had been incarcerated for embezzling funds.

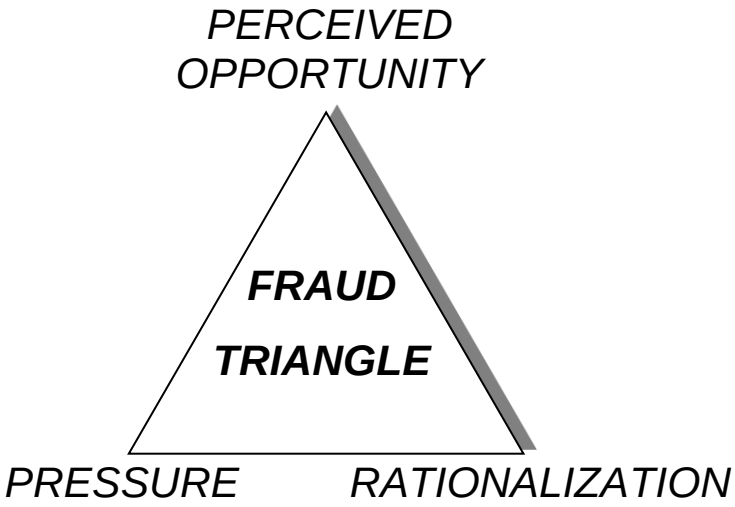
Cressey's Hypothesis

Cressey was intrigued by embezzlers, whom he called "trust violators." He was especially interested in the circumstances that led them to be overcome by temptation. For that reason, he excluded from his research those employees who took their jobs for the purpose of stealing—a relatively minor number of offenders at that time. Upon completion of his interviews, he developed what still remains the classic model for the occupational offender. His research was published in *Other People's Money: A Study in the Social Psychology of Embezzlement*.

Cressey's final hypothesis was:

> *Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.*[28]

Over the years, the hypothesis has become better known as *the fraud triangle*. One leg of the triangle represents a *perceived non-shareable financial need*. The second leg represents *perceived opportunity*, and the final leg stands for *rationalization*. The role of the *non-shareable* problem is important. According to Cressey, "When the trust violators were asked to explain why they refrained from violation of other positions of trust they might have held at previous times, or why they had not violated the subject position at an earlier time, those who had an opinion expressed the equivalent of one or more of the following quotations: (a) 'There was no need for it like there was this time.' (b) 'The idea never entered my head.' (c) 'I thought it was dishonest then, but this time it did not seem dishonest at first.'"[29]



"In all cases of trust violation encountered, the violator considered that a financial problem which confronted him could not be shared with persons who, from a more objective point of view, probably could have aided in the solution of the problem."[30]

[28] Donald R. Cressey, *Other People's Money* (Montclair: Patterson Smith, 1973), 30.
[29] Ibid., 33.
[30] Ibid., 34.

Non-Shareable Financial Problems

That which is considered "non-shareable" is wholly in the eyes of the potential occupational offender, Cressey said.

> *Thus a man could lose considerable money at the race track daily but the loss, even if it construed a problem for the individual, might not constitute a non-shareable problem for him. Another man might define the problem as one which must be kept secret and private, that is, as one which is non-shareable. Similarly, a failing bank or business might be considered by one person as presenting problems which must be shared with business associates and members of the community, while another person might conceive these problems as non-shareable.*[31]

In addition to being non-shareable, the problem that drives the fraudster is described as "financial" because these are problems that can generally be solved by the theft of cash or other assets. A person with large gambling debts, for instance, would need cash to pay those debts. Cressey did note, however, that there are some nonfinancial problems that could be solved by misappropriating funds through a violation of trust. For example, a person who embezzles in order to get revenge on his employer for perceived unfair treatment uses financial means to solve what is essentially a nonfinancial problem.

Through his research, Cressey also found that the non-shareable problems encountered by the people he interviewed arose from situations that could be divided into six basic categories: violation of ascribed obligations, problems resulting from personal failure, business reversals, physical isolation, status gaining, and employer-employee relations. All of these situations in some way dealt with status-seeking or status-maintaining activities by the subjects. In other words, the non-shareable problems threatened the status of the subjects, or threatened to prevent them from achieving a higher status than the one they occupied at the time of their violation.

THE IMPORTANCE OF SOLVING THE PROBLEM IN SECRET

Since Cressey's study was done in the early 1950s, the workforce was obviously different than today's workforce. But the employee faced with an immediate, non-shareable financial need hasn't changed much over the years. That employee still must find a way to relieve the financial pressure that bears down upon him. Simply stealing money, however, is not

[31] Ibid., 35.

enough; Cressey found it was crucial that the employee be able to resolve the financial problem in *secret*.

As discussed, the non-shareable financial problems identified by Cressey all dealt in some way with questions of status; the trust violators were afraid of losing the approval of those around them and, so, were unable to tell others about their financial problems. If they could not share the fact that they were under financial pressure, it follows that they would not be able to share the fact that they were resorting to illegal means to relieve that pressure. To do so would be to admit that the problems existed in the first place.

An interesting thing to note is that it is not the embezzlement that creates the need for secrecy in the perpetrator's mind; it is the circumstances that led to the embezzlement (a violation of ascribed obligation, a business reversal, etc.). Cressey said:

> *In all cases [in the study] there was a distinct feeling that, because of activity prior to the defalcation, the approval of groups important to the trusted person had been lost, or a distinct feeling that present group approval would be lost if certain activity were revealed [the non-shareable financial problem], with the result that the trusted person was effectively isolated from persons who could assist him in solving problems arising from that activity. Although the clear conception of a financial problem as non-shareable does not invariably result in trust violation, it does establish in trusted persons a desire for a specific kind of solution to their problems. The results desired in the cases encountered were uniform: the solution or partial solution of the problem by the use of funds which can be obtained in an independent, relatively secret, safe, and sure method in keeping with the 'rationalizations' available to the person at the time.*[32] (emphasis added)

Perceived Opportunity

According to the fraud triangle model, the presence of a non-shareable financial problem by itself will not lead an employee to commit fraud. The key to understanding Cressey's theory is to remember that all three elements must be present for a trust violation to occur. The non-shareable financial problem creates the motive for the crime to be committed, but the employee must also perceive that he has an opportunity to commit the crime without being caught. This *perceived opportunity* constitutes the second element.

[32] Ibid., 66–67.

In Cressey's view, there were two components of the perceived opportunity to commit a trust violation: general information and technical skill. *General information* is simply the knowledge that the employee's position of trust could be violated. This knowledge might come from hearing of other embezzlements, from seeing dishonest behavior by other employees, or just from generally being aware of the fact that the employee is in a position where he could take advantage of his employer's faith in him. *Technical skill* refers to the abilities needed to commit the violation. These are usually the same abilities that the employee needs to have in order to obtain and keep his position in the first place. Cressey noted that most embezzlers adhere to their occupational routines (and their job skills) in order to perpetrate their crimes.[33] In essence, the perpetrator's job will tend to define the type of fraud he will commit. "Accountants use checks which they have been entrusted to dispose of, sales clerks withhold receipts, bankers manipulate seldom-used accounts or withhold deposits, real estate men use deposits entrusted to them, and so on."[34]

Obviously, the general information and technical skill that Cressey identified are not unique to occupational offenders; most, if not all, employees have these same characteristics. But because trusted persons possess this information and skill, when they face a non-shareable financial problem, they see it as something that they have the power to correct. They apply their understanding of the *possibility* for trust violation to the specific crises they are faced with. Cressey observed, "It is the next step which is significant to violation: the application of the general information to the specific situation, and conjointly, the perception of the fact that in addition to having general possibilities for violation, a specific position of trust can be used for the specific purpose of solving a non-shareable problem."[35]

Rationalizations

The third and final factor in the fraud triangle is the *rationalization*. Cressey pointed out that rationalization is not an *ex post facto* means of justifying a theft that has already occurred. Significantly, rationalization is a necessary component of the crime *before* it takes place; in fact, it is a part of the motivation for the crime. Because the embezzler does not view himself as a criminal, he must justify his misdeeds before he ever commits them. The rationalization is necessary so that the perpetrator can make his illegal behavior intelligible to himself and maintain his concept of himself as a trusted person.[36]

[33] Ibid., 84.
[34] Ibid., 84.
[35] Ibid., 85.
[36] Ibid., 94–95.

After the criminal act has taken place, the rationalization will often be abandoned. That is, of course, because of the nature of us all; the first time we do something contrary to our morals, it bothers us. As we repeat the act, it becomes easier. One hallmark of occupational fraud and abuse offenders is that once the line is crossed, the illegal acts become more or less continuous. So, an occupational fraudster might begin stealing with the thought that "I'll pay the money back," but after the initial theft is successful, he will usually continue to steal past the point at which there is any realistic possibility of repaying the stolen funds.

Cressey found that the embezzlers he studied generally rationalized their crimes by viewing them as (1) essentially non-criminal, (2) justified, or (3) part of a general irresponsibility for which they were not completely accountable.[37] He also found that the rationalizations used by trust violators tended to be linked to their positions and to the manner in which they committed their violations. He examined this by dividing the subjects of his study into three categories: independent businessmen, long-term violators, and absconders. He discovered that each group had its own types of rationalizations.

INDEPENDENT BUSINESSMEN

The *independent businessmen* in Cressey's study were people who were in business for themselves and who converted "deposits" that had been entrusted to them.[38] Perpetrators in this category tended to use one of two common excuses: 1) they were "borrowing" the money they converted or 2) the funds entrusted to them were really theirs—you can't steal from yourself. Cressey found the "borrowing" rationalization was the one most frequently used. These perpetrators also tended to espouse the idea that "everyone" in business misdirects deposits in some way, which, therefore, made their own misconduct less wrong than "stealing."[39] Also, the independent businessmen almost universally felt their illegal actions were predicated by an "unusual situation," which Cressey concluded was in reality a non-shareable financial problem.

LONG-TERM VIOLATORS

Cressey defined *long-term violators* as individuals who converted their employer's funds, or funds belonging to their employer's clients, by taking relatively small amounts over a period of time.[40] Similar to independent businessmen, the long-term violators generally preferred

[37] Ibid., 93.
[38] Ibid., 101–102.
[39] Ibid., 102.
[40] Ibid., 102.

the "borrowing" rationalization. Other rationalizations of long-term violators were described, too, but they almost always were used in connection with the "borrowing" theme: (1) They were embezzling to keep their families from shame, disgrace, or poverty; (2) theirs was a case of "necessity"; their employers were cheating them financially; and (3) their employers were dishonest toward others and deserved to be fleeced. Some even pointed out that it was more difficult to return the funds than to steal them in the first place, and claimed that they did not pay back their "borrowings" because they feared that would lead to detection of their thefts. A few in the study actually kept track of their thefts, but most only did so at first. Later, as the embezzlements escalated, it is assumed that the offender would rather not know the extent of his "borrowings."

All of the long-term violators in the study expressed a feeling that they would like to eventually "clean the slate" and repay their debt. This feeling usually arose even before the perpetrators perceived that they might be caught. Cressey pointed out that, at this point, whatever fear the perpetrators felt in relation to their crimes was related to losing their social status by the exposure of their non-shareable *problem*, not the exposure of the theft itself or the possibility of punishment or imprisonment. This is because their rationalizations still prevented them from perceiving their misconduct as criminal. "The trust violator cannot fear the treatment usually accorded to criminals until he comes to look upon himself as a criminal."[41]

Eventually, most of the long-term violators finally realized they were "in too deep." It is at this point that the embezzler faces a crisis. While maintaining the borrowing rationalization (or other rationalizations, for that matter), the trust violator is able to maintain his self-image as a law-abiding citizen; but when the level of theft escalates to a certain point, the perpetrator is confronted with the idea that he is behaving in a criminal manner. This is contrary to his personal values and the values of the social groups to which he belongs. This conflict creates a great deal of anxiety for the perpetrator. A number of offenders described themselves as extremely nervous and upset, tense, and unhappy.[42]

Without the rationalization that they were borrowing, long-term offenders in the study found it difficult to reconcile converting money, while at the same time seeing themselves as honest and trustworthy. In this situation, they have two options: (1) they can readopt the

[41] Ibid., 120–121.
[42] Ibid., 121.

attitudes of the (law-abiding) social group with which they identified before the thefts began, or (2) they can adopt the attitudes of the new category of persons (criminals) with whom they now identify.[43] From his study, Cressey was able to cite examples of each type of behavior. Those who sought to readopt the attitudes of their law-abiding social groups "may report their behavior to the police or to their employer, quit taking funds or resolve to quit taking funds, speculate or gamble wildly in order to regain the amounts taken, or 'leave the field' by absconding or committing suicide."[44] On the other hand, those who adopt the attitudes of the group of criminals to which they now belong "may become reckless in their defalcations, taking larger amounts than formerly with [fewer] attempts to avoid detection and with no notion of repayment."[45]

ABSCONDERS

The third group of offenders Cressey discussed was *absconders*—people who take the money and run. Cressey found that the non-shareable problems for absconders usually resulted from physical isolation. He observed that these people, "usually are unmarried or separated from their spouses, live in hotels or rooming houses, have few primary group associations of any sort, and own little property. Only one of the absconders interviewed had held a higher status position of trust, such as an accountant, business executive, or bookkeeper."[46] He also found that the absconders tended to have lower occupational and socio-economic status than the members of the other two categories.

Because absconders tended to lack strong social ties, Cressey found that almost any financial problem could be defined as non-shareable for these persons, and also that rationalizations were easily adopted because the persons only had to sever a minimum of social ties when they absconded.[47] The absconders rationalized their conduct by noting that their attempts to live honest lives had been futile (hence their low status). They also adopted an attitude of not caring what happened to them and a belief that they could not help themselves because they were predisposed to criminal behavior. The latter two rationalizations, which were adopted by every absconder in Cressey's study, allowed them to remove almost all personal accountability from their conduct.[48]

---

[43] Ibid., 122.
[44] Ibid., 121.
[45] Ibid., 122.
[46] Ibid., 128.
[47] Ibid., 129.
[48] Ibid., 128–129.

In the 1950s, when this data was gathered by Cressey, embezzlers were considered persons of higher socioeconomic status who took funds over a limited period of time because of some personal problem such as drinking or gambling, while "thieves" were considered persons of lower status who took whatever funds were at hand. Cressey noted:

> *Since most absconders identify with the lower status group, they look upon themselves as belonging to a special class of thieves rather than trust violators. Just as long-term violators and independent businessmen do not at first consider the possibility of absconding with the funds, absconders do not consider the possibility of taking relatively small amounts of money over a period of time.*[49]

Conjuncture of Events

Perhaps the most important conclusion to be drawn from the Cressey study was that it took all three elements—perceived non-shareable financial problem, perceived opportunity, and the ability to rationalize—for the trust violation to occur.

> *The three events make up the conditions under which trust violation occurs and the term* cause *may be applied to their conjuncture since trust violation is dependent on that conjuncture. Whenever the conjuncture of events occurs, trust violation results, and if the conjuncture does not take place there is no trust violation.*[50]

Conclusions

Cressey's classic fraud triangle helps explain the nature of many—but not all—occupational offenders. For example, although academicians have tested his model, it has still not fully found its way into practice in terms of developing fraud prevention programs. Our sense tells us that one model—even Cressey's—will not fit all situations. Plus, the study is nearly half a century old. There has been considerable social change in the interim. And now, many anti-fraud professionals believe there is a new breed of occupational offender—one who simply lacks a conscience sufficient to overcome temptation.

[49] Ibid., 133.
[50] Ibid., 139.

Dr. Steve Albrecht

The Albrecht Study

Another pioneering researcher in occupational fraud and abuse is Dr. Steve Albrecht of Brigham Young University. Albrecht and two of his colleagues, Keith R. Howe and Marshall B. Romney, conducted an analysis of 212 frauds in the early 1980s under a grant from the Institute of Internal Auditors Research Foundation, leading to their book entitled *Deterring Fraud: The Internal Auditor's Perspective*.[51] The study's methodology involved obtaining demographics and background information on the frauds through the use of extensive questionnaires. The participants in the survey were internal auditors of companies that had experienced frauds.

Albrecht's research included an examination of comprehensive data sources to assemble a complete list of pressure, opportunity, and integrity variables, resulting in a set of 50 possible red flags or indicators of occupational fraud and abuse. These variables fell into two principal categories: perpetrator characteristics and organizational environment. The purpose of the study was to determine which of the red flags were most important to the commission (and, therefore, to the detection and prevention) of fraud. The red flags ranged from unusually high personal debts to belief that one's job is in jeopardy, from no separation of asset-custodial procedures to not adequately checking a potential employee's background.[52]

The researchers gave participants both sets of 25 motivating factors and asked which factors were present in the frauds they had dealt with. Participants were asked to rank these factors on a seven-point scale indicating the degree to which each factor existed in their specific frauds. The ten most highly ranked factors from the list of personal characteristics, based on this study, were:

1. Living beyond their means
2. An overwhelming desire for personal gain
3. High personal debt
4. A close association with customers

---

[51] Steve Albrecht, Keith R. Howe, and Marshall B. Romney, *Deterring Fraud: The Internal Auditor's Perspective* (Institute of Internal Auditor's Research Foundation, 1984).

[52] While such red flags may be present in many occupational fraud cases, one must re-emphasize Albrecht's caution that the perpetrators are hard to profile and fraud is difficult to predict. To underscore this point, Albrecht's research does not address—and no current research has been done to determine—if nonoffenders have many of the same characteristics. If so, then the list might not be discriminating enough to be useful. In short, while one should be mindful of potential red flags, they should not receive undue attention absent other compelling circumstances.

5. Feeling pay was not commensurate with responsibility
6. A wheeler-dealer attitude
7. Strong challenge to beat the system
8. Excessive gambling habits
9. Undue family or peer pressure
10. No recognition for job performance[53]

These motivators are very similar to the non-shareable financial problems Cressey identified. The ten most highly ranked factors from the list dealing with organizational environment were:

1. Placing too much trust in key employees
2. Lack of proper procedures for authorization of transactions
3. Inadequate disclosures of personal investments and incomes
4. No separation of authorization of transactions from the custody of related assets
5. Lack of independent checks on performance
6. Inadequate attention to details
7. No separation of custody of assets from the accounting for those assets
8. No separation of duties between accounting functions
9. Lack of clear lines of authority and responsibility
10. Department that is not frequently reviewed by internal auditors[54]

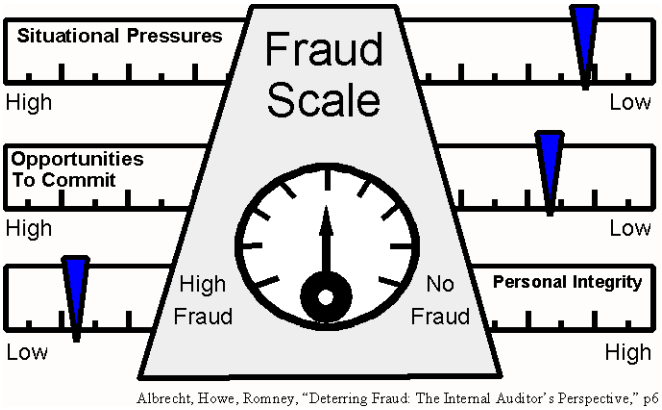
All of the factors on this list affect employees' opportunity to commit fraud without being caught. Opportunity, as you will recall, was the second factor identified in Cressey's fraud triangle. In many ways, the study by Albrecht, et al., supported Cressey's model. Like Cressey's study, the Albrecht study suggests there are three factors involved in occupational frauds:

> *It appears that three elements must be present for a fraud to be committed: a situational pressure (non-shareable financial pressure), a perceived opportunity to commit and conceal the dishonest act (a way to secretly resolve the dishonest act or the lack of deterrence by management), and some way to rationalize (verbalize) the act as either being inconsistent with one's personal level of integrity or justifiable.*[55]

[53] Albrecht, Howe, and Romney, 32.
[54] Ibid., 39.
[55] Ibid., 5.

The Fraud Scale[56]

To illustrate the concept, Albrecht developed the Fraud Scale, which included the components of situational pressures, perceived opportunities, and personal integrity. When situational pressures and perceived opportunities are high and personal integrity is low, occupational fraud is much more likely to occur than when the opposite is true.[57]



Albrecht, Howe, Romney, "Deterring Fraud: The Internal Auditor's Perspective," p6

Albrecht describes situational pressures as "the immediate problems individuals experience within their environments, the most overwhelming of which are probably high personal debts or financial losses."[58] Opportunities to commit fraud, Albrecht says, may be created by individuals, or by deficient or missing internal controls. Personal integrity "refers to the personal code of ethical behavior each person adopts. While this factor appears to be a straightforward determination of whether the person is honest or dishonest, moral development research indicates that the issue is more complex."[59]

In addition to its findings on motivating factors of occupational fraud, the Albrecht study also disclosed several interesting relationships between the perpetrators and the frauds they committed. For example, perpetrators of large frauds used the proceeds to purchase new homes and expensive automobiles, invest in recreation property, and go on expensive vacations, as well as to support extramarital relationships and make speculative investments. Those committing small frauds did not.[60] Perpetrators who were interested primarily in "beating the system" committed larger frauds. However, perpetrators who believed their pay was not adequate committed primarily small frauds. Lack of segregation

[56] Ibid., 5.
[57] Ibid., 6.
[58] Ibid., 5.
[59] Ibid., 6.
[60] Ibid., 42.

of responsibilities, placing undeserved trust in key employees, imposing unrealistic goals, and operating on a crisis basis were all pressures or weaknesses associated with large frauds. College graduates were less likely to spend the proceeds of their loot to go on extravagant vacations, purchase recreational property, support extramarital relationships, and buy expensive automobiles. Finally, those with lower salaries were more likely to have a prior criminal record.[61]

2014 *Report to the Nations on Occupational Fraud and Abuse*

Occupational fraud and abuse is a widespread problem that affects practically every organization, regardless of size, location, or industry. In 1996, the ACFE released the first *Report to the Nation on Occupational Fraud and Abuse*, which was intended to shed light on the immense and largely undefined costs that occupational fraud imposes on organizations. The stated goals of the first Report were to:

- Summarize the opinions of experts on the percentage and amount of organizational revenue lost to all forms of occupational fraud and abuse.
- Examine the characteristics of the employees who commit occupational fraud and abuse.
- Determine what kinds of organizations are victims of occupational fraud and abuse.
- Categorize the ways in which serious fraud and abuse occurs.

All of the enumerated goals of the first Report fell under one larger and more all-encompassing mission: to better educate the public and anti-fraud professionals about the threat of occupational fraud. Since that time, with each subsequent edition of the *Report to the Nation*, this has remained our primary goal.

We released updated editions of the Report in 2002, 2004, 2006, 2008, 2010, 2012, and 2014. Like the first study, each subsequent edition has been based on detailed case information about specific frauds provided by the CFEs who investigated those cases. Each *Report* has been structured along the same lines, focusing on the methods used by employees, managers, and executives to defraud their organizations; the losses caused by those frauds; and the characteristics of both the perpetrators and the victims of these crimes.

[61] Ibid., xiv.

The 2014 edition of the Report is based on 1,483 actual cases of occupational fraud that occurred within more than 100 countries throughout the world. Consequently, the 2014 *Report to the Nations* provides a view into the truly global nature of occupational fraud, as well as the severity and impact of these crimes.

The following is an excerpt containing some of the more significant findings from the 2014 Report. Copies of the entire *Report to the Nations* can be downloaded or viewed at no charge at www.ACFE.com/RTTN.

The Cost of Occupational Fraud

Understandably, there is considerable attention paid to determining the overall cost of fraud. Executives want to know how significant the risk of fraud is to their companies, anti-fraud professionals need to justify budgets and satisfy performance metrics, and the media and general public are curious about just how much money white-collar criminals are taking us for.

Unfortunately, the nature of fraud means that much of its cost is hidden. Because concealment is an intrinsic component of most fraud schemes, some frauds are never uncovered; further, of the cases that are detected, many are never measured or reported. In addition, most frauds carry substantial indirect costs, including lost productivity, reputational damage, and the related loss of business, as well as the costs associated with investigation and remediation of the issues that allowed them to occur. The result is the equivalent of a financial iceberg; some of the direct losses are plainly visible, but there is a huge mass of hidden harm that we cannot see.

Despite the inherent challenges in doing so, determining an estimate for the cost of fraud is an important endeavor. As part of our research, we asked the CFEs who participated in our survey what percentage of annual revenues they believe the typical organization loses to all types of fraud; their responses provided a median estimate of 5%. To illustrate the staggering effect of this finding, applying the percentage to the 2013 estimated Gross World Product of $74.31 trillion results in a projected potential total global fraud loss of nearly $3.7 trillion.[62]

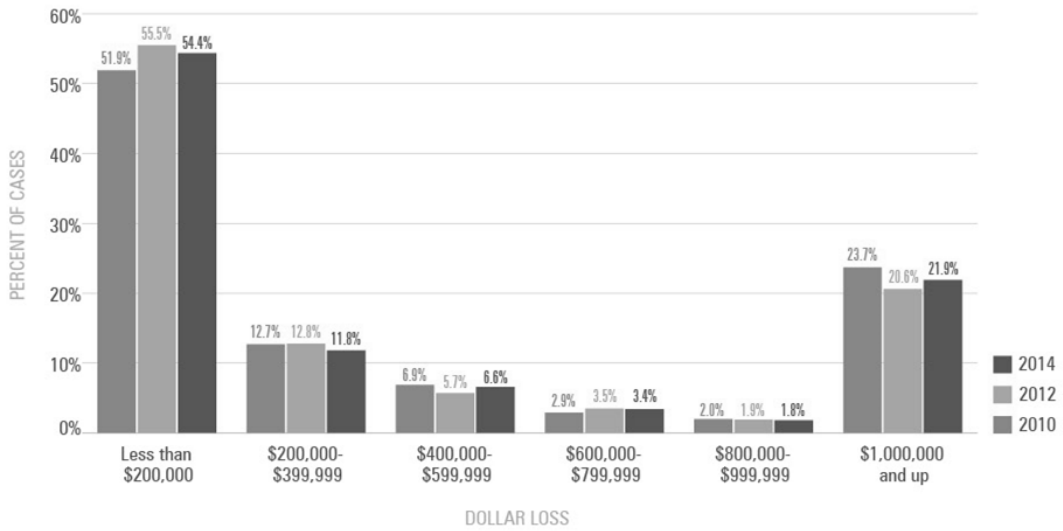
[62] United States Central Intelligence Agency, The World Factbook (www.cia.gov/library/publications/the-world-factbook/geos/xx.html).

It is important to note that this estimate is based on the collective opinion of the more than 1,400 anti-fraud experts who participated in our study, rather than on any specific data or factual observations. As such, it provides an important measure that can be used as a benchmark, but it should not be interpreted as a precise representation of the cost of fraud. Regardless of whether the true cost is 5% or some other portion of the global economy, the total financial impact of fraud surely amounts to hundreds of billions, if not trillions, of dollars each year—an enormous sum lost to an expense that provides absolutely no business or societal benefit.

DISTRIBUTION OF DOLLAR LOSSES

One metric that can be effectively measured and used to analyze the cost of fraud is the amount of financial damage caused by individual instances of known fraud. Of the 1,483 cases in our study, 1,445 included information about the total dollar amount lost to fraud; for those, the median loss caused by the scheme was $145,000. Additionally, over our last three studies, the dollar losses of the cases analyzed have followed a relatively distinct pattern, with just over half causing losses under $200,000 and more than one-fifth involving losses of at least $1 million.

Figure 2: Distribution of Dollar Losses



How Occupational Fraud Is Committed

Technological advancements and the continual evolution of the global business environment provide both enhanced tools and additional challenges for perpetration and concealment—as well as the prevention, detection, and investigation—of fraud. Even in light of such changes, however, our research into occupational fraud has revealed consistent and clear patterns about the form fraud schemes take and the relative cost of each scheme type.

Specifically, occupational frauds can be classified into three primary categories: asset misappropriation, corruption, and financial statement fraud, with each category further broken down into several subcategories as shown in the Occupational Fraud and Abuse Classification System, also known as the Fraud Tree. The thousands of occupational fraud cases analyzed over our last two decades of research have all fallen into one or more of the categories delineated by this graphic.

Of the three primary categories of occupational fraud, asset misappropriation is by far the most common, occurring in more than 85% of cases analyzed for this Report; however, it is also typically the least costly of the three types, causing a median loss of $130,000. In contrast, financial statement fraud occurs much less frequently, accounting for 9% of the cases in our latest survey, but it causes the greatest financial impact of the three categories by far, with a median loss of $1 million. Corruption tends to fall in the middle in terms of both frequency and median loss.

Figure 4: Occupational Frauds by Category — Frequency

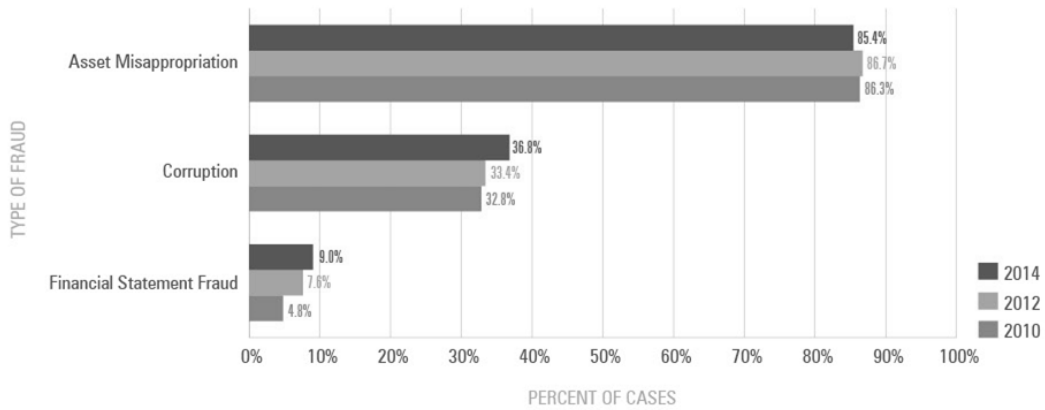
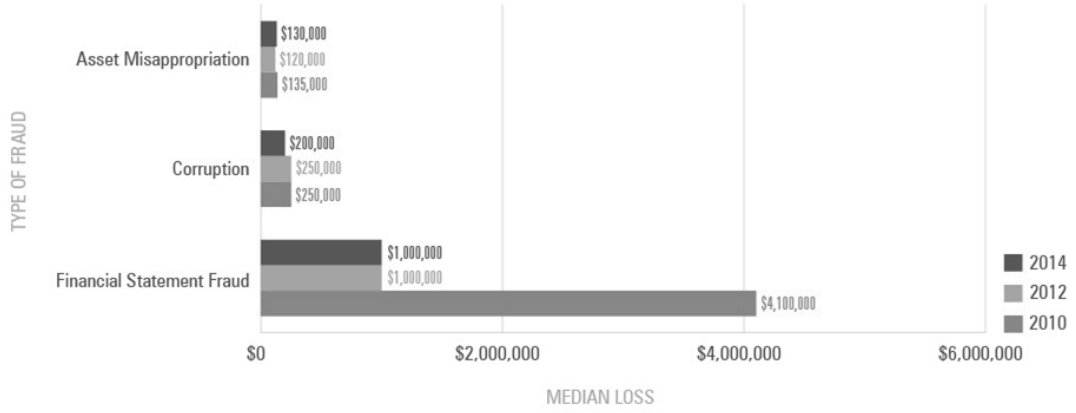


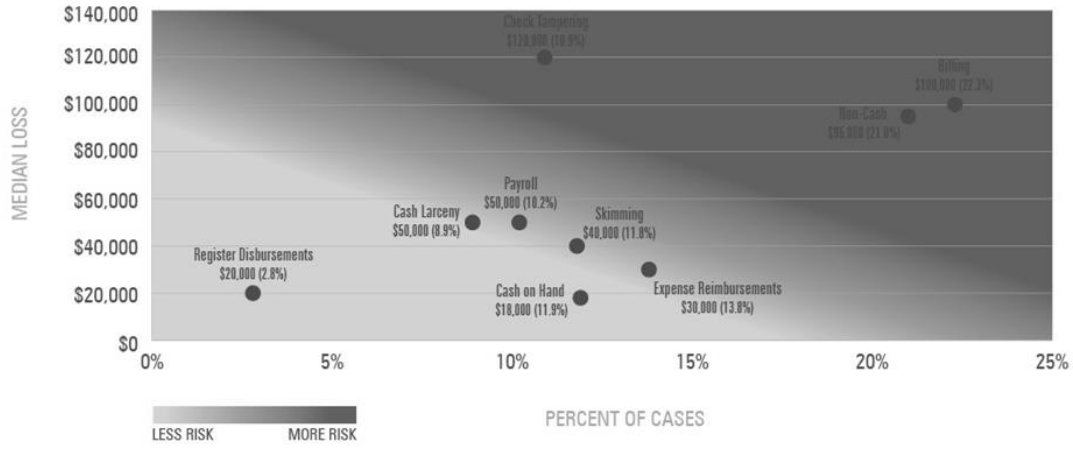
Figure 5: Occupational Frauds by Category — Median Loss



ASSET MISAPPROPRIATION SUB-SCHEMES

In addition to the three primary categories of occupational fraud, we have identified nine subcategories of asset misappropriation schemes, each representing a specific way that employees misappropriate organizational resources. The figure below shows the relative frequency and median loss for each of these scheme types. As illustrated in that figure, schemes involving check tampering, billing and noncash misappropriations tend to represent the greatest risk in terms of combined likelihood and cost.

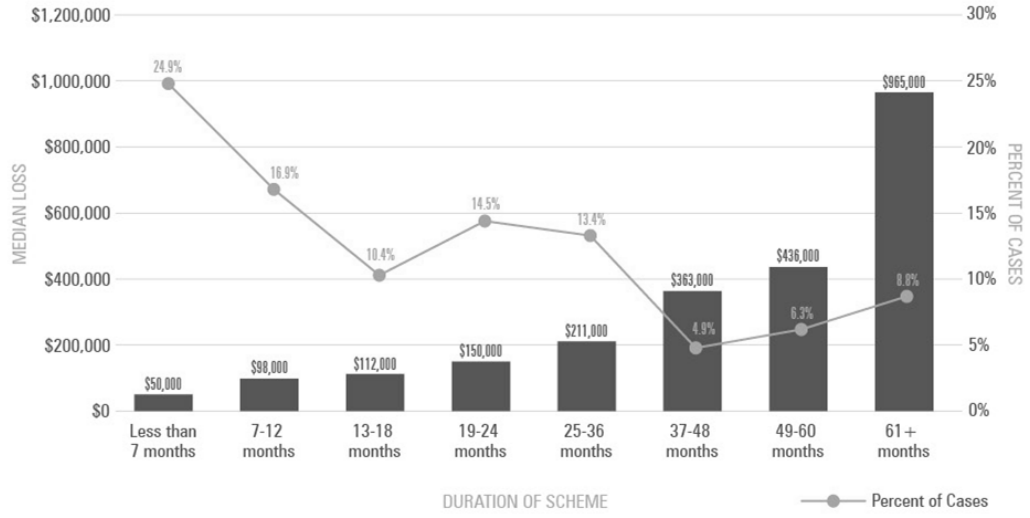
Figure 6: Frequency and Median Loss of Asset Misappropriation Sub-Schemes



DURATION OF FRAUD SCHEMES

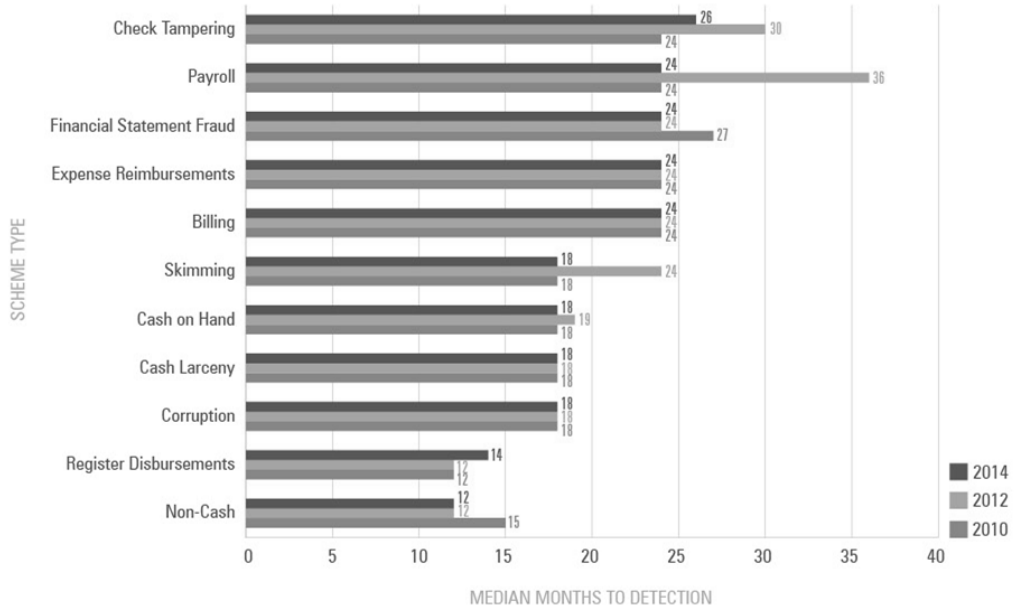
The correlation between how long fraud schemes last and the amount of financial damage they cause might seem self-evident. However, the figure below provides a clear illustration of the importance of early detection. It is encouraging to note that one-quarter of the frauds in our study were detected in the first six months of their occurrence; for those cases, the median loss was limited to $50,000. In contrast, the longer frauds were able to go undetected, the more costly they became.

Figure 9: Frequency and Median Loss Based on Duration of Fraud



The median duration—the amount of time from when the fraud commenced until it was detected—for all schemes in our study was 18 months. In the following figure, we have presented the median duration for each category of occupational fraud. This helps us see where organizational controls can be particularly helpful in identifying frauds earlier and thus limiting losses. The median duration of schemes ranged from 12 months for noncash misappropriations to 26 months for check tampering. Interestingly, although noncash misappropriations were detected the most quickly of all categories, they also had one of the highest median losses of the asset misappropriation categories, indicating that these schemes can cause a large amount of financial damage rather quickly.

Figure 10: Median Duration of Fraud Based on Scheme Type



Detection of Fraud Schemes

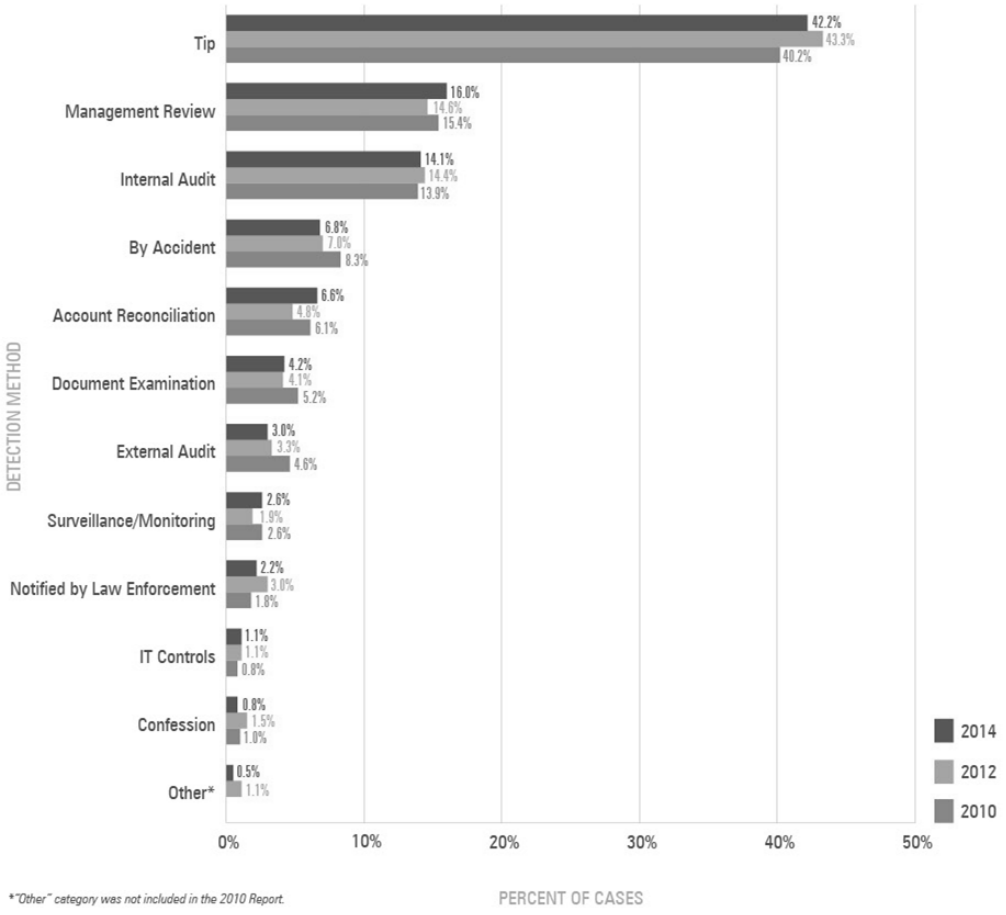
According to the fraud triangle theory—that those who commit occupational fraud tend to have a perceived financial need, opportunity, and rationalization—the threat of likely detection is one of the most powerful factors in fraud prevention because it all but eliminates the fraudster's perceived opportunity. In the 2014 Report and past versions, we asked respondents to provide information on how their occupational fraud schemes were first detected. One of the recurring trends we see is that some detection methods are more effective than others. When comparing the initial detection method to other information, such as the fraud's duration and the financial damage caused, we found substantial differences among the various ways frauds were uncovered. Detection method, therefore, is directly related to both fraud prevention and loss mitigation.

Additionally, the manner by which frauds are detected is not purely incidental. Our data suggests that the likelihood of discovering fraud in particular ways can be shaped by the procedures and controls that an organization has in place. This information can help organizations detect frauds more efficiently.

INITIAL DETECTION OF OCCUPATIONAL FRAUDS

As the figure below demonstrates, tips are consistently the most common detection method for cases of occupational fraud by a significant margin, which has been an observed trend since we first began tracking this data in 2002. Management review and internal audit follow tips, which was also true for the 2010 and 2012 Reports.

Figure 11: Initial Detection of Occupational Frauds



MEDIAN LOSS AND MEDIAN DURATION BY DETECTION METHOD

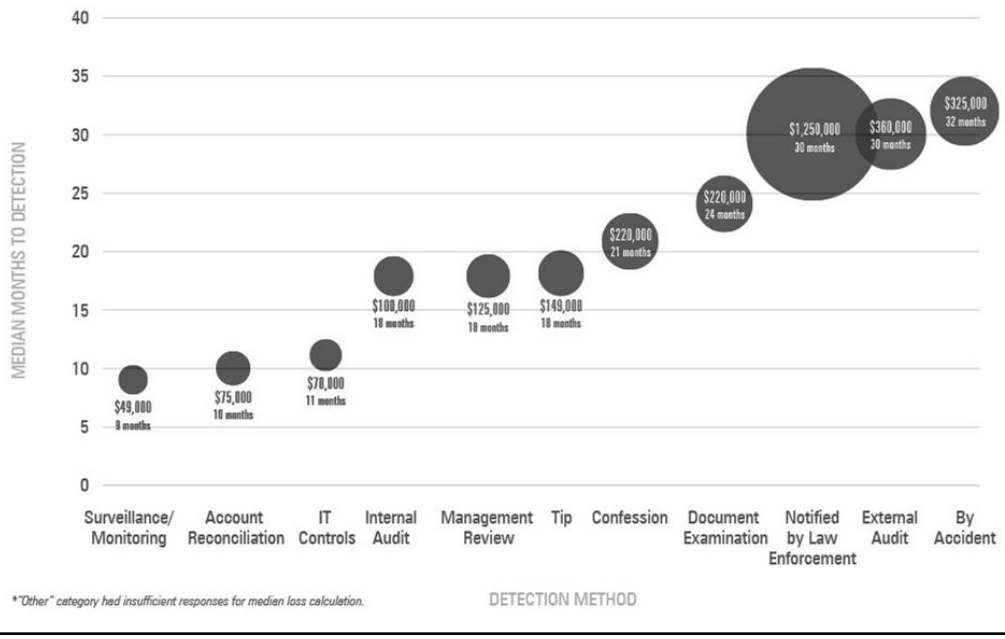
The following figure illustrates the relationship between the detection method, median loss, and median duration of occupational frauds. The larger circles represent a higher median loss, and the detection methods are organized left-to- right in order of median duration. Frauds that were discovered by accident tended to last the longest, with a median duration of 32 months, and had a median loss of $325,000. Schemes that were first detected by

notification from law enforcement caused the highest median loss at $1,250,000 and had a median duration of 30 months.

The data highlights how the results of fraud cases tend to differ based on the initial detection method. One of the most visible distinctions is that the five detection methods with both the shortest duration and lowest loss—surveillance/monitoring, account reconciliation, IT controls, internal audit, and management review—involved proactive efforts to discover fraud. In contrast, detection methods that are not the result of efforts within the organization to detect fraud—confession, notification by law enforcement, external audit, and by accident—tended to last longer and cost more. In other words, having adequate controls that seek out fraud, rather than relying on external or passive detection methods, can dramatically reduce the cost and duration of such schemes.

Other factors that might be affecting this data include the possibility that some schemes that are commonly detected through a particular method tend to involve lower amounts of assets. Additionally, some schemes generally will not be detected by certain methods (e.g., IT controls).

Figure 12: Median Loss and Median Duration by Detection Method

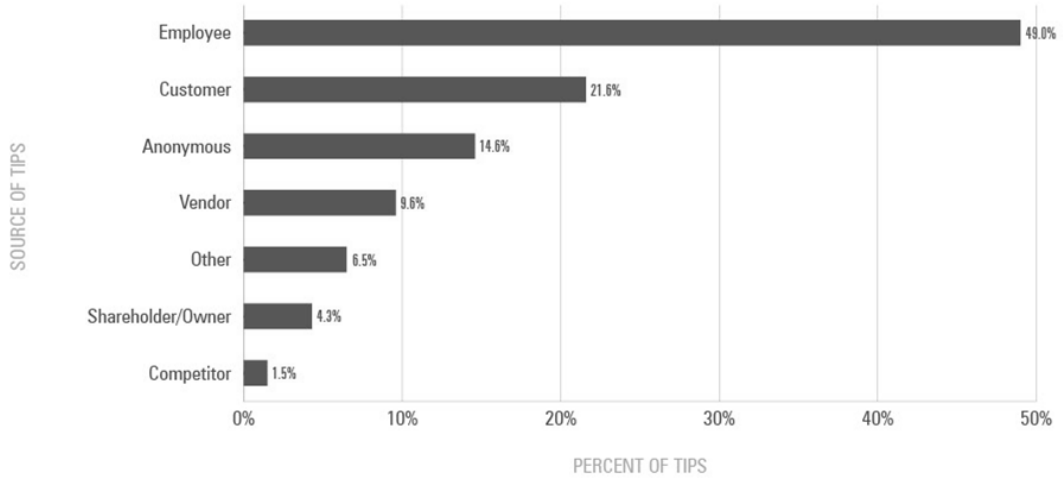


SOURCE OF TIPS

It is well known that employees are a valuable source of information for discovering potential fraud, and the figure below shows that employees were the source of almost half of all tips that led to the detection of fraud. Occupational fraud has a negative impact on an organization, including those who work for it, which might explain why employees so often step forward. At the same time, there is often a risk of backlash for whistleblowers, which might explain why a substantial amount of tips came from anonymous parties (14.6%).

The fact that more than half of all tips involved parties other than confirmed employees emphasizes the importance of cultivating tips from various sources. For example, many employers circulate a whistleblower policy or fraud hotline information to employees only, but our data indicates that it is also advantageous to educate vendors, customers and owners/shareholders on how to report suspicions of fraud.

Figure 13: Source of Tips



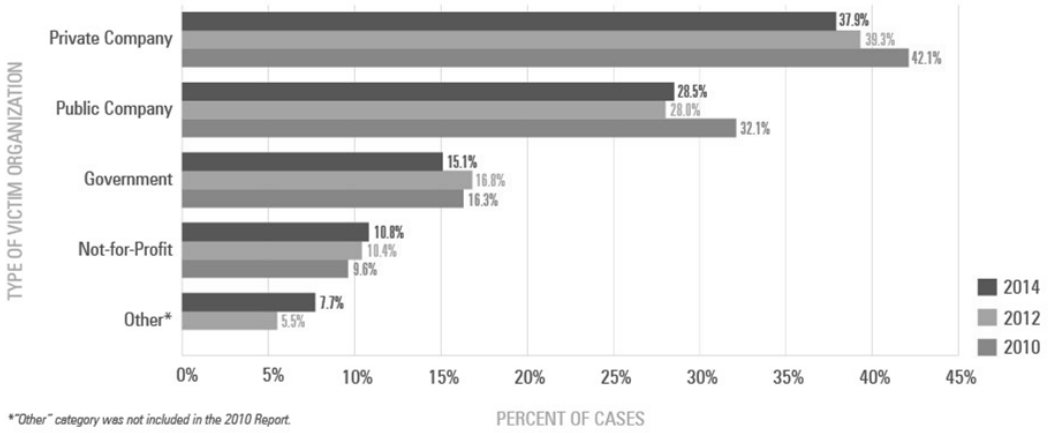
Victims of Occupational Fraud

TYPE OF VICTIM ORGANIZATION

As in our previous studies, privately owned and publicly traded organizations accounted for approximately two-thirds of the victims in the cases reported to us. These for-profit organizations also suffered the greatest median losses, which is consistent with our previous

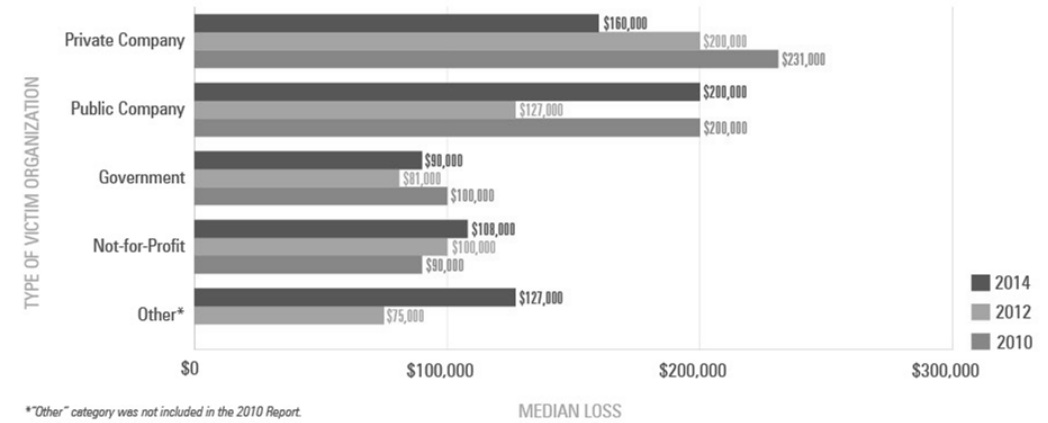
Reports. In contrast, government entities and not-for-profits made up 15.1% and 10.8%, respectively, of the cases analyzed and reported much lower median losses than their for-profit counterparts.

Figure 17: Type of Victim Organization — Frequency



*"Other" category was not included in the 2010 Report.

Figure 18: Type of Victim Organization — Median Loss



*"Other" category was not included in the 2010 Report.

SIZE OF VICTIM ORGANIZATION

Small businesses (defined as those with fewer than 100 employees) were victimized in the greatest percentage of cases reported to us, which is consistent with previous Reports. In addition, the median losses for small businesses and the largest entities (those with more than 10,000 employees) were the highest, at $154,000 and $160,000, respectively. While the absolute median loss for the largest entities is slightly higher than that for small businesses, it is important to note that the overall impact of a $154,000 loss for many small businesses is much greater than the relative impact of a $160,000 loss at an organization with more than 10,000 employees.

Figure 19: Size of Victim Organization — Frequency

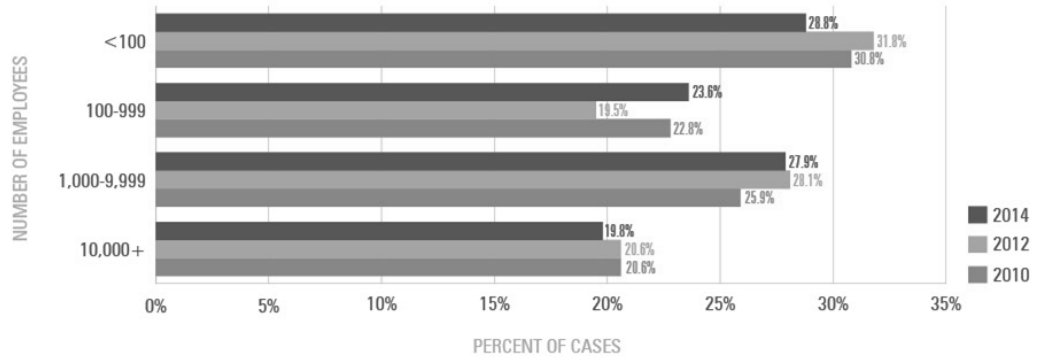
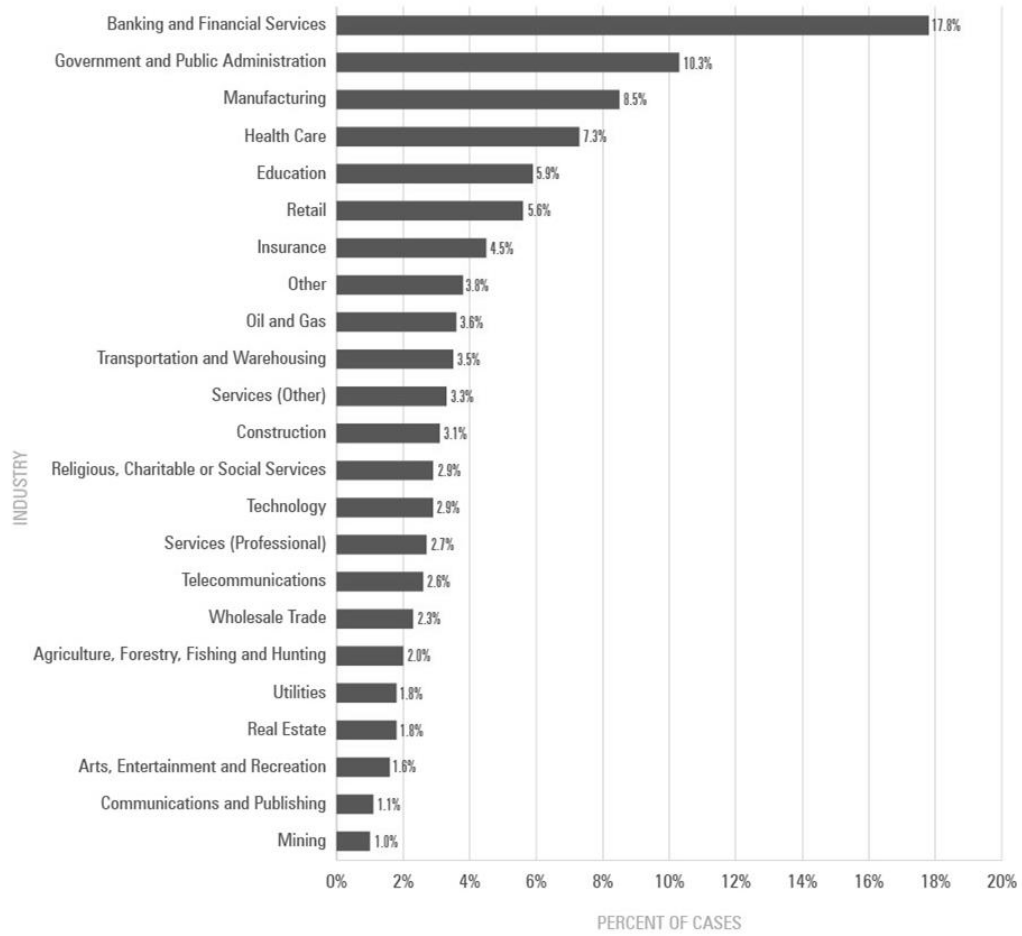


Figure 20: Size of Victim Organization — Median Loss

INDUSTRY OF VICTIM ORGANIZATION

The following figure categorizes the cases reported to us by industry of the victim organization. Similar to the findings in our previous Reports, banking and financial services, government and public administration, and manufacturing were the most represented sectors among the fraud cases analyzed. On the other end of the spectrum, the industries with the lowest frequency of fraud cases were mining; communications and publishing; and arts, entertainment, and recreation. While this data shows the distribution of cases in our study, it does not necessarily mean that certain industries are more at risk of fraud than others. Our study focuses on cases investigated by CFEs, so this figure primarily reflects the industries in which CFEs work. The fact that CFEs tend to be hired more in some industries than others could indicate those industries are at greater risk of fraud, but it could also be a sign that they are more proactive in dealing with anti-fraud issues.

Figure 22: Industry of Victim Organizations



The figure that follows sorts the various industries by median loss. Although the mining industry had the fewest number of cases, it suffered the greatest median loss of $900,000. Cases in the real estate, oil and gas, and wholesale trade industries also caused notably large median losses. In contrast, the government and public administration sector had the second largest number of reported cases of fraud, but those cases caused a median loss of only $64,000. Banking and financial services, manufacturing, and health care were also among the most represented industries in our study; however, the median losses incurred by these organizations were in the middle of the spectrum with median losses of $200,000, $250,000, and $175,000, respectively.

Figure 23: Industry of Victim Organizations (Sorted by Median Loss)

Industry	Number of Cases	Percent of Cases	Median Loss
Mining	13	1.0%	$900,000
Real Estate	24	1.8%	$555,000
Oil and Gas	49	3.6%	$450,000
Wholesale Trade	31	2.3%	$375,000
Technology	39	2.9%	$250,000
Manufacturing	116	8.5%	$250,000
Construction	43	3.1%	$245,000
Agriculture, Forestry, Fishing and Hunting	28	2.0%	$242,000
Transportation and Warehousing	48	3.5%	$202,000
Banking and Financial Services	244	17.8%	$200,000
Services (Professional)	37	2.7%	$180,000
Health Care	100	7.3%	$175,000
Arts, Entertainment and Recreation	22	1.6%	$168,000
Other	52	3.8%	$130,000
Services (Other)	45	3.3%	$125,000
Telecommunications	36	2.6%	$120,000
Utilities	25	1.8%	$100,000
Insurance	62	4.5%	$93,000
Religious, Charitable or Social Services	40	2.9%	$80,000
Government and Public Administration	141	10.3%	$64,000
Education	80	5.9%	$58,000
Retail	77	5.6%	$54,000
Communications and Publishing	15	1.1%	$50,000

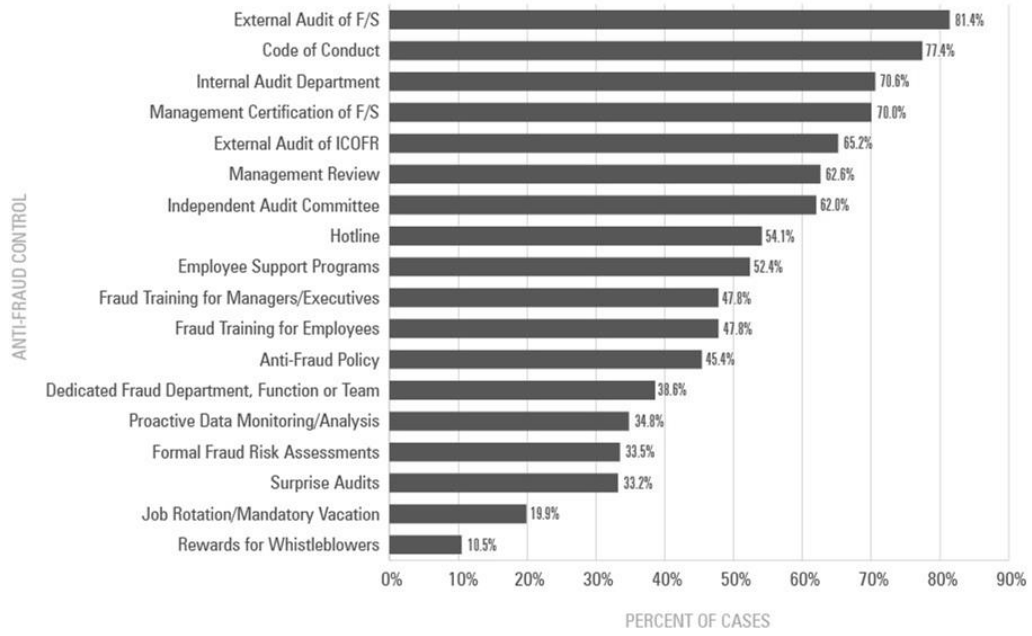
ANTI-FRAUD CONTROLS AT THE VICTIM ORGANIZATION

Proactive fraud prevention and detection controls are a vital part in managing the risk of fraud, but are all anti-fraud controls created equal? As part of our survey, we asked participants to identify which of 18 common anti-fraud controls were present at the victim organization at the time the fraud occurred. The responses are reflected in the following figure, which shows that external audits were the most common control enacted by the victim organizations, as they were present in more than 80% of the cases reported to us. But as noted previously, external audits accounted for the detection of just 3% of the cases in

our study. While external audits serve many important functions, this suggests they should not be strongly relied upon as a fraud detection tool.

With more than 42% of frauds being detected by tips, hotlines ought to play a critical role in organizations' anti-fraud programs. But of the organizations victimized by the frauds in our study, only 54% had a hotline mechanism in place, and less than 11% provided rewards for whistleblowers. These rates indicate that many organizations have room for improvement in encouraging the tips that so effectively help uncover fraudulent conduct.

Figure 26: Frequency of Anti-Fraud Controls

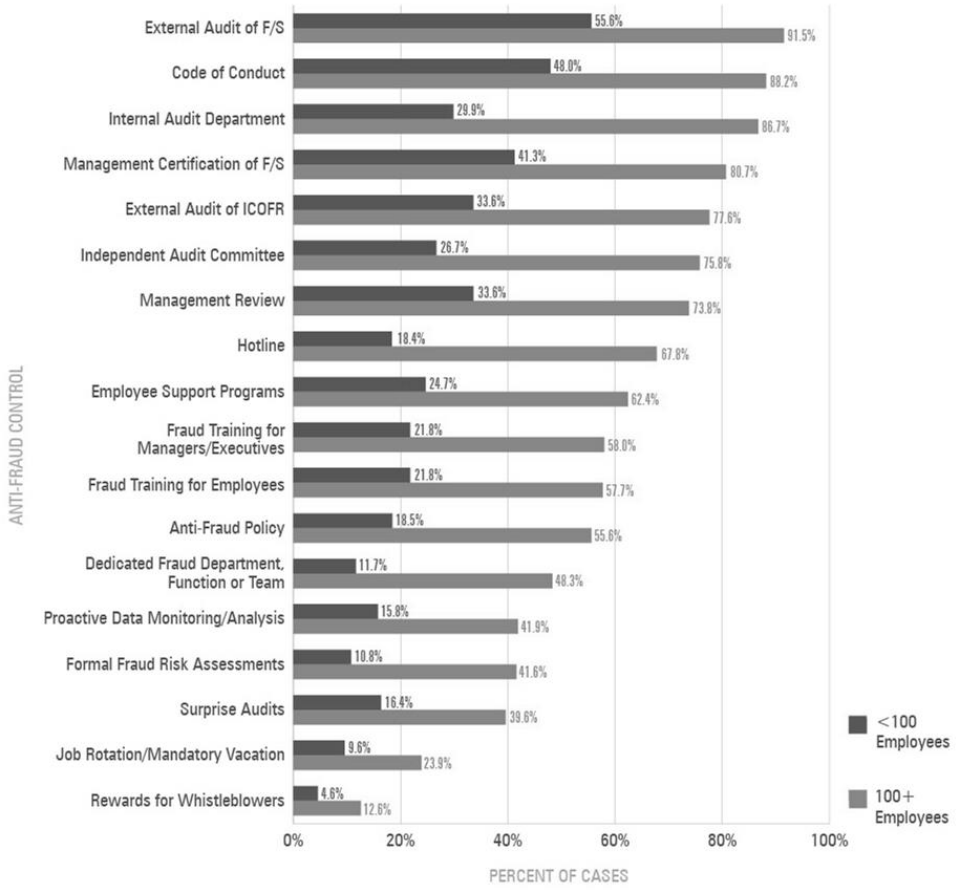


ANTI-FRAUD CONTROLS AT SMALL BUSINESSES

The limited financial and human resources at most small organizations make them uniquely susceptible to fraud; they often lack the means to enact sophisticated anti-fraud controls, and they can be particularly devastated by the fallout from any fraud that does occur. As noted above, the median loss per fraud scheme at small businesses is $154,000—an amount that represents a significant portion of many small businesses' budgets. In the following figure, we compared the frequency of anti-fraud controls at entities with fewer than 100 employees to the frequency of those controls at their larger counterparts. Across the board, the larger organizations had a substantially greater implementation rate than did the small businesses.

Although some of the controls analyzed require a significant investment and likely are not feasible for many small businesses to implement, many of the controls—such as a code of conduct, an anti-fraud policy, management review procedures, and anti-fraud training programs—can be enacted with relatively little cost and could greatly enhance small businesses' ability to protect their resources from fraud.

Figure 27: Frequency of Anti-Fraud Controls by Size of Victim Organization



EFFECTIVENESS OF CONTROLS

We compared the median loss and median duration of fraud schemes based on whether the victim organization had particular controls in place at the time the fraud occurred. As shown in the following two figures, every control was associated with reductions in both the cost and duration of fraud. Of the controls analyzed, proactive data monitoring and analysis appears to be the most effective at limiting the duration and cost of fraud schemes; victim organizations that implemented this control experienced losses 60% smaller and schemes 50% shorter than organizations that did not.

Figure 37: Median Loss Based on Presence of Anti-Fraud Controls

Control	Percent of Cases	Control in Place	Control Not in Place	Percent Reduction
Proactive Data Monitoring/Analysis	34.8%	$73,000	$181,000	59.7%
Employee Support Programs	52.4%	$90,000	$200,000	55.0%
Management Review	62.6%	$100,000	$208,000	51.9%
Code of Conduct	77.4%	$100,000	$200,000	50.0%
Internal Audit Department	70.6%	$100,000	$180,000	44.4%
Formal Fraud Risk Assessments	33.5%	$94,000	$168,000	44.0%
Surprise Audits	33.2%	$93,000	$164,000	43.3%
External Audit of ICOFR	65.2%	$103,000	$180,000	42.8%
Fraud Training for Managers/Executives	47.8%	$100,000	$168,000	40.5%
Hotline	54.1%	$100,000	$168,000	40.5%
Dedicated Fraud Department, Function or Team	38.6%	$100,000	$164,000	39.0%
Fraud Training for Employees	47.8%	$100,000	$164,000	39.0%
Anti-Fraud Policy	45.4%	$100,000	$155,000	35.5%
Management Certification of F/S	70.0%	$120,000	$184,000	34.8%
Job Rotation/Mandatory Vacation	19.9%	$100,000	$150,000	33.3%
External Audit of F/S	81.4%	$125,000	$186,000	32.8%
Rewards for Whistleblowers	10.5%	$100,000	$135,000	25.9%
Independent Audit Committee	62.0%	$120,000	$150,000	20.0%

Figure 38: Median Duration of Fraud Based on Presence of Anti-Fraud Controls

Control	Percent of Cases	Control in Place	Control Not in Place	Percent Reduction
Surprise Audits	33.2%	12 months	24 months	50.0%
Proactive Data Monitoring/Analysis	34.8%	12 months	24 months	50.0%
Dedicated Fraud Department, Function or Team	38.6%	12 months	24 months	50.0%
Anti-Fraud Policy	45.4%	12 months	24 months	50.0%
Fraud Training for Employees	47.8%	12 months	24 months	50.0%
Hotline	54.1%	12 months	24 months	50.0%
Formal Fraud Risk Assessments	33.5%	12 months	23 months	47.8%
Management Review	62.6%	13 months	24 months	45.8%
Independent Audit Committee	62.0%	14 months	24 months	41.7%
Internal Audit Department	70.6%	14 months	24 months	41.7%
Job Rotation/Mandatory Vacation	19.9%	12 months	20 months	40.0%
Fraud Training for Managers/Executives	47.8%	13 months	21 months	38.1%
External Audit of ICOFR	65.2%	15 months	24 months	37.5%
Management Certification of F/S	70.0%	15 months	24 months	37.5%
Rewards for Whistleblowers	10.5%	12 months	18 months	33.3%
Code of Conduct	77.4%	16 months	24 months	33.3%
External Audit of F/S	81.4%	18 months	24 months	25.0%
Employee Support Programs	52.4%	14 months	18 months	22.2%

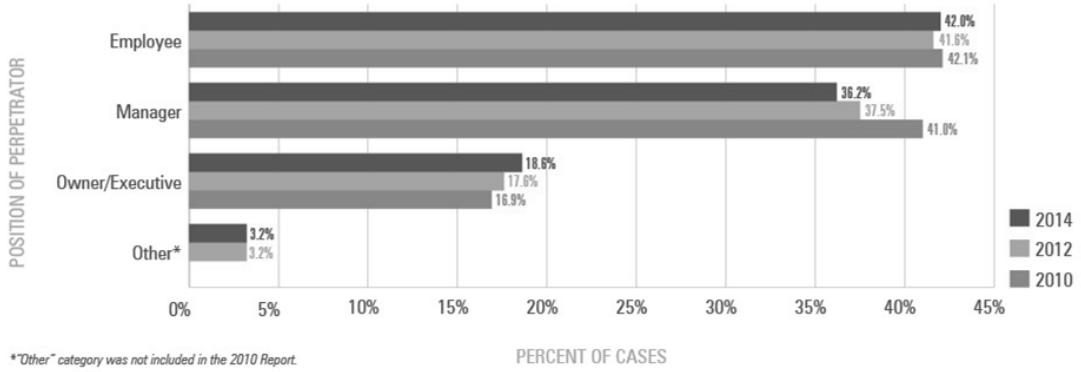
The Perpetrators

As part of our survey, we asked respondents to supply detailed information about the perpetrators of the frauds they had investigated. This includes data on level of authority, age, gender, tenure with the victim organization, education level, department, criminal and employment history, and red flags that the fraudster exhibited before the scheme was detected. The value of this information is that it helps us identify and quantify where fraud risk might lie within a particular organization: What departments tend to be associated with which types of frauds? What demographic factors seem to impact the frequency or severity of occupational frauds? What behavioral clues might have led the victim organizations to identify these crimes earlier? Also, because this data has been gathered over several years' worth of reports, we are able to show how consistent the patterns of fraud and abuse tend to be over time.

PERPETRATOR'S POSITION

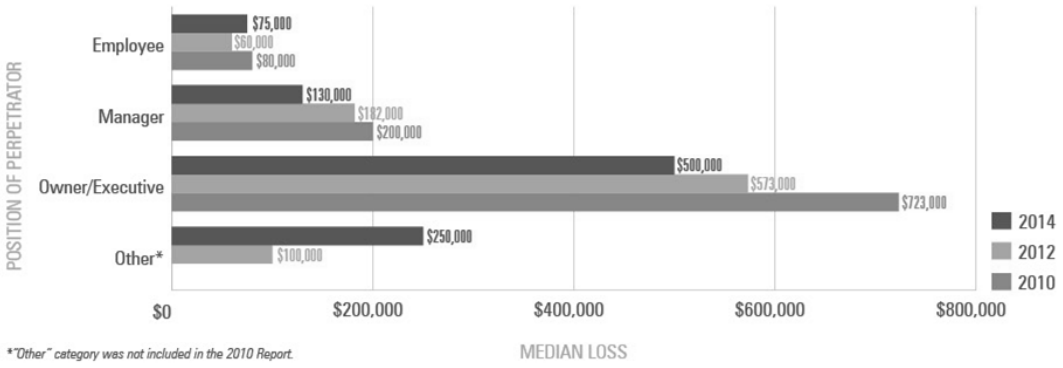
The following figure shows the distribution of fraud perpetrators based on their level of authority. Forty-two percent of occupational frauds were committed by employee-level perpetrators, 36% were committed by managers, and approximately 19% were committed by owners/executives. The distribution of these categories has remained remarkably consistent from year to year.

Figure 40: Position of Perpetrator — Frequency



The following figure shows the strong correlation between a fraudster's level of authority and the financial impact of the fraud. In our 2014 data, owners/executives accounted for less than one-fifth of all frauds, but the median loss in owner/executive cases was $500,000, approximately four times higher than the median loss caused by managers and nearly seven times that of employees. Authority tends to be strongly correlated with loss because high-level fraudsters generally have greater access to organizational assets and are better able to evade or override controls than lower-level employees.

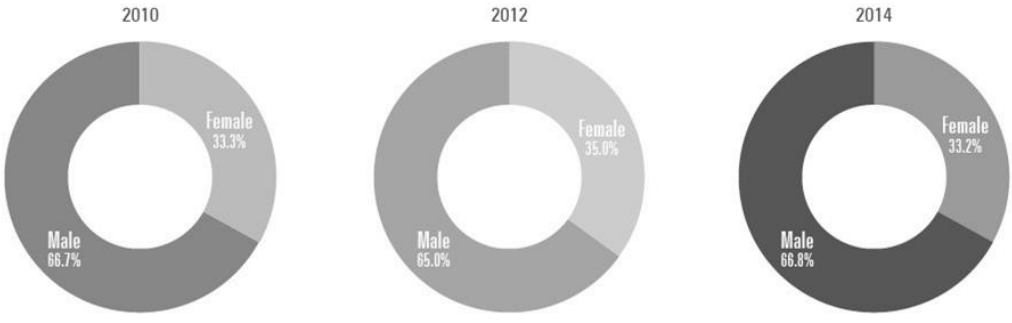
Figure 41: Position of Perpetrator — Median Loss



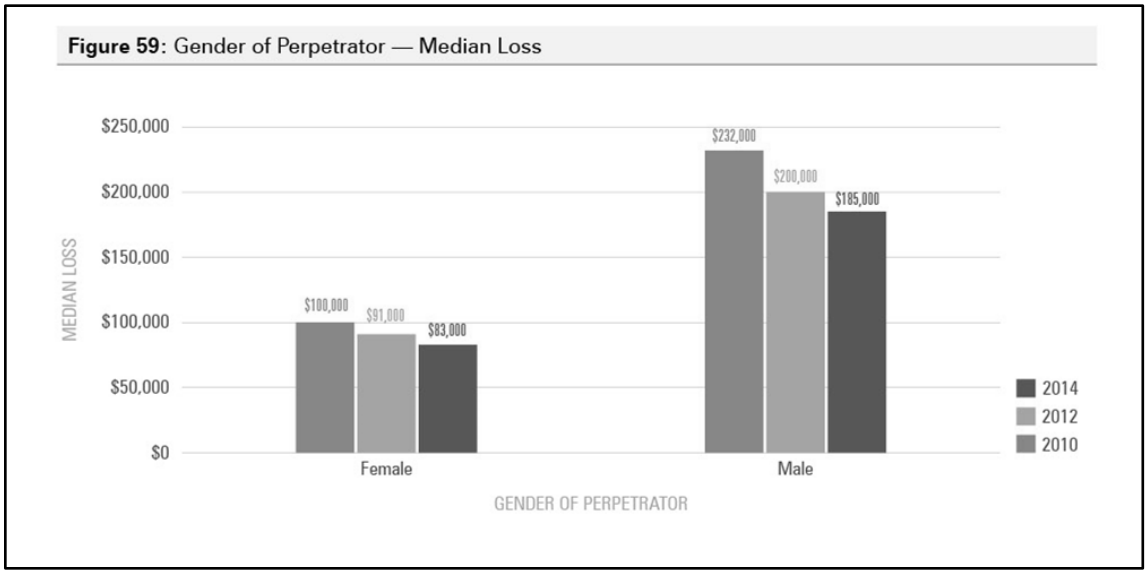
PERPETRATOR'S GENDER

The following figure shows that approximately two-thirds of the fraudsters identified in our study were male, which is consistent with past findings.

Figure 57: Gender of Perpetrator — Frequency



As in our past studies, we found that males tend to cause much higher fraud losses than females. In our 2014 study, the median male loss was $185,000, which was 123% higher than the median female loss. This relationship has remained extremely consistent over time. In our last three studies, the median loss caused by males has ranged between 120% and 132% higher than the female median loss. Interestingly, the ratio in the size of losses caused by each gender did not significantly change, even though our dataset changed from U.S.-only cases (in 2010) to global cases (2012 and 2014), which have a much higher proportion of male fraudsters.



PERPETRATOR'S AGE

The age distribution of the fraudsters in our study is shown below. This distribution is very similar to those of our previous studies, with approximately 52% of perpetrators between the ages of 31 and 45.

While the age distribution of fraudsters fits a bell curve model, the median loss of frauds tends to rise with the age of the perpetrator. In our 2014 data, the rise was fairly gradual and consistent as ages increased. In 2010 and 2012, we saw certain outlier categories where median losses jumped significantly (in the >60 age range for 2010 and in the 51–55 age range for 2012). Overall, however, the data seem to show that older fraudsters tend to generate larger losses. This is probably an indirect reflection of the fact that high-level personnel within an organization tend to be older than lower-level employees. For example, 36% of the fraudsters in our study who were over 50 years of age were owners/executives, while only 15% of those who were 50 or younger were owners/executives.

Figure 55: Age of Perpetrator — Frequency

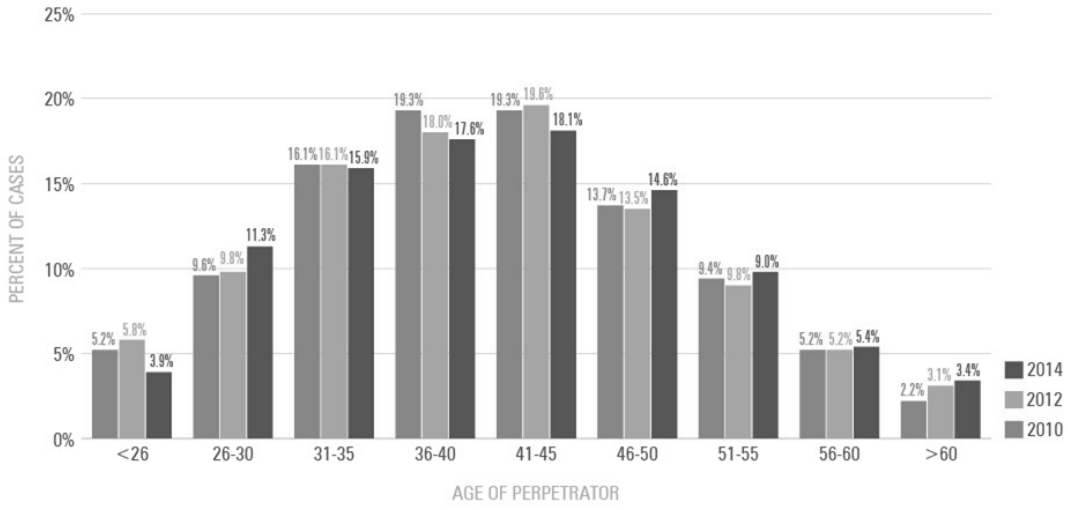
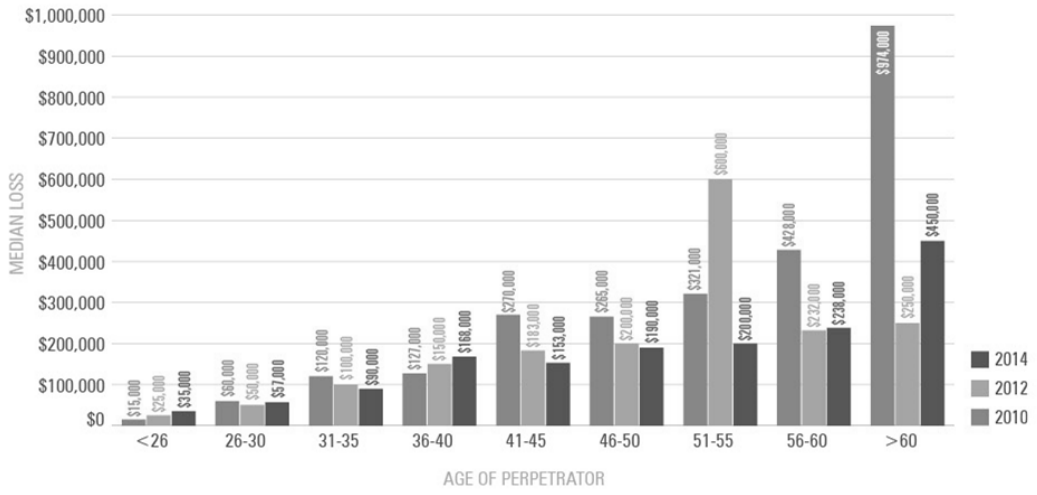


Figure 56: Age of Perpetrator — Median Loss

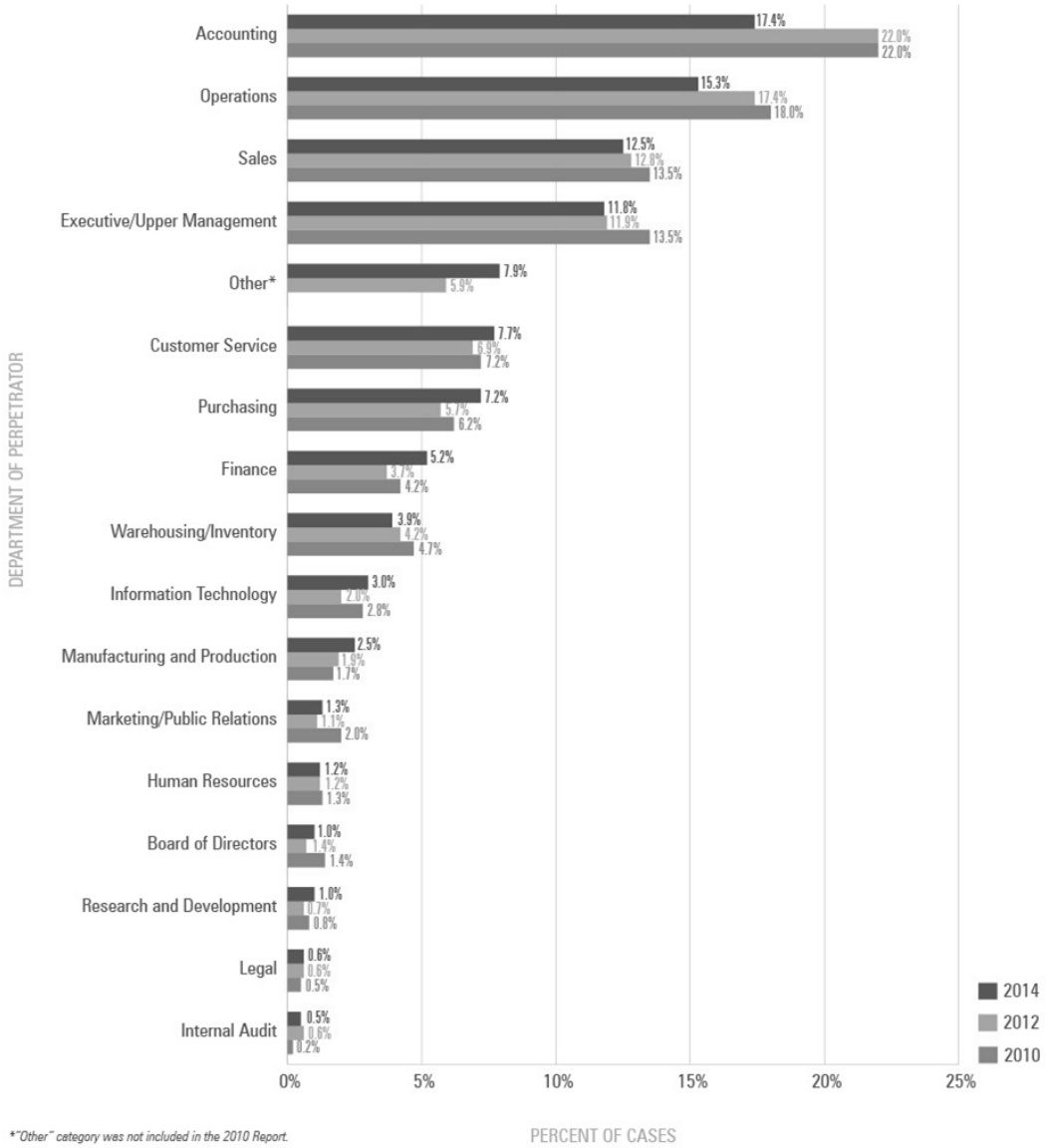


PERPETRATOR'S DEPARTMENT

The following figure shows the departments that the fraud perpetrators worked in. There were seven departments that each accounted for 5% or more of all cases: accounting, operations, sales, executive/upper management, customer service, purchasing, and finance. Collectively, these seven departments were responsible for approximately 77% of all frauds in our study. The department with the greatest incidence of fraud was accounting, but the

level of frauds perpetrated by accounting personnel in our 2014 study (17%) was much lower than what we found in our two previous Reports. However, this was the first study we've conducted in which frauds in the finance department accounted for at least 5% of all cases.

Figure 66: Department of Perpetrator — Frequency



Sorting departments based on median loss shows that the largest frauds are committed by executives and upper management. This is not surprising because this group tends to have the highest authority within an organization. Among the seven departments that each accounted for at least 5% of cases, the finance department caused the second-highest median loss, followed by purchasing, accounting, operations, sales, and customer service.

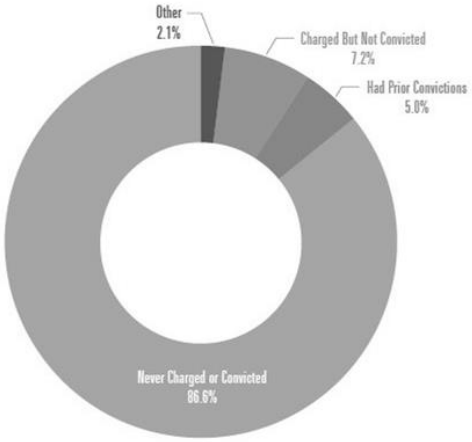
Figure 67: Department of Perpetrator (Sorted by Median Loss)

Department	Number of Cases	Percentage	Median Loss
Executive/Upper Management	156	11.8%	$680,000
Board of Directors	13	1.0%	$500,000
Finance	69	5.2%	$500,000
Warehousing/Inventory	52	3.9%	$245,000
Purchasing	95	7.2%	$166,000
Marketing/Public Relations	17	1.3%	$160,000
Manufacturing and Production	33	2.5%	$150,000
Accounting	230	17.4%	$150,000
Other	105	7.9%	$100,000
Operations	203	15.3%	$100,000
Human Resources	16	1.2%	$94,000
Sales	166	12.5%	$80,000
Customer Service	102	7.7%	$54,000
Research and Development	13	1.0%	$50,000
Information Technology	40	3.0%	$50,000
Legal	8	0.6%	$44,000
Internal Audit	7	0.5%	$25,000

PERPETRATOR'S CRIMINAL BACKGROUND

Only 5% of the fraudsters in our study had been convicted of a fraud-related offense prior to committing the crimes in our study. This is consistent with our previous data, which show that generally fewer than 8% of fraud perpetrators have a prior conviction. Interestingly, when we compared perpetrators with prior convictions to those without, we found no significant difference in the size of their frauds. The median loss caused by those with prior convictions was $154,000, while the median loss caused by those who had never been charged or convicted was $153,000.

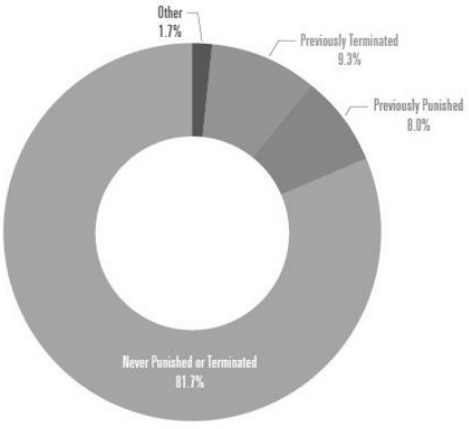
Figure 69: Criminal Background of Perpetrator



PERPETRATOR'S EMPLOYMENT HISTORY

In addition to collecting data about prior convictions, we asked respondents to tell us whether the fraudsters had ever been punished or fired for fraud-related conduct prior to the crimes reported in our study. Only 710 respondents were able to answer this question, but from those who did, we found that just over 9% of fraudsters had been previously terminated and 8% had been previously punished for fraud-related conduct. Those who had previously been punished or terminated actually caused significantly lower losses than those with no record of employer discipline. The median loss for those who had been previously terminated was $125,000, and the median loss for those who had been previously punished was $109,000; in contrast, the median loss caused by individuals who had never been punished or terminated was $200,000.

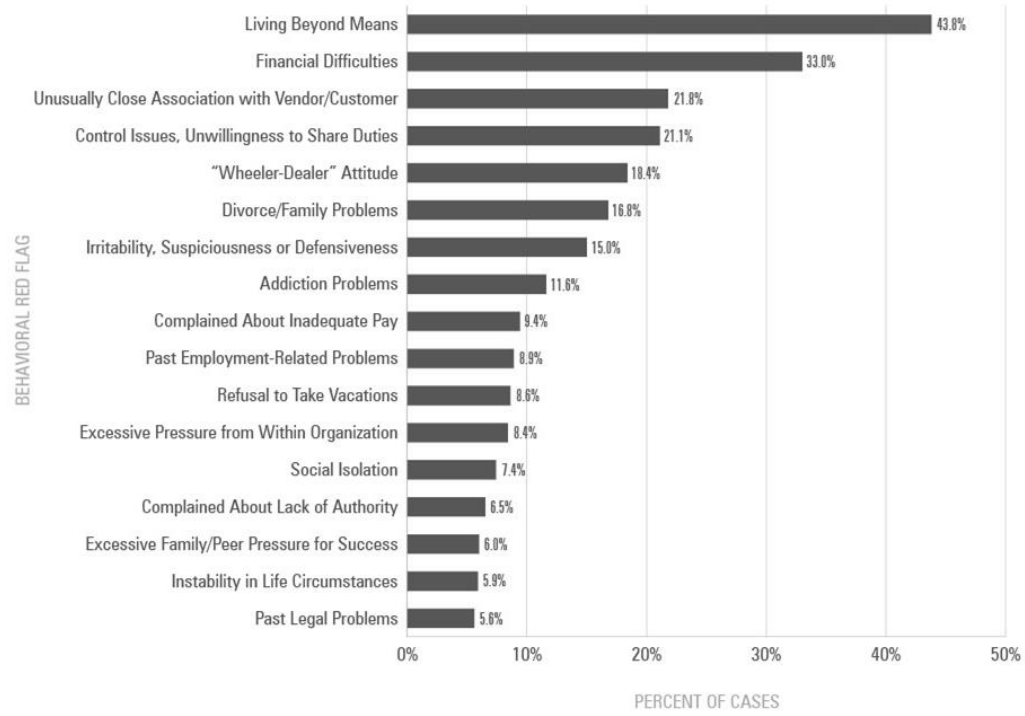
Figure 70: Employment Background of Perpetrator



BEHAVIORAL RED FLAGS DISPLAYED BY PERPETRATORS

Our survey respondents were asked to identify which, if any, common behavioral indicators were exhibited by the perpetrators before their frauds were detected. Overall, at least one red flag was identified in 92% of cases, and, in 64% of cases, the fraudster displayed two or more behavioral red flags. The following figure shows the distribution of those red flags. Approximately 44% of fraud perpetrators were living beyond their means while the fraud was ongoing, and 33% were experiencing known financial difficulties. Other common red flags were an unusually close association with a vendor or customer (22%), displaying control issues or an unwillingness to share duties (21%), a general "wheeler-dealer" attitude involving shrewd or unscrupulous behavior (18%), and recent divorce or family problems (17%). These six red flags were also the most common behavioral indicators in each of our last three studies. In general, the distribution of behavioral red flags from year to year has followed a remarkably consistent curve despite the fact that each of our studies contains entirely distinct cases of fraud and perpetrators.

Figure 71: Behavioral Red Flags Displayed by Perpetrators



CORPORATE GOVERNANCE

What Is Corporate Governance?

The term *corporate governance* essentially refers to a corporation's government; the term is broadly used to describe the oversight responsibilities of different parties for an organization's direction, operations, and performance. More specifically, the Organisation for Economic Co-operation and Development (OECD) defines corporate governance as:

> *[The] procedures and processes according to which an organisation is directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among the different participants in the organisation—such as the board, managers, shareholders and other stakeholders—and lays down the rules and procedures for decision-making.*[1]

Sir Adrian Cadbury, chairman of the committee that developed the foundational corporate governance guidance *The Cadbury Report*, stated that the purpose of corporate governance is "to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources. The aim is to align as nearly as possible the interests of individuals, corporations, and society."[2]

An organization's corporate governance structure provides the lines of accountability and reporting, defines the relationships and expectations of the parties involved, and sets the rules and practices that these parties must follow in carrying out their responsibilities. The checks-and-balances system of corporate governance ensures that no single party is capable of making all the business decisions without the influence, input, or approval of other parties. Solid corporate governance practices are most necessary in organizations in which a company's owners are not also the individuals responsible for setting its strategy and carrying out its business activities (e.g., in publicly traded companies).

Who Is Involved in Corporate Governance?

Historically, the concept of corporate governance has centered primarily on the activities of the board of directors. In recent years, however, the concept has generally expanded to

[1] OECD, "Glossary of Statistical Terms," July 2005. https://stats.oecd.org/glossary/detail.asp?ID=6778.
[2] Sir Adrian Cadbury, *Corporate Governance: A Framework for Implementation* (Foreword), World Bank, 2000.

include the rights and responsibilities of all parties across the entire business. Typical parties now considered to be included in the corporate governance structure are:

- The board of directors and its sub-committees
- Management
- Shareholders

Board of Directors

The board is made up of individuals—or directors—generally elected by the entity's voting members (e.g., shareholders in the case of a corporation or members in the case of an association). Depending on an organization's structure, type, and location, this body might also be called the board of governors, board of regents, or board of trustees.

Elected directors might be major shareholders or executives of the organization (often referred to as *inside directors*), or they might be completely independent of the organization aside from their role on the board (often referred to as *independent directors* or *outside directors*).

In some countries, such as many in the European Union and in Asia, corporations are governed by two separate boards, providing a formalized two-tiered system. The *executive board*, headed by the company CEO and composed of company executives, oversees the business's day-to-day operations. Overseeing the executive board is the *supervisory board*, which is headed by the chairman and composed of non-executive directors who are elected by the shareholders.

The directors represent the middlemen between the corporation's owners (i.e., shareholders) and those actually carrying out its activities (i.e., management), and act as guardians of the organization's resources and assets. As such, the board oversees business operations by assessing the strategy and underlying purpose of management's decisions and actions.

Board Structure

Board structures vary across countries. Some countries, such as the United States, have a one-tier board system in which the independent and non-independent directors form a single board, the board of directors. Many other countries, such as those in Western Europe, have a two-tier board system. A two-tier system features two separate boards: executive/management and supervisory. The executive/management board comprises company executives and other non-independent directors. The supervisory board consists of independent directors.

On a one-tier board, directors are responsible for both the performance of the organization and ensuring its interests are aligned with those of shareholders. In other words, the board is expected to be involved in strategy formulation and policy making, while also supervising management performance and ensuring appropriate compliance with regulations. In contrast, in a two-tier board structure, the executive board is responsible for performance and the supervisory board for conformance, with no common membership allowed between the two boards.

Board Selection

Theoretically, the shareholders choose who is going to sit on a board. Shareholders typically submit their votes for directors either at the general shareholder meeting or by proxy statement. Potential board members are primarily nominated by the board as a whole or by its nominating committee; in many jurisdictions, shareholders are also permitted to submit nominees, though there are often restrictions to doing so.

Independent nomination of board members is critical to ensure there are no conflicts of interest, to prevent instances of collusion between board members and management, and to make certain that board members have shareholders' best interests in mind.

CEO as Chairman

Public companies are required to have someone serve as chairman of the board. The norm in some jurisdictions has been for companies to combine the position of CEO and board chairman (CEO duality). However, concern that this arrangement leads to an inherent conflict of interest has driven many companies to reconsider this dual role.

CEO duality concentrates significant power in the hands of one person by allowing the CEO to undertake the two most important functions of corporate governance—managerial and oversight. In essence, the CEO is empowered to manage the company's operations while also overseeing the board.

Ideally, two qualified individuals with knowledge of the organization's industry should serve these roles independently. The advantages of separating these roles include:

- Better alignment with corporate governance best practices
- Improvement of CEO's accountability
- Reduction in CEO's potential conflicts of interest
- More effective board oversight

Board Committees

To aid in oversight of specific issues, the board might delegate members to focused sub-committees. It is considered a best practice for public companies to form at least the following three board committees:

- Audit committee
- Compensation committee
- Nominating committee

Many private companies and nonprofit organizations elect to have these committees as well. Additionally, some boards delegate other committees, such as a governance committee or a risk committee.

AUDIT COMMITTEE

The presence of an audit committee gives stakeholders comfort that an independent body is ensuring the integrity of the financial statements. Audit committees are intended to protect investors' interests by taking the lead on oversight responsibilities in the areas of internal controls, financial reporting, audit activities, and compliance. They must meet regularly with key internal parties, such as the chief audit executive, to discuss identified fraud risks and the steps taken to prevent fraud.

Responsibilities of the audit committee include, but are not limited to:

- Appointing, compensating, and overseeing external auditors
- Reviewing financial reports
- Overseeing the effectiveness of both design and operation of the company's internal control structure
- Reviewing management's and auditors' reports on internal controls over financial reporting
- Overseeing the company's whistleblower policy and being available to receive tips from potential whistleblowers
- Overseeing the establishment and implementation of the ethical code of conduct
- Evaluating and communicating any possible instances of fraud to the company's legal counsel

To fulfill these responsibilities, it is essential for the audit committee to meet regularly with internal and external auditors. These groups share a common function: assessing and managing fraud risks while maintaining independence from management. During these

meetings, the audit committee must engage in candid and open conversations with the external auditors about any known or suspected fraud.

COMPENSATION COMMITTEE

A compensation committee is responsible for determining the compensation and benefits of directors and executives. To be effective, this committee should be composed of independent, outside directors with human resources experience in compensation. Also, the committee should hire compensation consultants who report directly to and are compensated by the committee itself to ensure independence from management.

NOMINATING COMMITTEE

The nominating committee is responsible for identifying, evaluating, and nominating new directors to the board. It also facilitates the election of the new directors by shareholders. Although management nominates board members as well, an effective nominating committee will take charge in selecting new members to ensure independence.

Responsibilities of the nominating committee include, but are not limited to:

- Reviewing performance of current directors
- Assessing the need for new directors
- Having an objective nominating process for qualified candidates to the board
- Communicating any issues regarding board candidates with shareholders

Management

An organization's management team leads the organization and its employees. Management is responsible for making the day-to-day decisions that affect company performance and, ultimately, shareholder wealth.

The management team is typically led by the chief executive officer (CEO) and the chief financial officer (CFO). There are often other senior executives as well, such as a chief operating officer (COO), chief information officer (CIO), and a chief audit executive (CAE), but these positions differ depending on the organization.

Management's roles pertaining to corporate governance include:

- Establishing strategic goals and operating objectives under the board's oversight
- Directing employees to carry out business activities and managing their performance of those tasks

- Determining the use and allocation of company resources and assets
- Evaluating the organization's successes or failures and recalibrating the strategic approach accordingly
- Holding responsibility for the design and operation of the organization's internal controls
- Setting the true ethical tone of the organization

Shareholders

Shareholders are the owners of corporations; they can be individual investors or institutional investors, such as pension funds, mutual fund groups, investment trusts, or insurance companies. Such parties are primarily concerned with maximizing the return on their investment. To that end, shareholders have a responsibility to be actively involved in the corporate governance process. This can include the following:

- Remaining informed on company operations and performance
- Reading annual reports and other communications from management to the shareholders
- Attending shareholder meetings
- Electing capable individuals to serve as board directors
- Holding the board of directors accountable for proper governance and oversight
- Appointing or ratifying the audit committee's appointment of the organization's independent auditors
- Voting on other significant issues, such as specific changes relating to business operations, the company's corporate governance framework, and the rights and responsibilities of the board of directors and executive managers

The Role of Corporate Governance in Fighting Fraud

Effectively fighting fraud requires dedicated, deliberate focus and consideration, including a formal process for oversight by directors and active participation by other stakeholders. As stated in *Managing the Business Risk of Fraud: A Practical Guide*, a publication jointly released by the IIA, AICPA, and ACFE, "effective governance processes are the foundation of fraud risk management. Lack of effective corporate governance seriously undermines any fraud risk management program."[3]

[3] The Institute of Internal Auditors, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide*, April 28, 2008. www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf.

The importance of active and committed board participation in the fraud risk management process cannot be overstated. Dedicated and observable fraud risk oversight activities by the board not only set the stage for an internal anti-fraud culture, but they also serve to increase confidence among various stakeholders and to enhance the organization's ethical reputation. Such oversight can be delegated to a specific committee, such as the audit committee; however, discussions of the fraud risk management program design, components, and effectiveness should be formally incorporated into the board or committee's agenda to ensure adequate and purposeful attention is given to this risk. The committee charged with fraud risk oversight "should meet frequently enough, for long enough periods, and with sufficient preparation to adequately assess and respond to the risk of fraud, especially management fraud, because such fraud typically involves override of the organization's internal controls."[4]

The crux of fraud prevention rests in the programs, activities, controls, and tone established by management and interpreted and carried out by employees. The board of directors oversees these components and evaluates their holistic effectiveness, and it is up to shareholders to ensure that the board is competent and effectual in exercising this oversight. This interdependence of parties underscores the role of sound corporate governance practices as a necessary groundwork for effective fraud risk management.

Principles of Corporate Governance

Most systems of corporate governance are focused on several core principles or values, which include:

- Accountability
- Transparency
- Fairness
- Responsibility

Accountability

The ownership and reporting structures within an organization set the stage for the involved parties' accountability. In most corporations, the owners (i.e., shareholders) are separate from the decision makers (i.e., management) and overseers (i.e., board of directors). To make sure that the organization operates effectively and efficiently, there must be mechanisms in

[4] Ibid., 12.

place to ensure that management is accountable to the board and that the board is accountable to the shareholders.

Transparency

Transparency in the context of corporate governance generally refers to the clarity, accuracy, completeness, and timeliness of the financial statements and other information provided by management to shareholders. The organization's governance processes must include policies and procedures designed to ensure transparent disclosure of all material matters that the shareholders need to make timely and informed decisions regarding their investment in the company. An independent audit of the financial statements is one such mechanism that helps meet this objective.

Fairness

Sound corporate governance practices ensure that all stakeholders (e.g., shareholders, creditors, employees, management, and others) are treated equitably and given just and appropriate consideration. In a system where the owners of the company are separate from those employing the owners' investments to conduct business operations, there is an inherently lopsided balance of power. Consequently, corporate governance processes work to eliminate any resulting bias toward any party. For example, minority shareholders, including those owning just a single share of stock, must receive the same rights—including equal protection of those rights, and equal remedies for violations of those rights—as majority shareholders, such as institutional investors.

Responsibility

Responsibility, as it pertains to corporate governance, applies both to the duty of internal parties (e.g., employees, managers, directors, and owners) to act in the best interest of the organization and to the duty of the organization as a whole to act in society's best interest. Both of these considerations include acting within legal, regulatory, and ethical bounds. Responsible corporate governance is reflected in the concepts of corporate ethics and corporate citizenship. These ideas have garnered increased attention in recent years, as evidenced by the growing number of investors focused on "socially responsible investing" and by the increasing popularity of mutual funds that specialize in "green" companies.

OECD *Principles of Corporate Governance*

The OECD *Principles of Corporate Governance* is regarded as one of the hallmark sources of guidance for corporate governance practices for organizations throughout the world.

According to the OECD, the Principles "are intended to help policy makers evaluate and improve the legal, regulatory, and institutional framework for corporate governance with a view to support economic efficiency, sustainable growth, and financial stability."[5] Indeed, policy makers in many countries have used these Principles as a basis for legislative and regulatory corporate governance initiatives.

It is important to note that the Principles are nonbinding, as their implementation must be adapted to different legal, economic, and cultural circumstances. This is a key strength of the Principles that makes them a useful tool worldwide, both in developed economies and in emerging markets. Governments and regulators also need to find a balance between rules and regulations and flexibility. By agreeing on the Principles, OECD governments have established a benchmark for high standards of corporate governance. The legislation needed to enforce these standards is the responsibility of individual governments.

The OECD *Principles of Corporate Governance* cover six main areas, which are divided into chapters. The Principles:

- Request that governments have in place an effective legal, regulatory, and institutional framework to support good corporate governance practices (Chapter I).
- Call for a corporate governance framework that protects the exercise of shareholders' rights and supports the equal treatment of all shareholders, including minority and foreign shareholders (Chapter II).
- Address the effect of institutional investors and other intermediaries in stock markets and the resulting corporate governance implications (Chapter III).
- Recognize the importance of the role of stakeholders in corporate governance (Chapter IV).
- Examine the importance of timely, accurate, and transparent disclosure mechanisms (Chapter V).
- Address board structures, responsibilities, and procedures (Chapter VI).

The following are the main provisions of the Principles.[6]

[5] OECD, "Principles of Corporate Governance," 2015. www.oecd.org/corporate/oecdprinciplesofcorporategovernance.htm.

[6] The full text of the OECD *Principles of Corporate Governance* can be viewed at: www.oecd.org/corporate/principles-corporate-governance.htm.

I. Ensuring the Basis for an Effective Corporate Governance Framework

The corporate governance framework should promote transparent and fair markets and the efficient allocation of resources. It should be consistent with the rule of law and support effective supervision and enforcement.

A. The corporate governance framework should be developed with a view to its impact on overall economic performance, market integrity, and the incentives it creates for market participants and the promotion of transparent and well-functioning markets.

B. The legal and regulatory requirements that affect corporate governance practices should be consistent with the rule of law, transparent and enforceable.

C. The division of responsibilities among different authorities should be clearly articulated and designed to serve the public interest.

D. Stock market regulation should support effective corporate governance.

E. Supervisory, regulatory, and enforcement authorities should have the authority, integrity, and resources to fulfill their duties in a professional and objective manner. Moreover, their rulings should be timely, transparent, and fully explained.

F. Cross-border cooperation should be enhanced, including through bilateral and multilateral arrangements for exchange of information.

Effective corporate governance requires a sound legal, regulatory, and institutional framework that market participants can rely on when they establish their private contractual relations. This corporate governance framework typically comprises elements of legislation, regulation, self-regulatory arrangements, voluntary commitments, and business practices that are the result of a country's specific circumstances, history, and tradition. The desirable mix between legislation, regulation, self-regulation, voluntary standards, and business practices in this area will therefore vary from country to country.

The corporate governance framework's legislative and regulatory elements can usefully be complemented by soft law elements based on the "comply or explain" principle, such as corporate governance codes, in order to allow for flexibility and address specificities of individual companies. What works well in one company for one investor or a particular stakeholder may not necessarily be generally applicable to corporations, investors, and stakeholders that operate in another context and under different circumstances. As new experiences accrue and business circumstances change, the different provisions of the corporate governance framework should be reviewed and, when necessary, adjusted.

Countries seeking to implement the Principles should monitor their corporate governance framework, including regulatory and listing requirements and business practices, with the objective of maintaining and strengthening their contribution to market integrity and economic performance. As part of this, it is important to take into account the interactions and complementarities between different elements of the corporate governance framework and its overall ability to promote ethical, responsible, and transparent corporate governance practices. Such analysis should be viewed as an important tool in the process of developing an effective corporate governance framework. To this end, effective and continuous consultation with the public is an essential element. In some jurisdictions, this may need to be complemented by initiatives to inform companies and their stakeholders about the benefits of implementing sound corporate governance practices. Moreover, in developing a corporate governance framework in each jurisdiction, national legislators and regulators should duly consider the need for, and the results from, effective international dialogue and cooperation. If these conditions are met, the corporate governance framework is more likely to avoid over-regulation, support the exercise of entrepreneurship, and limit the risks of damaging conflicts of interest in both the private sector and in public institutions.

II. The Rights and Equitable Treatment of Shareholders and Key Ownership Functions

The corporate governance framework should protect and facilitate the exercise of shareholders' rights and ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights.

A. Basic shareholder rights should include the right to: (1) secure methods of ownership registration; (2) convey or transfer shares; (3) obtain relevant and material information on the corporation on a timely and regular basis; (4) participate and vote in general shareholder meetings; (5) elect and remove members of the board; and (6) share in the profits of the corporation.

B. Shareholders should be sufficiently informed about, and have the right to approve or participate in, decisions concerning fundamental corporate changes such as: (1) amendments to the statutes, or articles of incorporation or similar governing documents of the company; (2) the authorization of additional shares; and (3) extraordinary transactions, including the transfer of all or substantially all assets, that in effect result in the sale of the company.

C. Shareholders should have the opportunity to participate effectively and vote in general shareholder meetings and should be informed of the rules, including voting procedures, that govern general shareholder meetings:

1. *Shareholders should be furnished with sufficient and timely information concerning the date, location and agenda of general meetings, as well as full and timely information regarding the issues to be decided at the meeting.*
2. *Processes and procedures for general shareholder meetings should allow for equitable treatment of all shareholders. Company procedures should not make it unduly difficult or expensive to cast votes.*
3. *Shareholders should have the opportunity to ask questions to the board, including questions relating to the annual external audit, to place items on the agenda of general meetings, and to propose resolutions, subject to reasonable limitations.*
4. *Effective shareholder participation in key corporate governance decisions, such as the nomination and election of board members, should be facilitated. Shareholders should be able to make their views known, including through votes at shareholder meetings, on the remuneration of board members and/or key executives, as applicable. The equity component of compensation schemes for board members and employees should be subject to shareholder approval.*
5. *Shareholders should be able to vote in person or in absentia, and equal effect should be given to votes whether cast in person or in absentia.*
6. *Impediments to cross-border voting should be eliminated.*

D. *Shareholders, including institutional shareholders, should be allowed to consult with each other on issues concerning their basic shareholder rights as defined in the Principles, subject to exceptions to prevent abuse.*

E. *All shareholders of the same series of a class should be treated equally. Capital structures and arrangements that enable certain shareholders to obtain a degree of influence or control disproportionate to their equity ownership should be disclosed.*
   1. *Within any series of a class, all shares should carry the same rights. All investors should be able to obtain information about the rights attached to all series and classes of shares before they purchase them. Any changes in economic or voting rights should be subject to approval by those classes of shares which are negatively affected.*
   2. *The disclosure of capital structures and control arrangements should be required.*

F. *Related-party transactions should be approved and conducted in a manner that ensures proper management of conflicts of interest and protects the interest of the company and its shareholders.*
   1. *Conflicts of interest inherent in related-party transactions should be addressed.*
   2. *Members of the board and key executives should be required to disclose to the board whether they, directly, indirectly or on behalf of third parties, have a material interest in any transaction or matter directly affecting the corporation.*

G. *Minority shareholders should be protected from abusive actions by, or in the interest of, controlling shareholders acting either directly or indirectly, and should have effective means of redress. Abusive self-dealing should be prohibited*

H. Markets for corporate control should be allowed to function in an efficient and transparent manner.

1. *The rules and procedures governing the acquisition of corporate control in the capital markets, extraordinary transactions such as mergers, and sales of substantial portions of corporate assets should be clearly articulated and disclosed so that investors understand their rights and recourse. Transactions should occur at transparent prices and under fair conditions that protect the rights of all shareholders according to their class.*
2. *Anti-take-over devices should not be used to shield management and the board from accountability.*

Equity investors have certain property rights. For example, an equity share in a publicly traded company can be bought, sold, or transferred. An equity share also entitles the investor to participate in the profits of the corporation, with liability limited to the amount of the investment. In addition, ownership of an equity share provides a right to information about the corporation and a right to influence the corporation, primarily by participation in general shareholder meetings and by voting.

As a practical matter, however, the corporation cannot be managed by shareholder referendum. The shareholding body is made up of individuals and institutions whose interests, goals, investment horizons, and capabilities vary. Moreover, the corporation's management must be able to take business decisions rapidly. In light of these realities and the complexity of managing the corporation's affairs in fast-moving and ever-changing markets, shareholders are not expected to assume responsibility for managing corporate activities. The responsibility for corporate strategy and operations is typically placed in the hands of the board and a management team that is selected, motivated, and, when necessary, replaced by the board.

Shareholders' rights to influence the corporation center on certain fundamental issues, such as the election of board members, or other means of influencing the board's composition, amendments to the company's organic documents, approval of extraordinary transactions, and other basic issues as specified in company law and internal company statutes. This Section can be seen as a statement of the most basic rights of shareholders, which are recognized by law in most countries. Additional rights such as the approval or election of auditors, direct nomination of board members, the ability to pledge shares, the approval of distributions of profits, shareholder ability to vote on board member and/or key executive compensation, approval of material related-party transactions, and others have also been established in various jurisdictions.

Investors' confidence that the capital they provide will be protected from misuse or misappropriation by corporate managers, board members, or controlling shareholders is an important factor in the development and proper functioning of capital markets. Corporate boards, managers, and controlling shareholders may have the opportunity to engage in activities that may advance their own interests at the expense of non-controlling shareholders. In providing protection to investors, a distinction can usefully be made between ex-ante and ex-post shareholder rights. *Ex-ante rights* are, for example, pre-emptive rights and qualified majorities for certain decisions. *Ex-post rights* allow the seeking of redress once rights have been violated. In jurisdictions where the enforcement of the legal and regulatory framework is weak, it can be desirable to strengthen the ex-ante rights of shareholders such as by establishing low share ownership thresholds for placing items on the agenda of the shareholders meeting or by requiring a supermajority of shareholders for certain important decisions. The Principles support equal treatment for foreign and domestic shareholders in corporate governance. They do not address government policies to regulate foreign direct investment.

One of the ways in which shareholders can enforce their rights is to be able to initiate legal and administrative proceedings against management and board members. Experience has shown that an important determinant of the degree to which shareholder rights are protected is whether effective methods exist to obtain redress for grievances at a reasonable cost and without excessive delay. The confidence of minority investors is enhanced when the legal system provides mechanisms for minority shareholders to bring lawsuits when they have reasonable grounds to believe that their rights have been violated. The provision of such enforcement mechanisms is a key responsibility of legislators and regulators.

There is some risk that a legal system which enables any investor to challenge corporate activity in the courts can become prone to excessive litigation. Thus, many legal systems have introduced provisions to protect management and board members against litigation abuse in the form of tests for the sufficiency of shareholder complaints, so-called safe harbors for management and board member actions (such as the business judgement rule), as well as safe harbors for the disclosure of information. In the end, a balance must be struck between allowing investors to seek remedies for infringement of ownership rights and avoiding excessive litigation. Many countries have found that alternative adjudication procedures, such as administrative hearings or arbitration procedures organized by the securities regulators or other regulatory bodies, are an efficient method for dispute settlement, at least at the first instance level. Specialized court procedures can also be a

practical instrument to obtain timely injunctions, and ultimately facilitate the rapid settlement of disputes.

III. Institutional Investors, Stock Markets, and Other Intermediaries

The corporate governance framework should provide sound incentives throughout the investment chain and provide for stock markets to function in a way that contributes to good corporate governance.

A. Institutional investors acting in a fiduciary capacity should disclose their corporate governance and voting policies with respect to their investments, including the procedures that they have in place for deciding on the use of their voting rights.

B. Votes should be cast by custodians or nominees in line with the directions of the beneficial owner of the shares.

C. Institutional investors acting in a fiduciary capacity should disclose how they manage material conflicts of interest that may affect the exercise of key ownership rights regarding their investments.

D. The corporate governance framework should require that proxy advisors, analysts, brokers, rating agencies, and others that provide analysis or advice relevant to decisions by investors, disclose and minimize conflicts of interest that might compromise the integrity of their analysis or advice.

E. Insider trading and market manipulation should be prohibited and the applicable rules enforced.

F. For companies that are listed in a jurisdiction other than their jurisdiction of incorporation, the applicable corporate governance laws and regulations should be clearly disclosed. In the case of cross-listings, the criteria and procedure for recognizing the listing requirements of the primary listing should be transparent and documented.

G. Stock markets should provide fair and efficient price discovery as a means to help promote effective corporate governance.

To be effective, the legal and regulatory framework for corporate governance must be developed with a view to the economic reality in which it is to be implemented. In many jurisdictions, the real world of corporate governance and ownership is no longer characterized by a straight and uncompromised relationship between the company's performance and the income of the ultimate beneficiaries of shareholdings. In reality, the investment chain is often long and complex, with numerous intermediaries that stand between the ultimate beneficiary and the company. The presence of intermediaries acting as independent decision makers influences the incentives and the ability to engage in corporate governance.

The share of equity investments held by institutional investors such as mutual funds, pension funds, insurance companies, and hedge funds has increased significantly, and many of their assets are managed by specialized asset managers. The ability and interest of institutional investors and asset managers to engage in corporate governance varies widely. For some, engagement in corporate governance, including the exercise of voting rights, is a natural part of their business model. Others may offer their beneficiaries and clients a business model and investment strategy that does not include or motivate spending resources on active shareholder engagement. If shareholder engagement is not part of the institution's business model and investment strategy, mandatory requirements to engage, for example through voting, may be ineffective and lead to a box-ticking approach.

The Principles recommend that institutional investors disclose their policies with respect to corporate governance. Voting at shareholder meetings is, however, only one channel for shareholder engagement. Direct contact and dialogue with the board and management represent other forms of shareholder engagement that are frequently used. In recent years, some countries have begun to consider adoption of codes on shareholder engagement ("stewardship codes") that institutional investors are invited to sign up to on a voluntary basis.

IV. The Role of Stakeholders in Corporate Governance

The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active cooperation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.

A. The rights of stakeholders that are established by law or through mutual agreements are to be respected.

B. Where stakeholder interests are protected by law, stakeholders should have the opportunity to obtain effective redress for violation of their rights.

C. Mechanisms for employee participation should be permitted to develop.

D. Where stakeholders participate in the corporate governance process, they should have access to relevant, sufficient, and reliable information on a timely and regular basis.

E. Stakeholders, including individual employees and their representative bodies, should be able to freely communicate their concerns about illegal or unethical practices to the board and to the competent public authorities, and their rights should not be compromised for doing this.

F. The corporate governance framework should be complemented by an effective, efficient insolvency framework and by effective enforcement of creditor rights.

A key aspect of corporate governance is concerned with ensuring the flow of external capital to companies both in the form of equity and credit. Corporate governance is also concerned with finding ways to encourage the various stakeholders in the firm to undertake economically optimal levels of investment in firm-specific human and physical capital. The competitiveness and ultimate success of a corporation is the result of teamwork that embodies contributions from a range of different resource providers, including investors, employees, creditors, customers and suppliers, and other stakeholders. Corporations should recognize that the contributions of stakeholders constitute a valuable resource for building competitive and profitable companies. It is, therefore, in the long-term interest of corporations to foster wealth-creating cooperation among stakeholders. The governance framework should recognize the interests of stakeholders and their contribution to the long-term success of the corporation.

V. Disclosure and Transparency

The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company.

A. Disclosure should include, but not be limited to, material information on:

1. *The financial and operating results of the company.*
2. *Company objectives and nonfinancial information.*
3. *Major share ownership, including beneficial owners, and voting rights.*
4. *Remuneration of members of the board and key executives.*
5. *Information about board members, including their qualifications, the selection process, other company directorships, and whether they are regarded as independent by the board.*
6. *Related-party transactions.*
7. *Foreseeable risk factors.*
8. *Issues regarding employees and other stakeholders.*
9. *Governance structures and policies, including the content of any corporate governance code or policy and the process by which it is implemented.*

B. Information should be prepared and disclosed in accordance with high-quality standards of accounting and financial and nonfinancial disclosure.

C. An annual audit should be conducted by an independent, competent, and qualified auditor in accordance with high-quality auditing standards in order to provide an external and objective assurance to the board and shareholders that the financial statements fairly represent the financial position and performance of the company in all material respects.

D. *External auditors should be accountable to the shareholders and owe a duty to the company to exercise due professional care in the conduct of the audit.*
E. *Channels for disseminating information should provide for equal, timely, and cost-efficient access to relevant information by users.*

In most countries, a large amount of information, both mandatory and voluntary, is compiled on publicly traded and large unlisted enterprises, and subsequently disseminated to a broad range of users. Public disclosure is typically required, at a minimum, on an annual basis, though some countries require periodic disclosure on a semi-annual or quarterly basis, or even more frequently in the case of material developments affecting the company. Companies often make voluntary disclosures that go beyond minimum disclosure requirements in response to market demand.

The Principles support timely disclosure of all material developments that arise between regular reports. They also support simultaneous reporting of material or required information to all shareholders in order to ensure their equitable treatment. In maintaining close relations with investors and market participants, companies must be careful not to violate this fundamental principle of equitable treatment.

Disclosure requirements are not expected to place unreasonable administrative or cost burdens on enterprises. Nor are companies expected to disclose information that may endanger their competitive position unless disclosure is necessary to fully inform the investment decision and to avoid misleading the investor. In order to determine what information should be disclosed at a minimum, many countries apply the concept of materiality. *Material information* can be defined as information whose omission or misstatement could influence the economic decisions taken by users of that information. Material information can also be defined as information that a reasonable investor would consider important in making an investment or voting decision.

A strong disclosure regime that promotes real transparency is a pivotal feature of market-based monitoring of companies and is central to shareholders' ability to exercise their ownership rights on an informed basis. Experience shows that disclosure can also be a powerful tool for influencing the behavior of companies and for protecting investors. A strong disclosure regime can help to attract capital and maintain confidence in the capital markets. By contrast, weak disclosure and non-transparent practices can contribute to unethical behavior and to a loss of market integrity at great cost, not just to the company and

its shareholders, but also to the economy as a whole. Shareholders and potential investors require access to regular, reliable, and comparable information in sufficient detail for them to assess the stewardship of management and make informed decisions about the valuation, ownership, and voting of shares. Insufficient or unclear information may hamper the ability of the markets to function, increase the cost of capital, and result in a poor allocation of resources.

Disclosure also helps improve public understanding of the structure and activities of enterprises, corporate policies and performance with respect to environmental and ethical standards, and companies' relationships with the communities in which they operate. The OECD *Guidelines for Multinational Enterprises* may be relevant for multinational enterprises in many jurisdictions.

VI. The Responsibilities of the Board

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders.

A. Board members should act on a fully informed basis, in good faith, with due diligence and care, and in the best interest of the company and the shareholders.

B. Where board decisions may affect different shareholder groups differently, the board should treat all shareholders fairly.

C. The board should apply high ethical standards. It should take into account the interests of stakeholders.

D. The board should fulfil certain key functions, including:

1. *Reviewing and guiding corporate strategy, major plans of action, risk management policies and procedures, annual budgets, and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions, and divestitures.*
2. *Monitoring the effectiveness of the company's governance practices and making changes as needed.*
3. *Selecting, compensating, monitoring, and, when necessary, replacing key executives and overseeing succession planning.*
4. *Aligning key executive and board remuneration with the longer-term interests of the company and its shareholders.*
5. *Ensuring a formal and transparent board nomination and election process.*
6. *Monitoring and managing potential conflicts of interest of management, board members, and shareholders, including misuse of corporate assets and abuse in related-party transactions.*

7. *Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.*
8. *Overseeing the process of disclosure and communications.*

E. *The board should be able to exercise objective independent judgement on corporate affairs.*
   1. *Boards should consider assigning a sufficient number of non-executive board members capable of exercising independent judgement to tasks where there is a potential for conflict of interest. Examples of such key responsibilities are ensuring the integrity of financial and nonfinancial reporting, the review of related-party transactions, nomination of board members and key executives, and board remuneration.*
   2. *Boards should consider setting up specialized committees to support the full board in performing its functions, particularly in respect to audit, and, depending upon the company's size and risk profile, also in respect to risk management and remuneration. When committees of the board are established, their mandate, composition, and working procedures should be well defined and disclosed by the board.*
   3. *Board members should be able to commit themselves effectively to their responsibilities.*
   4. *Boards should regularly carry out evaluations to appraise their performance and assess whether they possess the right mix of background and competences.*

F. *In order to fulfil their responsibilities, board members should have access to accurate, relevant, and timely information.*

G. *When employee representation on the board is mandated, mechanisms should be developed to facilitate access to information and training for employee representatives, so that this representation is exercised effectively and best contributes to the enhancement of board skills, information, and independence.*

Board structures and procedures vary both within and among countries. Some countries have two-tier boards that separate the supervisory function and the management function into different bodies. Such systems typically have a "supervisory board" composed of non-executive board members and a "management board" composed entirely of executives. Other countries have "unitary" boards, which bring together executive and non-executive board members. In some countries there is also an additional statutory body for audit purposes. The Principles are intended to apply to whatever board structure is charged with the functions of governing the enterprise and monitoring management.

Together with guiding corporate strategy, the board is chiefly responsible for monitoring managerial performance and achieving an adequate return for shareholders, while preventing

conflicts of interest and balancing competing demands on the corporation. In order for boards to effectively fulfill their responsibilities, they must be able to exercise objective and independent judgement. Another important board responsibility is to oversee the risk management system and systems designed to ensure that the corporation obeys applicable laws, including tax, competition, labor, environmental, equal opportunity, health, and safety laws. In some countries, companies have found it useful to explicitly articulate the responsibilities that the board assumes and those for which management is accountable.

The board is not only accountable to the company and its shareholders but also has a duty to act in their best interests. In addition, boards are expected to take due regard of, and deal fairly with, other stakeholder interests including those of employees, creditors, customers, suppliers, and local communities. Observance of environmental and social standards is relevant in this context.

Establishing a Corporate Governance Framework

In its *Principles of Corporate Governance*, the OECD states that "there is no single model of good corporate governance."[7] Consequently, corporate governance structure and practices vary widely and should be determined based on the specific needs of each organization.

In developing a corporate governance framework for an organization, directors and management must give consideration to the legal, regulatory, institutional, and ethical environments in which the company operates. Additionally, good corporate governance is fluid—that is, it maintains the ability to find a different course when its current direction runs into barriers, such as changes in the corporate landscape, new regulations or legal requirements, or shifts in organizational strategy.

Even while remaining adaptable, sound corporate governance is based on established best practices. As increased attention has been provided to the need for strong corporate governance, several models have been produced to outline such best practices and to provide guidance for directors, managers, and other stakeholders in establishing sound governance policies and practices for their organizations. Such models generally take a country- or region-specific approach to reflect the differing regulatory, legal, and institutional realities of various operating environments.

[7] OECD *Principles of Corporate Governance* (2015), p. 10.

Corporate Governance Codes and Guidance

Country-Specific Corporate Governance Guidelines

Legislators, regulators, and other bodies in locations around the world have issued corporate governance guidance specific to their jurisdictions. Companies should be familiar with the existing guidance specific to all the regions in which they operate, and those charged with governance should consult the laws and regulations governing their organization. The European Corporate Governance Institute provides a comprehensive index of corporate governance codes by country, which can be extremely helpful in identifying the pertinent governance guidelines. This index is available at the following site: www.ecgi.org/codes/all_codes.php.

The Treadway Commission

The National Commission on Fraudulent Financial Reporting, more commonly referred to as the *Treadway Commission*, was formed in the United States in 1985 with the purpose of defining the auditor's responsibility in preventing and detecting fraud. Five predominant professional accounting organizations at the time—the American Institute of Certified Public Accountants, The Institute of Internal Auditors, the American Accounting Association, Financial Executives International, and the Institute of Management Accountants—established the Treadway Commission to underwrite a study and make recommendations.

In an effort to curb fraudulent financial reporting, the Treadway Commission offered the following four recommendations that, in combination with other measures, are designed to reduce the probability of fraud in financial reports. These recommendations are addressed to the board of directors' audit committee.

- *Mandatory independent audit committee*—The board of directors oversees management's conduct. The Treadway Commission recommended that each board of directors have an audit committee composed of outside directors.
- *Written charter*—The Treadway Commission also suggested that companies develop a written charter setting forth the audit committee's duties and responsibilities. The board of directors should periodically review, modify, and approve this written charter.
- *Resources and authority*—According to the Treadway Commission, the existence of an audit committee and a written charter is not enough. The committee also must have adequate resources and authority to carry out its responsibilities.

- *Informed, vigilant, and effective audit committee members*—The audit committee should be composed of members who are informed, vigilant, and effective.

The spirit of these recommendations has been incorporated into the corporate governance requirements for public companies in many jurisdictions, including the United States; however, these recommendations are foundational best practices for all organizations.

MANAGEMENT'S FRAUD-RELATED RESPONSIBILITIES

While many parties—including the board of directors, internal audit, and external auditors—play an important role in combatting fraud, management is ultimately responsible for the prevention and detection of fraud within an organization. This chapter explores management's specific requirements in carrying out these responsibilities. (Further details regarding the implementation and components of fraud prevention programs are discussed in the "Fraud Prevention Programs" chapter in this section of the *Fraud Examiners Manual*.)

The Legal Foundation for Management's Fraud-Related Responsibilities

Vicarious or Imputed Liability

Corporations and other organizations can be held liable for criminal acts committed as a matter of organizational policy. Fortunately, most organizations do not expressly set out to break the law. The specific legal terms and extent of the organization's liability vary by jurisdiction; however, corporations and other organizations might also be held liable for the criminal acts of their employees if those acts are *done in the course and scope of their employment* and *for the ostensible purpose of benefiting the corporation*. An employee's acts are generally considered to be in the course and scope of employment if the employee has *actual authority* or *apparent authority* to engage in those acts. *Apparent authority* means that a third party would reasonably believe the employee is authorized to perform the act on behalf of the company. Therefore, an organization could be held liable for something an employee does on behalf of the organization even if the employee is not authorized to perform that act.

An organization will not be vicariously liable for the acts of an employee unless the employee acted for the ostensible purpose of benefiting the corporation. This does not mean that the corporation has to receive an actual benefit from the illegal acts of its employee. All that is required is that the employee *intended* to benefit the corporation.

A company cannot seek to avoid vicarious liability for the acts of its employees by simply claiming that it did not know what was going on. Legally speaking, an organization is deemed to have knowledge of all facts known by its officers and employees. That is, if the government can prove that an officer or employee knew of conduct that raised a question as to the company's liability, and the government can show that the company willfully failed to

act to correct the situation, then the company may be held liable even if senior management had no knowledge or suspicion of the wrongdoing.

In addition, the evolving legal principle of *conscious avoidance* allows the government to prove the employer had knowledge of a particular fact, which establishes liability by showing that the employer knew there was a high probability the fact existed and consciously avoided confirming the fact. Employers cannot simply turn a blind eye when there is reason to believe that there might be criminal conduct within the organization. If steps are not taken to deter the activity, the company itself may be found liable.

The corporation can generally be held criminally responsible *even if those in management had no knowledge of or participation in* the underlying criminal events and even if there were specific policies or instructions prohibiting the activity undertaken by the employees. The acts of any employee, from the lowest clerk to the CEO, can impute liability upon a corporation. In fact, in many jurisdictions, a corporation can be criminally responsible for the *collective knowledge* of several of its employees even if no single employee intended to commit an offense.

Management's Responsibility for Internal Controls

It is management's job to ensure that proper internal controls are in place to prevent fraud, as well as to detect it. Although management may not execute all of the controls—as the performance of internal control functions are generally spread across individuals throughout the entire organization, including individual contributors, management, and even the board of directors—management is also responsible for monitoring and remediating internal controls to ensure they are effectively designed and operating to prevent and detect fraud.

COSO *Internal Control—Integrated Framework*

The National Commission on Fraudulent Financial Reporting (commonly known as the Treadway Commission) was established in 1985 with the purpose of defining the responsibility of the auditor in preventing and detecting fraud. The commission was formed and sponsored by five predominant professional auditing organizations at the time—the American Institute of Certified Public Accountants, The Institute of Internal Auditors, the American Accounting Association, Financial Executives International, and the Institute of Management Accountants.

In 1987, the Treadway Commission recommended that the five professional accounting organizations sponsoring the commission work together to provide guidance for organizations' internal controls. The Committee of Sponsoring Organizations (COSO) was formed to actualize the Treadway Commission's recommendation, and, in 1992, COSO issued its *Internal Control—Integrated Framework*. The Framework, which is meant to apply to all entities—public and private, regardless of size— was revisited and amended in 2012, and an updated Framework was released in 2013. The following section provides an overview of the Framework as provided in COSO's Executive Summary.[1]

According to the Framework, "Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance." As noted in this definition, internal controls should be designed to assist management in meeting the following three categories of objectives:

- *Operations objectives*, which pertain to the effectiveness and efficiency of the organization's operations
- *Reporting objectives*, which pertain to the reporting of financial and nonfinancial information to internal and external parties
- *Compliance objectives*, which pertain to the organization's adherence to the laws and the regulations to which it is subject

To meet these objectives, the Framework identifies five interrelated components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Across the five integrated components are seventeen principles that encompass fundamental concepts involved in an effective system of internal control. Consequently, the effectiveness of internal controls can be determined from an assessment of whether (1) each of these five components is in place and functioning effectively and (2) the five components are operating together in an integrated manner.

Control Environment

The *control environment* provides the foundation for the internal control system throughout the entire organization. Established by the directors and senior management, it sets the moral and ethical tone of an organization, which reinforces the importance of internal controls and expected standards of conduct.

[1] Available at http://coso.org/documents/COSO%202013%20ICFR%20Executive_Summary.pdf.

COSO provides five principles supporting the design and implementation of an effective control environment:

1. Personnel at all levels demonstrate a commitment to integrity and ethical values.
2. The board of directors is independent from management and oversees the development and performance of internal control.
3. With board oversight, management establishes the structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of organizational objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

According to the COSO Framework, "Every entity faces a variety of risks from external and internal sources. *Risk* is defined as the possibility that an event will occur and adversely affect the achievement of objectives." *Risk assessment* involves the identification and assessment of the risks the entity faces in achieving its organizational objectives. This process is dynamic and iterative, and it forms the basis for determining how risks will be managed.

According to COSO, the risk assessment involves the following principles:

1. The organization sets sufficiently clear objectives to enable the identification and assessment of risks relating to the objectives.
2. The organization identifies risks to the achievement of its objectives across the entity and analyzes these risks as a basis for determining how the risks should be managed.
3. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
4. The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

Control activities are the policies and procedures that enforce management's directives intended to mitigate risk. These actions are performed at all levels of the organization, at all stages of business processes, and though both manual and automated procedures. They can be designed to prevent the occurrence of risks, detect the occurrence of risks, or both.

The following principles pertain to an organization's control activities:

1. The organization selects and develops control activities that mitigate risks to the achievement of objectives to acceptable levels.
2. The organization selects and develops general control activities over technology to support the achievement of objectives.
3. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

The *information and communication* component relates to the exchange of information in a way that allows employees to carry out their internal control responsibilities and achieve the organization's objectives. According to COSO, the following principles pertain to this component:

1. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
2. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
3. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring

Monitoring is the process that assesses the effectiveness of a control system over time. This component should include both ongoing, automated evaluations and periodic, separate evaluations, the findings of which should be evaluated against pre-defined criteria. The following are the Framework principles supporting this component:

1. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
2. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

More information on the COSO reports and guidance can be found at www.coso.org.

Management's Responsibility for an Effective Corporate Compliance and Ethics Program

The U.S. Congress, in the Comprehensive Crime Control Act of 1984, mandated the uniform sentencing guidelines. The Act also established the United States Sentencing Commission (USSC), which ultimately adopted the Corporate Sentencing Guidelines. The Guidelines provide for the substantial reduction of fines for corporations that have vigorous fraud prevention programs. An effective program to detect and prevent violations of law, within the meaning set out in the Guidelines, is the only action that can be implemented by the corporation prior to the criminal acts that may later mitigate the organization's liability. Such a program, if properly structured and maintained, earns credit for a corporation, which is taken into account at sentencing and reduces the sanctions that are imposed.

Corporations in the U.S. that wish to take advantage of the mitigation provisions of the Guidelines must implement a "corporate compliance program." While the Guidelines obviously do not apply to non-U.S. organizations, many governments and agencies in other countries recommend that corporations use this model for development of their own compliance programs.

Under the Guidelines, if a convicted organization has an effective compliance program in place at the time of the offense, the sentencing judge will consider the organization's acts of due diligence in trying to prevent the illegality when deciding whether to increase or mitigate the sentence. The Guidelines define an *effective compliance program* as one that is reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct. However, the Guidelines also provide that the failure to prevent or detect the offense in question does not necessarily mean that the program is ineffective.

As provided by the Guidelines, to have an "effective compliance and ethics program," the organization shall:

- Exercise due diligence to prevent and detect criminal conduct.
- Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

In designing such a program, certain factors must be considered by each organization:

- *Applicable industry size and practice*—An organization's failure to incorporate and follow industry practice or the standards called for by any applicable government regulation weighs against a finding that the program is effective.

- *Size of the organization*—Large organizations are expected to devote more formal operations and greater resources to meeting the requirements than small organizations. For example, smaller organizations may use available personnel rather than employ separate staff to carry out ethics and compliance.
- *Recurrence of similar misconduct*—The recurrence of a similar event creates doubt as to whether the organization took reasonable steps to meet the requirements.

To meet the two requirements of due diligence and promotion of an ethical culture, the Guidelines set forth the seven factors that are minimally required for such a program to be considered effective:

1. The organization must have established standards and procedures to prevent and detect criminal conduct.
2. Item 2 has three specific subparts:
   a. The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to implementation and effectiveness of the compliance and ethics program.
   b. High-level personnel shall ensure that the organization has an effective compliance and ethics program, and specific individual(s) within the organization shall be assigned overall responsibility for the compliance and ethics program.
   c. Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. These individuals shall report periodically to high-level personnel and, as appropriate, to the governing authority (or a subgroup thereof) on the effectiveness of the program. It is also required that these specific individuals be given adequate resources and authority to accomplish their responsibilities and be given direct access to the governing authority.
3. The organization shall use reasonable efforts not to include within the substantial authority personnel any individual whom the organization knew, or should have known, has engaged in illegal activities or other conducts inconsistent with an effective compliance and ethics program.
4. Item 4 has two subparts:
   a. The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subpart (b) below by conducting

effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

b. The individuals referred to in subpart (a) above are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

5. The organization shall take reasonable steps to accomplish the following:
   a. Ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct.
   b. Evaluate periodically the effectiveness of the organization's compliance and ethics program.
   c. Have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.
6. The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (1) appropriate incentives to perform in accordance with the program and (2) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.
7. After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

The following are some tips and suggestions for developing a compliance and ethics program that complies with these seven requirements.

Establishing Standards

The first step is to establish standards and procedures that are reasonably capable of preventing and detecting criminal conduct. One should start by producing a clear statement of management philosophy. This statement will serve as the backbone of all compliance procedures. This is similar to the COSO requirement that management must set the ethical tone for the organization.

Organizations should draft clear, concise compliance standards that are consistent with management's ethics policy and are relevant to business operations.

Assigning Responsibility

The Guidelines require that the company's governing authority be knowledgeable about the content and operation of the compliance and ethics program and exercise reasonable oversight with respect to the program's implementation and effectiveness. *Governing authority* is defined as the board of directors or, if the organization does not have a board of directors, the organization's highest-level governing body.

It is also required that *high-level personnel* shall ensure that the company has an effective program and that specific individuals within this group be assigned the overall responsibility for the program.

High-level personnel are those who have "substantial control over the organization or who have a substantial role in the making of policy within the organization." Specific examples of high-level personnel include:

- Directors
- Executive officers
- Individuals in charge of major business or functional units of the organization
- Individuals with substantial ownership interests in the organization

Audit Committees

If a board of directors exists, such as in a public company, the board must be knowledgeable about the content and operation of the compliance program and oversee its implementation. Accordingly, it is preferable for the board of directors or one of the board's committees to control the organization's compliance program. For instance, many companies place their compliance programs under the control of audit committees. There are four principal benefits to this practice:

- The involvement of the board of directors lends an air of authority to the compliance program. It clearly identifies the program as a matter of company policy.
- The involvement of a board committee provides oversight to the operation of the program by personnel who are not involved in the program's day-to-day operation.
- Efforts to implement an effective compliance program can be documented in the committee's meeting minutes. This documentation can prove useful if the company ever has to defend its actions and seek mitigation of a criminal fine.

- The involvement of those board members who are on the audit committee will help ensure that the board is knowledgeable about the content and operation of the compliance program.

Although the board and the officers may delegate the day-to-day operational responsibility for the program to other individuals (e.g., a compliance officer and his staff), these individuals must report periodically to the board or other high-level personnel regarding the effectiveness of the program. They must also have sufficient authority to ensure that standards are strictly adhered to, as well as adequate resources to implement and monitor the program.

Due Diligence in Hiring

The USSC guidelines require that the organization "use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program."

Substantial authority personnel is defined as individuals who exercise a substantial measure of discretion in acting on behalf of an organization. The term includes high-level personnel of the organization, individuals who exercise substantial supervisory authority (e.g., a plant manager or a sales manager), and any other individuals who, although not a part of an organization's management, nevertheless exercise substantial discretion when acting within the scope of their authority (e.g., an individual with authority in an organization to negotiate or set price levels or an individual authorized to negotiate or approve significant contracts). Whether an individual falls within this category must be determined on a case-by-case basis.

Like COSO, the USSC guidelines require that organizations hire ethical employees. This requires careful screening of applicants, thorough background checks (where permitted by law), and effective monitoring of the performance of current employees. Although the guidelines only require such screening for "substantial authority personnel," it is recommended that such screening be adopted for all employees.

Communicating the Policy

The corporate compliance policy should be communicated to everyone who can potentially bind a corporation through their own misconduct. This includes the following:

- Board of directors
- Executive officers
- Managers and supervisors
- Low-level employees
- Independent contractors

Note in particular that organizations can be held liable for the acts of independent contractors if the contractor is acting for the benefit of the organization. It is therefore important to distribute copies of the compliance program to contractors as well as employees.

Training Employees

Organizations must conduct "effective training programs." This includes periodically and appropriately communicating the program's compliance requirements and procedures to all employees affected by the program, including upper-level personnel. These programs should be designed to inform employees about the company's stance on corporate compliance. They should also inform employees about what kinds of acts and omissions are prohibited by law and by the organization. The training should be designed to help employees identify and avoid situations that could lead to criminal conduct. Common training techniques include:

- Lectures
- Training films
- Interactive workshops
- Computer-based courses

Employees should be trained to understand the organization's ethical policy. They should also be trained to identify potentially compromising situations and learn how to avoid them. This training should be tailored to the nature of the organization's business, taking into account the external and internal risks that are inherent in that business. Training should also include a review of statutes and regulations that are particularly applicable to the organization.

Training should not be a one-time event. Simply handing out a copy of the company's compliance policy at the beginning of an employee's tenure is insufficient. Organizations should stress compliance by regularly emphasizing their standards to all personnel. For

example, many companies disseminate a copy of their ethics policies every six months along with employee paychecks.

Achieving Compliance

An organization is required to take reasonable measures to ensure program compliance through monitoring, auditing, periodically evaluating the program's effectiveness, and having a publicized reporting system whereby employees and agents may retain anonymity or confidentiality when reporting or seeking guidance regarding actual or potential illegal conduct without fear of retribution. These include such things as proactive fraud detection and hotlines, which are discussed in more detail in the "Fraud Prevention Programs" chapter.

Disciplinary Action

Enforcing a compliance program means adhering to a system of disciplinary actions for rule breakers. Employees must know that if they violate the company's compliance policy, they will be punished. The opportunity to commit fraud is psychologically more acceptable when employees believe fraud normally goes undetected and unprosecuted. New employees should be advised of the compliance program at the time of hire and should sign an annual statement acknowledging their understanding of it. The range of possible punishments for violations of the policy should be spelled out. These may include:

- Reprimand
- Probation
- Suspension
- Reduction in salary
- Demotion
- Reimbursement of losses of damages
- Dismissal
- Referral for criminal prosecution or civil action
- A combination of the above

In addition, the USSC guidelines recommend the discipline of individuals who are responsible for failing to detect offenses.

The primary purpose of any compliance program is to prevent criminal conduct. Additionally, in many jurisdictions, there is also a secondary purpose: to mitigate potential fines for criminal conduct by showing that the organization is dedicated to preventing illegal

activity. If an organization does not enforce its compliance program, it will have little chance of mitigating fines. Therefore, organizations should adhere to well-defined procedures when investigating potential violations and when disciplining individuals for offenses. The organization's efforts should be documented so that it can prove that it made every effort to enforce compliance. For every allegation of an offense, the company should maintain:

- An account of the alleged offense
- A description of the steps taken to investigate the allegation
- A description of the actions taken by the organization in response to the violation

Members of management should promote their organization's compliance and ethics program through appropriate incentives that encourage employees to perform in accordance with the program. Such incentives can include rewards for reporting ethical concerns or misconduct, or rewards for ideas for new or innovative detection and monitoring methods.

Appropriate Responses

After detection of an offense, the organization must take all reasonable steps to appropriately respond to this offense and to prevent further similar offenses—including modifying its program and administering appropriate discipline for the individuals responsible for the offense and those who failed to detect it. When a control failure is identified, changes might be necessary. Both COSO and the USSC guidelines require organizations to identify the weakness in the control system and make modifications to prevent similar failures in the future. The guidelines require that organizations explain the modifications they have made and demonstrate why they will be effective.

Periodic Assessment

Organizations must also periodically assess the risk that criminal conduct will occur and modify its actions and its compliance and ethics program accordingly. In doing so, the organization should assess the following:

- The nature and seriousness of criminal conduct that could occur
- The likelihood that certain criminal conduct might occur because of the nature of the organization's business
- The prior history of the organization, which might indicate the types of criminal conduct that the company should be trying to prevent

Relation of COSO and USSC Corporate Sentencing Guidelines

The USSC guidelines and COSO focus on the development of a stronger control system. The guidelines contain explicit requirements for an effective control program. COSO does not mandate specific actions. It only provides illustrations of what constitutes a strong control system. The seven minimum requirements of the guidelines are covered within the COSO system. The following table summarizes the relation between the components of the two pronouncements.

COMPONENTS	COSO *INTERNAL CONTROL—INTEGRATED FRAMEWORK*	USSC SENTENCING GUIDELINES
Control Environment	• Ethical tone at the top • Organizational structure, including key areas of authority and reporting lines • Policies—both formal and informal—to reward ethical conduct and punish unethical actions • Mechanism and support for employee reporting • HR policies to ensure hiring and promotion of those who demonstrate integrity • Consistent and appropriate discipline	• Code of conduct • Promote a culture that encourages ethical conduct and compliance • Knowledgeable governing authority with reasonable oversight • High-level personnel assigned overall responsibility for the program • Incentives to promote proper conduct and discourage improper conduct • Reporting mechanisms for employees and agents • Prohibit retaliation against those who make good faith reports of suspected violations • Due diligence to avoid delegation of authority to those with criminal tendencies • Consistent and appropriate discipline
Risk Assessment	• Identification and analysis of risks related to operations, financial reporting, and compliance • A strategy to manage risks • Tailoring ethics and compliance programs to the specifics of the organization	• Develop compliance standards and procedures using risk assessment • Periodic assessments of compliance and ethics risk • Incentives to maintain internal controls • Identification of industry-specific compliance risks

Control Activities	• Policies and procedures to help ensure that management's directives are followed • Activities to ensure fraud risks are addressed	• Standards and procedures capable of reducing the prospect of criminal conduct • Determination of modifications needed to prevent future problems
Information and Communication	• Methods used to identify, capture, classify, and report pertinent information in an appropriate format and time frame • Communication of roles and responsibilities pertaining to internal control	• Effective communication of standards and procedures to all employees and other agents • Required participation in compliance and ethics training programs • Compliance and ethics training and communications that are ongoing, updated, and appropriate to each group of employees
Monitoring	• Ongoing assessment of the internal control system • Actions to correct and remediate any deficiencies	• Use of monitoring and auditing systems designed to detect criminal conduct • Periodic evaluation of program effectiveness • After discovering misconduct, take reasonable steps to remedy the harm caused (e.g., provide restitution to victims and self-reporting and cooperation with authorities) • Respond to identified offenses by assessing the compliance program and making necessary modifications to prevent future problems

Document Retention Policies

An organization's management should ensure that the organization has a proper and effective document retention policy (DRP) in place. When establishing a document retention policy, it is imperative that the organization consider all applicable laws and regulations regarding recordkeeping requirements. In many jurisdictions, industries such as health care, banking, and auditing contain trade-specific rules for documenting and retaining records. Furthermore, companies should continuously check for legal updates concerning these requirements. To have a document retention policy that ignores pertinent recordkeeping requirements could lead to statutory violations.

An effective document retention policy requires that a company (1) establish retention protocols before it foresees litigation or official investigation; (2) develop, review, and/or amend a policy for compliance with the applicable laws and regulations; (3) ensure the reasonableness of the policy according to the company's business practices; (4) provide a concise explanation of what is to be destroyed and when; (5) provide adequate protocols for management of electronic documents; and (6) clearly set forth when the policy should be immobilized due to a pending investigation or foreseeable litigation.

Because industries vary significantly in the types of documents produced, received, and distributed, courts often lean toward a subjective "reasonableness" standard in determining whether a particular policy is adequate. Thus, each company must develop a policy that is specifically tailored to its business practices. A company may find it helpful to refer to retention policies of other companies for guidance, but should avoid duplicating such policies. By establishing individual business policies and compartmentalizing low-value and high-value documents, companies can gain quick access to internal documents. A properly planned and executed document retention policy will do little good if individuals within the company are unaware of it. Not only must employees be aware of the policy, they must also understand what is to be destroyed and when.

It is vital that companies include protocols for preserving and destroying electronic documents. Companies should work with their information technology (IT) departments to develop procedures for handling electronic data. Company counsel, executives, and managers should be aware of how electronic data is stored and destroyed. For example, an email deleted by an employee may remain in the company's computer system until an administrator permanently deletes it. Such situations must be recognized and addressed when designing a document retention policy.

What Documents Should Be Kept?

Obviously, one of the first steps must be to identify the types of documents that need to be retained or destroyed. It is important to remember that every organization is different; thus, an organization may require the retention of documents that are not provided for in this text. All types of documents produced by an organization must be initially accounted for. This includes tangible and electronic documents, and is never limited to financial documents. Accounting records, corporate tax records, bank records, employment records, various workplace records (including in-house emails and client correspondence), and legal records must be considered when constructing a DRP for a particular organization.

Other factors to consider in identifying documents include stakeholders' expectations, tax regulations, and internal factors (such as changes in the Board of Directors, Board resolutions, patents, or copyrights).

Records typically generated by a company that reflect or materially relate to professional services must also be identified in the DRP. For example, accounting and auditing firms should mention the retention and destruction of documents that make up client files such as client billing and payment records, correspondence, and time records.

Document Storage

Whether stored on electronic media or in file cabinets, and whether stored in-house or with a document storage company, documents must remain safe (for confidentiality and destruction purposes) and be easily accessible in the event of potential litigation and legal requests for documents.

Document Destruction

An organization must cease destruction of documents when faced with potential litigation or when a legal document request is pending or imminent. Destruction under a valid DRP will be ineffective if documents were not actually destroyed before a potential litigation trigger occurs. Thus, it is imperative that the DRP provides for complete destruction of documents that can be validly destroyed during the proper periods under the policy. Documents should be destroyed by shredding or by some other means that will render them unreadable. Similarly, a protocol for the destruction of electronic data should be in place to ensure that documents to be destroyed are actually destroyed. The deletion of emails or other files on one's computer does not mean that such records are removed from evidence.

DRP Managers

Finally, in order to properly execute a DRP, someone with detailed knowledge of the DRP should be in charge of the policy and should ensure that employees understand and follow it as designed. This individual should be a senior-level employee with the power to enforce the policy. A DRP manager is responsible for:

- Implementing the DRP
- Ensuring that employees understand and follow the DRP's purpose
- Providing oversight on actual retention and destruction of documents
- Ensuring proper storage of documents
- Periodically following up with counsel to ensure proper retention periods are in place

- Suspending the destruction of documents upon foreseeable litigation
- Informing corporate officers, directors, and employees of changes in relation to the DRP

AUDITORS' FRAUD-RELATED RESPONSIBILITIES

Auditors have specific responsibilities with respect to the prevention and detection of fraud. This chapter of the *Fraud Examiners Manual* describes the regulations, professional standards, and best practices guidance that govern auditors in carrying out their anti-fraud responsibilities.

External Audit Standards Related to Fraud

International Standard on Auditing (ISA) 240, *The Auditor's Responsibility Relating to Fraud in an Audit of Financial Statements*[1]

In 2006, the International Auditing and Assurance Standards Board (IAASB) of the International Federation of Accountants (IFAC) redrafted International Standard on Auditing (ISA) 240 under a project to apply certain clarity conventions to all ISAs. ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, requires the auditor to focus on areas where there is a risk of material misstatement due to fraud, including management fraud.

The standard emphasizes the need for the auditor to maintain an attitude of professional skepticism throughout the audit, notwithstanding the auditor's past experience about the honesty and integrity of management and those charged with governance. The standard became effective for audits of financial statements for financial periods beginning on or after December 15, 2009.

Purpose of the Standard

The purpose of ISA 240 is to establish standards and provide guidance on the auditor's responsibility to consider fraud in an audit of financial statements. ISA 240 also expands on how the standards and guidance in ISA 315, *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment*, and ISA 330, *The Auditor's Responses to Assessed Risks*, are to be applied in relation to the risks of material misstatement due to fraud. The standards and guidance in ISA 240 are intended to be integrated into the overall audit process.

[1] The material in this section is compiled from materials and resources issued by the International Auditing and Assurance Standards Board. For more information about this organization, please see www.ifac.org.

Characteristics of Fraud

Misstatements in the financial statements can arise from error or fraud. The distinguishing factor between error and fraud is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional.

Although fraud is a broad legal concept, for the purposes of the ISAs, the auditor is concerned with fraud that causes a material misstatement in the financial statements. Two types of intentional misstatements are relevant to the auditor: misstatements resulting from fraudulent financial reporting and misstatements resulting from misappropriation of assets. Although the auditor may suspect or, in rare cases, identify the occurrence of fraud, the auditor does not make legal determinations of whether fraud has actually occurred.

Fraud, whether fraudulent financial reporting or misappropriation of assets, involves incentive or pressure to commit fraud, a perceived opportunity to do so, and some rationalization of the act. For example:

- Incentive or pressure to commit fraudulent financial reporting may exist when management is under pressure, from sources outside or inside the entity, to achieve an expected (and perhaps unrealistic) earnings target or financial outcome—particularly since the consequences to management for failing to meet financial goals can be significant. Similarly, individuals may have an incentive to misappropriate assets, for example, because the individuals are living beyond their means.
- A perceived opportunity to commit fraud may exist when an individual believes internal control can be overridden, for example, because the individual is in a position of trust or has knowledge of specific deficiencies in internal control.
- Individuals may be able to rationalize committing a fraudulent act. Some individuals possess an attitude, character, or set of ethical values that allow them knowingly and intentionally to commit a dishonest act. However, even otherwise honest individuals can commit fraud in an environment that imposes sufficient pressure on them.

Fraudulent financial reporting involves intentional misstatements including omissions of amounts or disclosures in financial statements to deceive financial statement users. It can be caused by the efforts of management to manage earnings in order to deceive financial statement users by influencing their perceptions as to the entity's performance and profitability. Such earnings management may start out with small actions or inappropriate adjustment of assumptions and changes in judgments by management. Pressures and incentives may lead these actions to increase to the extent that they result in fraudulent

financial reporting. Such a situation could occur when, due to pressures to meet market expectations or a desire to maximize compensation based on performance, management intentionally takes positions that lead to fraudulent financial reporting by materially misstating the financial statements. In some entities, management may be motivated to reduce earnings by a material amount to minimize tax or to inflate earnings to secure bank financing.

Fraudulent financial reporting may be accomplished by the following:

- Manipulation, falsification (including forgery), or alteration of accounting records or supporting documentation from which the financial statements are prepared
- Misrepresentation in, or intentional omission from, the financial statements of events, transactions, or other significant information
- Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure

Fraudulent financial reporting often involves management override of controls that may otherwise appear to be operating effectively. Fraud can be committed by management overriding controls using such techniques as:

- Recording fictitious journal entries, particularly close to the end of an accounting period, to manipulate operating results or achieve other objectives
- Inappropriately adjusting assumptions and changing judgments used to estimate account balances
- Omitting, advancing, or delaying recognition in the financial statements of events and transactions that have occurred during the reporting period
- Concealing, or not disclosing, facts that could affect the amounts recorded in the financial statements
- Engaging in complex transactions that are structured to misrepresent the financial position or financial performance of the entity
- Altering records and terms related to significant and unusual transactions

Misappropriation of assets involves the theft of an entity's assets and is often perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management who are usually more able to disguise or conceal misappropriations in ways that are difficult to detect. Misappropriation of assets can be accomplished in a variety of ways, including:

- Embezzling receipts (for example, misappropriating collections on accounts receivable or diverting receipts in respect of written-off accounts to personal bank accounts)
- Stealing physical assets or intellectual property (for example, stealing inventory for personal use or for sale, stealing scrap for resale, or colluding with a competitor by disclosing technological data in return for payment)
- Causing an entity to pay for goods and services not received (for example, payments to fictitious vendors, kickbacks paid by vendors to the entity's purchasing agents in return for inflating prices, or payments to fictitious employees)
- Using an entity's assets for personal use (for example, using the entity's assets as collateral for a personal loan or a loan to a related party)

Misappropriation of assets is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorization.

Responsibility for the Prevention and Detection of Fraud

The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. Management, with the oversight of those charged with governance, should place a strong emphasis on both fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment.

This involves a commitment to creating a culture of honesty and ethical behavior which can be reinforced by an active oversight by those charged with governance. In exercising oversight responsibility, those charged with governance consider the potential for override of controls or other inappropriate influence over the financial reporting process, such as efforts by management to manage earnings in order to influence the perceptions of analysts and investors as to the entity's performance and profitability.

Responsibilities of the Auditor

An auditor conducting an audit in accordance with ISAs is responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by error or fraud. As described in ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, owing to the inherent limitations of an audit, there is an unavoidable risk that some

material misstatements of the financial statements will not be detected, even though the audit is properly planned and performed in accordance with the ISAs.

The risk of not detecting a material misstatement resulting from fraud is higher than the risk of not detecting one resulting from error. This is because fraud may involve sophisticated and carefully organized schemes designed to conceal it, such as forgery, deliberate failure to record transactions, or intentional misrepresentations being made to the auditor. Such attempts at concealment may be even more difficult to detect when accompanied by collusion, as collusion may cause the auditor to believe that audit evidence is persuasive when it is, in fact, false.

The auditor's ability to detect a fraud depends on factors such as the skillfulness of the perpetrator, the frequency and extent of manipulation, the degree of collusion involved, the relative size of individual amounts manipulated, and the seniority of those individuals involved. While the auditor may be able to identify potential opportunities for fraud to be perpetrated, it is difficult for the auditor to determine whether misstatements in judgment areas such as accounting estimates are caused by fraud or error.

Furthermore, the risk of the auditor not detecting a material misstatement resulting from management fraud is greater than for employee fraud, because management is frequently in a position to directly or indirectly manipulate accounting records, present fraudulent financial information, or override control procedures designed to prevent similar frauds by other employees.

When obtaining reasonable assurance, the auditor is responsible for maintaining an attitude of professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in ISA 240 are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement.

Objectives

The objectives of the auditor, as outlined in ISA 240, are:

- To identify and assess the risks of material misstatement of the financial statements due to fraud;

- To obtain sufficient appropriate audit evidence about the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses; and
- To respond appropriately to identified or suspected fraud.

Definitions

For purposes of the ISAs, the following terms have the meanings attributed below:

- *Fraud*—An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.
- *Fraud risk factors*—Events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud

Professional Skepticism

According to ISA 200, the auditor shall maintain an attitude of professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance.

Unless the auditor has reason to believe the contrary, the auditor may accept records and documents as genuine. If conditions identified during the audit cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, the auditor shall investigate further.

Where responses to inquiries of management or those charged with governance are inconsistent, the auditor shall investigate the inconsistencies.

Discussion Among the Engagement Team

ISA 315 (Redrafted) requires a discussion among the engagement team members and a determination by the engagement partner of which matters are to be communicated to those team members not involved in the discussion.

This discussion shall place particular emphasis on how and where the entity's financial statements may be susceptible to material misstatement due to fraud. Additionally, the discussion should include matters such as:

- How management could perpetrate and conceal fraudulent financial reporting
- How the entity's assets could be misappropriated

- Circumstances that might be indicative of earnings management
- The known external and internal organizational factors that might:
  - Create an incentive or pressure for individuals to commit fraud
  - Provide the opportunity for fraud to be perpetrated
  - Indicate a culture or environment that enables the rationalization of fraud
- Management's involvement in overseeing employees with access to cash or other assets susceptible to misappropriation
- Any unusual or unexplained changes in behavior or lifestyle of management or employees which have come to the attention of the engagement team
- The importance of maintaining a proper state of mind throughout the audit regarding the potential for material misstatement due to fraud
- The types of circumstances that, if encountered, might indicate the possibility of fraud
- How an element of unpredictability will be incorporated into the nature, timing and extent of the audit procedures to be performed
- The audit procedures that might be selected to respond to the susceptibility of the entity's financial statement to material misstatement due to fraud and whether certain types of audit procedures are more effective than others
- Any allegations of fraud that have come to the auditor's attention
- The risk of management override of controls

Additionally, the discussion shall occur with the setting aside of any beliefs that the engagement team members may have that management and those charged with governance are honest and have integrity.

Risk Assessment Procedures and Related Activities

When performing risk assessment procedures and related activities to obtain an understanding of the entity and its environment, including the entity's internal control, required by ISA 315 (Redrafted), the auditor shall perform the following procedures to obtain information for use in identifying the risks of material misstatement due to fraud.

INQUIRIES OF MANAGEMENT AND OTHERS WITHIN THE ENTITY

The auditor shall make inquiries of management regarding:

- Management's assessment of the risk that the financial statements may be materially misstated due to fraud, including the nature, extent, and frequency of such assessments;
- Management's process for identifying and responding to the risks of fraud in the entity, including any specific risks of fraud that management has identified or that have been

brought to its attention, or classes of transactions, account balances, or disclosures for which a risk of fraud is likely to exist;
- Management's communication, if any, to those charged with governance regarding its processes for identifying and responding to the risks of fraud in the entity; and
- Management's communication, if any, to employees regarding its views on business practices and ethical behavior.

The auditor shall make inquiries of management, and others within the entity as appropriate, to determine whether they have knowledge of any actual, suspected, or alleged fraud affecting the entity.

For those entities that have an internal audit function, the auditor shall make inquiries of internal audit to determine whether it has knowledge of any actual, suspected, or alleged fraud affecting the entity, and to obtain its views about the risks of fraud.

INQUIRIES OF THOSE CHARGED WITH GOVERNANCE

Unless all of those charged with governance are involved in managing the entity, the auditor shall obtain an understanding of how those charged with governance exercise oversight of management's processes for identifying and responding to the risks of fraud in the entity and the internal control that management has established to mitigate these risks.

The auditor shall make inquiries of those charged with governance to determine whether they have knowledge of any actual, suspected, or alleged fraud affecting the entity. These inquiries are made in part to corroborate the responses to the inquiries of management.

EVALUATION OF UNUSUAL OR UNEXPECTED RELATIONSHIPS IDENTIFIED

The auditor shall evaluate whether unusual or unexpected relationships that have been identified in performing analytical procedures, including those related to revenue accounts, may indicate risks of material misstatement due to fraud.

CONSIDERATION OF OTHER INFORMATION

The auditor shall consider whether other information obtained by the auditor indicates risks of material misstatement due to fraud.

EVALUATION OF FRAUD RISK FACTORS

The auditor shall evaluate whether the information obtained from the other risk assessment procedures and related activities performed indicates that one or more fraud risk factors are present. While fraud risk factors may not necessarily indicate the existence of fraud, they have often been present in circumstances where frauds have occurred and therefore may indicate risks of material misstatement due to fraud.

The fact that fraud is usually concealed can make it very difficult to detect. Nevertheless, the auditor may identify events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud (fraud risk factors). For example:

- The need to meet expectations of third parties to obtain additional equity financing may create pressure to commit fraud;
- The granting of significant bonuses if unrealistic profit targets are met may create an incentive to commit fraud; and
- A control environment that is not effective may create an opportunity to commit fraud.

Fraud risk factors cannot easily be ranked in order of importance. The significance of fraud risk factors varies widely. Some of these factors will be present in entities where the specific conditions do not present risks of material misstatement. Accordingly, the determination of whether a fraud risk factor is present and whether it is to be considered in assessing the risks of material misstatement of the financial statements due to fraud requires the exercise of professional judgment.

Examples of fraud risk factors related to fraudulent financial reporting and misappropriation of assets are presented in the Appendix to ISA 240 (discussed below). These illustrative risk factors are classified based on the three conditions that are generally present when fraud exists:

- An incentive or pressure to commit fraud;
- A perceived opportunity to commit fraud; and
- An ability to rationalize the fraudulent action.

Risk factors reflective of an attitude that permits rationalization of the fraudulent action may not be susceptible to observation by the auditor. Nevertheless, the auditor may become aware of the existence of such information. Although the fraud risk factors described in the ISA's appendix cover a broad range of situations that may be faced by auditors, they are only examples and other risk factors may exist.

The size, complexity, and ownership characteristics of the entity have a significant influence on the consideration of relevant fraud risk factors. For example, in the case of a large entity, there may be factors that generally constrain improper conduct by management, such as:

- Effective oversight by those charged with governance
- An effective internal audit function
- The existence and enforcement of a written code of conduct

Furthermore, fraud risk factors considered at a business segment operating level may provide different insights when compared with those obtained when considered at an entity-wide level.

Identification and Assessment of the Risks of Material Misstatement Due to Fraud

In accordance with ISA 315 (Redrafted), the auditor shall identify and assess the risks of material misstatement due to fraud at the financial statement level, and at the assertion level for classes of transactions, account balances, and disclosures.

When identifying and assessing the risks of material misstatement due to fraud, the auditor shall, based on a presumption that there are risks of fraud in revenue recognition, evaluate which types of revenue, revenue transactions, or assertions give rise to such risks. Specific documentation is required when the auditor concludes that the presumption is not applicable in the circumstances of the engagement and, accordingly, has not identified revenue recognition as a risk of material misstatement due to fraud.

The auditor shall treat those assessed risks of material misstatement due to fraud as significant risks and accordingly, to the extent not already done so, the auditor shall obtain an understanding of the entity's related controls, including control activities, relevant to such risks.

Responses to the Assessed Risks of Material Misstatement Due to Fraud

OVERALL RESPONSES

In accordance with ISA 330 (Redrafted), the auditor shall determine overall responses to address the assessed risks of material misstatement due to fraud at the financial statement level. In doing so, the auditor shall:

- Assign and supervise personnel, taking account of the knowledge, skill, and ability of the individuals to be given significant engagement responsibilities and the auditor's assessment of the risks of material misstatement due to fraud for the engagement;

- Evaluate whether the selection and application of accounting policies by the entity, particularly those related to subjective measurements and complex transactions, may be indicative of fraudulent financial reporting resulting from management's effort to manage earnings; and
- Incorporate an element of unpredictability in the selection of the nature, timing, and extent of audit procedures.

AUDIT PROCEDURES RESPONSIVE TO ASSESSED RISKS OF MATERIAL MISSTATEMENT DUE TO FRAUD AT THE ASSERTION LEVEL

In accordance with ISA 330 (Redrafted), the auditor shall design and perform further audit procedures whose nature, timing, and extent are responsive to the assessed risks of material misstatement due to fraud at the assertion level.

AUDIT PROCEDURES RESPONSIVE TO RISKS RELATED TO MANAGEMENT OVERRIDE OF CONTROLS

Management is in a unique position to perpetrate fraud because of management's ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Although the level of risk of management override of controls will vary from entity to entity, the risk is nevertheless present in all entities. Due to the unpredictable way in which such override could occur, it is a significant risk of material misstatement due to fraud.

To respond to the risk of management override of controls, the auditor shall design and perform audit procedures to:

- Test the appropriateness of journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements. In designing and performing audit procedures for such tests, the auditor shall:
  - Make inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments;
  - Select journal entries and other adjustments made at the end of a reporting period; and
  - Consider the need to test journal entries and other adjustments throughout the period.

- Review accounting estimates for biases and evaluate whether the circumstances producing the bias, if any, represent a risk of material misstatement due to fraud. In performing this review, the auditor shall:
  - Evaluate whether the judgments and decisions made by management in making the accounting estimates included in the financial statements, even if they are individually reasonable, indicate a possible bias on the part of the entity's management that may represent a risk of material misstatement due to fraud. If so, the auditor shall re-evaluate the accounting estimates taken as a whole; and
  - Perform a retrospective review of management judgments and assumptions related to significant accounting estimates reflected in the financial statements of the prior year.
- For significant transactions that are outside the normal course of business for the entity, or that otherwise appear to be unusual given the auditor's understanding of the entity and its environment and other information obtained during the audit, the auditor shall evaluate whether the business rationale (or the lack thereof) of the transactions suggests that they may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets.

The auditor shall determine whether, in order to respond to the identified risks of management override of controls, the auditor needs to perform other audit procedures in addition to those specifically referred to above.

Evaluation of Audit Evidence

The auditor shall evaluate whether analytical procedures that are performed when forming an overall conclusion as to whether the financial statements as a whole are consistent with the auditor's understanding of the entity and its environment indicate a previously unrecognized risk of material misstatement due to fraud.

When the auditor identifies a misstatement, the auditor shall evaluate whether such a misstatement is indicative of fraud. If there is such an indication, the auditor shall evaluate the implications of the misstatement in relation to other aspects of the audit, particularly the reliability of management representations, recognizing that an instance of fraud is unlikely to be an isolated occurrence.

If the auditor identifies a misstatement, whether material or not, and the auditor has reason to believe that it is or may be the result of fraud and that management (in particular, senior

management) is involved, the auditor shall re-evaluate the assessment of the risks of material misstatement due to fraud and its resulting impact on the nature, timing, and extent of audit procedures to respond to the assessed risks. The auditor shall also consider whether circumstances or conditions indicate possible collusion involving employees, management, or third parties when reconsidering the reliability of evidence previously obtained.

When the auditor confirms that, or is unable to conclude whether, the financial statements are materially misstated as a result of fraud the auditor shall evaluate the implications for the audit.

Auditor Unable to Continue the Engagement

If, as a result of a misstatement resulting from fraud or suspected fraud, the auditor encounters exceptional circumstances that bring into question the auditor's ability to continue performing the audit, the auditor shall:

- Determine the professional and legal responsibilities applicable in the circumstances, including whether there is a requirement for the auditor to report to the person or persons who made the audit appointment or, in some cases, to regulatory authorities;
- Consider whether it is appropriate to withdraw from the engagement, where withdrawal from the engagement is legally permitted; and
- If the auditor withdraws:
  - Discuss with the appropriate level of management and those charged with governance the auditor's withdrawal from the engagement and the reasons for the withdrawal; and
  - Determine whether there is a professional or legal requirement to report to the person or persons who made the audit appointment or, in some cases, to regulatory authorities, the auditor's withdrawal from the engagement and the reasons for the withdrawal.

Management Representations

The auditor shall obtain written representations from management that:

- It acknowledges its responsibility for the design, implementation, and maintenance of internal control to prevent and detect fraud;
- It has disclosed to the auditor the results of its assessment of the risk that the financial statements may be materially misstated as a result of fraud;
- It has disclosed to the auditor its knowledge of fraud or suspected fraud affecting the entity involving:

  - Management;
  - Employees who have significant roles in internal control; or
  - Others where the fraud could have a material effect on the financial statements; and
- It has disclosed to the auditor its knowledge of any allegations of fraud, or suspected fraud, affecting the entity's financial statements communicated by employees, former employees, analysts, regulators, or others.

Communications to Management and with Those Charged with Governance

If the auditor has identified a fraud or has obtained information that indicates that a fraud may exist, the auditor shall communicate these matters on a timely basis to the appropriate level of management in order to inform those with primary responsibility for the prevention and detection of fraud of matters relevant to their responsibilities.

Unless all of those charged with governance are involved in managing the entity, if the auditor has identified or suspects fraud involving management, employees who have significant roles in internal control, or others where the fraud results in a material misstatement in the financial statements, the auditor shall communicate these matters to those charged with governance on a timely basis. If the auditor suspects fraud involving management, the auditor shall communicate these suspicions to those charged with governance and discuss with them the nature, timing and extent of audit procedures necessary to complete the audit.

The auditor shall communicate with those charged with governance any other matters related to fraud that are, in the auditor's judgment, relevant to their responsibilities.

Communications to Regulatory and Enforcement Authorities

If the auditor has identified or suspects a fraud, the auditor shall determine whether there is a responsibility to report the occurrence or suspicion to a party outside the entity. Although the auditor's professional duty to maintain the confidentiality of client information may preclude such reporting, the auditor's legal responsibilities may override the duty of confidentiality in some circumstances.

Documentation

The auditor's documentation of the understanding of the entity and its environment and the assessment of the risks of material misstatement required by ISA 315 (Redrafted) shall include:

- The significant decisions reached during the discussion among the engagement team regarding the susceptibility of the entity's financial statements to material misstatement due to fraud; and
- The identified and assessed risks of material misstatement due to fraud at the financial statement level and at the assertion level.

The auditor's documentation of the responses to the assessed risks of material misstatement required by ISA 330 (Redrafted) shall include:

- The overall responses to the assessed risks of material misstatement due to fraud at the financial statement level and the nature, timing, and extent of audit procedures, and the linkage of those procedures with the assessed risks of material misstatement due to fraud at the assertion level; and
- The results of the audit procedures, including those designed to address the risk of management override of controls.

The auditor shall document communications about fraud made to management, those charged with governance, regulators, and others.

When the auditor has concluded that the presumed risk of material misstatement due to fraud related to revenue recognition is not applicable in the circumstances of the engagement, the auditor shall document the reasons for that conclusion.

Appendix

EXAMPLES OF FRAUD RISK FACTORS

The fraud risk factors identified in the Appendix to ISA 240 are examples of such factors that may be faced by auditors in a broad range of situations. Separately presented are examples relating to the two types of fraud relevant to the auditor's consideration—that is, fraudulent financial reporting and misappropriation of assets. For each of these types of fraud, the risk factors are further classified based on the three conditions generally present when material misstatements due to fraud occur: incentives/pressures, opportunities, and attitudes/rationalizations. Although the risk factors cover a broad range of situations, they are only examples and, accordingly, the auditor may identify additional or different risk factors. Not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size or with different ownership characteristics or circumstances. Also, the order of the examples of risk factors provided is not intended to reflect their relative importance or frequency of occurrence.

RISK FACTORS RELATING TO MISSTATEMENTS ARISING FROM FRAUDULENT FINANCIAL REPORTING

The following are examples of risk factors relating to misstatements arising from fraudulent financial reporting.

INCENTIVES/PRESSURES

- Financial stability or profitability is threatened by economic, industry, or entity operating conditions.
- Excessive pressure exists for management to meet the requirements or expectations of third parties.
- Information available indicates that the personal financial situation of management or those charged with governance is threatened by the entity's financial performance.
- There is excessive pressure on management or operating personnel to meet financial targets established by those charged with governance, including sales or profitability incentive goals.

OPPORTUNITIES

- The nature of the industry or the entity's operations provides opportunities to engage in fraudulent financial reporting.
- The monitoring of management is not effective.
- There is a complex or unstable organizational structure.
- Internal control components are deficient.

ATTITUDES/RATIONALIZATIONS

- Communication, implementation, support, or enforcement of the entity's values or ethical standards by management, or the communication of inappropriate values or ethical standards, that are not effective.
- Nonfinancial management's excessive participation in or preoccupation with the selection of accounting policies or the determination of significant estimates.
- Known history of violations of securities laws or other laws and regulations, or claims against the entity, its senior management, or those charged with governance alleging fraud or violations of laws and regulations.
- Excessive interest by management in maintaining or increasing the entity's stock price or earnings trend.
- The practice by management of committing to analysts, creditors, and other third parties to achieve aggressive or unrealistic forecasts.

- Management failing to remedy known significant deficiencies in internal control on a timely basis.
- An interest by management in employing inappropriate means to minimize reported earnings for tax-motivated reasons.
- Low morale among senior management.
- The owner-manager makes no distinction between personal and business transactions.
- Dispute between shareholders in a closely held entity.
- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality.
- The relationship between management and the current or predecessor auditor is strained.

RISK FACTORS ARISING FROM MISSTATEMENTS ARISING FROM MISAPPROPRIATION OF ASSETS

Risk factors that relate to misstatements arising from misappropriation of assets are also classified according to the three conditions generally present when fraud exists: incentives/pressures, opportunities, and attitudes/rationalization. Some of the risk factors related to misstatements arising from fraudulent financial reporting also may be present when misstatements arising from misappropriation of assets occur. For example, ineffective monitoring of management and other deficiencies in internal control may be present when misstatements due to either fraudulent financial reporting or misappropriation of assets exist. The following are examples of risk factors related to misstatements arising from misappropriation of assets.

INCENTIVES/PRESSURES

- Personal financial obligations may create pressure on management or employees with access to cash or other assets susceptible to theft to misappropriate those assets.
- Adverse relationships between the entity and employees with access to cash or other assets susceptible to theft may motivate those employees to misappropriate those assets.

OPPORTUNITIES

- Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation. For example, opportunities to misappropriate assets increase when large amounts of cash are on hand or processed; inventory items are small in size, of high value, or in high demand; the company holds easily convertible assets, such as

bearer bonds, diamonds, or computer chips; fixed assets are small in size, marketable, or lacking observable identification of ownership.
- Inadequate internal control over assets may increase the susceptibility of misappropriation of those assets.

ATTITUDES/RATIONALIZATIONS

- Disregard for the need for monitoring or reducing risks related to misappropriations of assets.
- Disregard for internal control over misappropriation of assets by overriding existing controls or by failing to take appropriate remedial action on known deficiencies in internal control.
- Behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee.
- Changes in behavior or lifestyle that may indicate assets have been misappropriated.
- Tolerance of petty theft.

International Principles for Auditor Oversight

Auditor oversight—whether through a regulatory body or some other process—is a necessary external check on the quality and integrity of the independent audit process. Some jurisdictions directly regulate the audit profession. In addition, as a result of several large financial scandals, a number of other jurisdictions have or are considering adjusting their approaches in this area. Likewise, the International Federation of Accountants (IFAC), an international industry association that has spearheaded efforts to develop International Standards of Audit (ISAs), promoted the establishment of a Public Interest Oversight Board (PIOB) to add greater public policy input into its workings and thereby improve the quality of IFAC's standards-setting procedures and the standards themselves.

Yet even effective auditor oversight might be insufficient to prevent audit failures that are the result of fraud and the complicity of the auditors themselves. However, effective auditor oversight, combined with strong enforcement measures, might help deter fraud from occurring in the first place or detect it relatively soon after it has occurred.

An additional issue regarding auditor oversight arises in situations where international networks of auditors exist. These networks, which frequently market themselves under a single brand identity, are often composed of elements incorporated and regulated separately in a number of jurisdictions. Network members often share information and resources

amongst each other for some marketing and operational purposes, and they might also have internal quality control reviews on a worldwide basis.

However, the extent of international quality control and policy implementation is often limited because of national laws mandating local control of audit firms, desires of the auditing firms to limit their liability for failures of a member of the network in another jurisdiction, and many other reasons. Efforts to remove these barriers to creating true international audit firms may be necessary. In addition, enhanced cooperation among regulators may be necessary to ensure proper oversight of the entire audit network.

The International Organization of Securities Commissions' Principles for Auditor Oversight[2]

The International Organization of Securities Commissions (IOSCO) is an international association of securities regulators that was created in 1983. The Organization's membership includes more than 120 securities regulators and 80 other securities markets participants, accounting for over 95 percent of the world's capital markets.

The stated objectives of the organization's members are:

- To cooperate in developing, implementing, and promoting adherence to internationally recognized and consistent standards of regulation, oversight, and enforcement in order to protect investors; maintain fair, efficient, and transparent markets; and seek to address systemic risks.
- To enhance investor protection and promote investor confidence in the integrity of securities markets, through strengthened information exchange and cooperation in enforcement against misconduct and in supervision of markets and market intermediaries.
- To exchange information at both global and regional levels on their respective experiences in order to assist the development of markets, strengthen market infrastructure, and implement appropriate regulation.[3]

IOSCO has undertaken considerable work regarding auditor oversight issues. In 2002, the Technical Committee released its *Principles for Auditor Oversight*, which laid out a comprehensive set of objectives that any auditor oversight approach should strive to achieve.

[2] The material in this section is compiled from materials and resources issued by the International Organization of Securities Commissions. For more information about this organization, please see www.iosco.org.

[3] www.iosco.org/about/?subsection=about_iosco

These *Principles for Auditor Oversight* note that auditor oversight should take place at several levels—within the audit firm, by professional associates, and through government regulation. However, the *Principles for Auditor Oversight* state that, within jurisdictions, audit firms should be subject to oversight by some body that acts and is seen to act in the public interest. Further, this auditor oversight body should have in place a regular review process designed to ascertain whether audit firms adhere to quality control policies and procedures that address all significant aspects of auditing. The following is the full text of the Principles as released by IOSCO's Technical Committee[4] :

INTRODUCTION

1. Investor confidence is fundamental to the successful operation of the world's financial markets. That confidence depends on investors having credible and reliable financial information when making decisions about capital allocation.

2. The objectives of securities regulation include the protection of investors; ensuring that markets are fair, efficient, and transparent; and the reduction of systemic risk. In pursuit of these objectives, in the area of reporting to investors, there should be full, timely, and accurate disclosure of financial results and other information that is material to investors' decisions. Full and fair disclosure is essential to investor protection, enhances investor confidence, and promotes market liquidity and efficiency.

3. Independent auditors play a critical role in enhancing the reliability of financial information by attesting as to whether the financial statements prepared by management fairly present the financial position and past performance of the public enterprise in compliance with accepted accounting standards.

4. Effective oversight of the accounting profession and of independent audits is critical to the reliability and integrity of the financial reporting process. The Technical Committee of the IOSCO has developed a list of general principles for oversight of audit firms and auditors that audit financial statements of companies whose securities are publicly traded in the capital markets (hereinafter referred to as "auditors").

5. At the present time, a variety of systems for auditor oversight exist among the IOSCO Technical Committee members. In many cases, these existing systems are undergoing

[4] www.iosco.org/library/pubdocs/pdf/IOSCOPD134.pdf

review as a result of financial reporting failures, weaknesses discovered in self-regulatory structures, changes in public expectations, requirements of new legislation, or for other reasons. One jurisdiction has reported that firm-on-firm peer review under self-regulation failed and that new legislation has directed the creation of an auditor oversight body, independent of the accounting profession, with strengthened powers for rulemaking, inspection and disciplinary authority. A number of other jurisdictions have announced that changes will be made in auditor oversight processes and structures. The Technical Committee believes that there is a growing consensus internationally as to the benefits of an auditor oversight system that is not based exclusively or predominantly on self-regulation.

6. The principles set forth herein are intended to assist securities market regulatory authorities, and other authorities with responsibility for auditor oversight, in developing and enhancing regulatory structures for auditor oversight in the wide range of different legal, business and professional environments that exist in IOSCO member jurisdictions. The Technical Committee encourages IOSCO members to work toward implementing these principles in their own jurisdictions. In jurisdictions in which the securities regulator does not have primary responsibility for auditor oversight, it will nevertheless have an interest in ensuring that the oversight system is consistent with maintaining and enhancing investor confidence in published financial statements.

OVERSIGHT PRINCIPLES

1. Oversight of auditors can occur in several ways, including within audit firms, by professional organizations and public or private sector oversight bodies, and through government oversight. In addition, oversight may be provided by supervisory boards and audit committees representing investors in matters relating to individual companies.

2. Within a jurisdiction, auditors should be subject to oversight by a body that acts and is seen to act in the public interest. While the nature of an auditor oversight body and the process through which it carries out its activities may differ among jurisdictions, IOSCO believes that effective oversight generally includes the following:

I. QUALIFICATIONS AND COMPETENCY

A mechanism should exist to require that auditors to have proper qualifications and competency before being licensed to perform audits and to maintain professional competence. A mechanism also should exist to withdraw authorization to perform

audits of publicly traded companies if proper qualifications and competency are not maintained.

IOSCO believes establishing qualification requirements and requiring maintenance of professional competency should improve the quality of auditing. Moreover, the risk that authorization can be revoked for failure to have or maintain the necessary qualification should be an incentive for compliance and adherence to auditing standards.

II. INDEPENDENCE

A mechanism should exist to require that auditors are independent of the enterprises that they audit, both in fact and in appearance. Effective standards, regular assessments, and regulatory oversight generally increase the likelihood that independence is maintained.

III. OVERSIGHT BODY

A mechanism should exist to provide that a body, acting in the public interest, provides oversight over the quality and implementation of auditing, independence, and ethical standards used in the jurisdiction, as well as audit quality control environments.

IV. OVERSIGHT PROCESS

A mechanism should exist to require auditors to be subject to the discipline of an auditor oversight body that is independent of the audit profession, or, if a professional body acts as the oversight body, is overseen by an independent body. Such an auditor oversight body must operate in the public interest, and have an appropriate membership, an adequate charter of responsibilities and powers, and adequate funding that is not under the control of the auditing profession, to carry out those responsibilities.

An auditor oversight body should establish a process for performing regular reviews of audit procedures and practices of firms that audit the financial statements of listed public companies. This oversight process may be performed in coordination with similar quality control mechanisms that are in place within the audit profession, provided the oversight body maintains control over key issues such as the scope of reviews, access to and retention of audit work papers and other information needed

in reviews, and follow-up of the outcome of reviews. Reviews should be conducted on a recurring basis, and should be designed to determine the extent to which audit firms have and adhere to adequate quality control policies and procedures that address all significant aspects of auditing. Matters to be considered include:

a. Independence, integrity and ethics of auditors
b. Objectivity of audits
c. Selection, training, and supervision of personnel
d. Acceptance, continuation, and termination of audit clients
e. Audit methodology
f. Audit performance, that is, compliance with applicable generally accepted auditing standards
g. Consultation on difficult, contentious or sensitive matters and resolution of differences of opinion during audits
h. Second partner reviews of audits
i. Communications with management, supervisory boards and audit committees of audit clients
j. Communications with bodies charged with oversight over the financial reporting process, for example, on matters such as regulatory inquiries, changes in auditors, or other matters as may be required
k. Provisions for continuing professional education.

An auditor oversight body also should address other matters such as professional competency, rotation of audit personnel, employment of audit personnel by audit clients, consulting and other non-audit services, and other matters as deemed appropriate.

V. REMEDIAL MEASURES

An auditor oversight body should have the authority to stipulate remedial measures for problems detected and to initiate and/or carry out disciplinary proceedings to impose sanctions on auditors and audit firms, as appropriate.

VI. INTERNATIONAL COOPERATION

In relation to companies operating or listing on a cross-border basis, IOSCO members are encouraged to provide each other, whether directly or through coordinating with the auditor oversight body in their jurisdiction, with the fullest assistance permissible in efforts to examine or investigate matters in which improper

auditing may have occurred and on any other matters relating to auditor oversight. Members are also encouraged to explore approaches to enhance cooperation among jurisdictions.

The Public Interest Oversight Board[5]

The Public Interest Oversight Board (PIOB) is the global independent oversight body that seeks to improve the quality and public-interest focus of the international auditing, education, and ethics standards promulgated by the International Federation of Accountants (IFAC). Through its oversight activities, the PIOB works to bring greater transparency and integrity to the global audit profession, thereby contributing to the enhanced quality of international financial reporting.[6]

The PIOB's objective is to increase the confidence of investors and others that the public interest activities of IFAC—including the setting of standards by independent boards operating under the auspices of IFAC—are properly responsive to the public interest. To meet this objective, the PIOB provides independent oversight of IFAC's full standard-setting process to help ensure that the resulting standards meet stakeholder needs and are accountable and transparent.

OVERVIEW

The PIOB was formally established in February 2005 to oversee IFAC's auditing and assurance, ethics, and education standard-setting activities, as well as its Member Body Compliance Program. This last activity is designed to encourage member bodies to adopt international standards and to implement quality assurance and investigation and discipline programs.

The establishment of the PIOB was the result of a collaborative effort by the international financial regulatory community, working with IFAC, to ensure that auditing and assurance, ethics, and educational standards for the accounting profession are set in a transparent manner that reflects the public interest. It was mutually recognized that high quality, transparent standard-setting processes with public and regulatory input, together with

[5] The material in this section is compiled from materials and resources issued by the Public Interest Oversight Board. For more information about this organization, please see www.ipiob.org.
[6] www.ipiob.org/index.php/about-piob

regulatory monitoring and public interest oversight, are necessary to enhance the quality of external audits of entities. For this reason, the PIOB also maintains active liaison with independent audit regulators around the world.

ORGANIZATION

The Public Interest Oversight Board comprises individuals from a number of professions and all branches of regulation. Its ten members were nominated by the International Organization of Securities Commissions, the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors, the World Bank, and the European Commission.

RESPONSIBILITIES

The PIOB oversees IFAC's Public Interest Activity Committees (PIACs) comprising the International Auditing and Assurance Standards Board, International Accounting Education Standards Board, International Ethics Standards Board for Accountants, their respective Consultative Advisory Groups (CAGs), and the Compliance Advisory Panel (CAP). In this capacity, the PIOB:

- Ensures that the processes of standard development under its oversight follow due process and are responsive to the public interest
- Ensures the completeness of the strategies and work plans of the standard setting boards
- Oversees the process of nominations to all PIACs and CAGs under its oversight
- Oversees the CAP

Internal Auditors' Fraud-Related Responsibilities

Internal auditors play a key role in helping organizations prevent and detect fraudulent activity. Because of their proximity to and understanding of the inner workings of the organization, internal auditors are in a unique position to uncover potential unscrupulous acts. In fact, the ACFE's 2014 *Report to the Nations on Occupational Fraud and Abuse* shows that the internal audit function plays a vital role in detecting occupational frauds, accounting for the detection of 14 percent of the 1,483 cases included in the study.

As part of its *International Professional Practices Framework* (IPPF), The Institute of Internal Auditors (IIA) has developed the *International Standards for the Professional Practice of Internal Auditing*. This section includes those IIA standards that pertain to the internal auditor's responsibilities for preventing, detecting, and assessing the risk of fraud within an

organization. More detail on these and all other IIA standards can be found at the IIA's website (www.theiia.org).

Standard 1210—Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

1210.A2

Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

Standard 1220—Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1

Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied
- Adequacy and effectiveness of governance, risk management, and control processes
- Probability of significant errors, fraud, or noncompliance
- Cost of assurance in relation to potential benefits

1220.A3

Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

Standard 2060—Reporting to Senior Management and the Board

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including

fraud risks, governance issues, and other matters needed or requested by senior management and the board.

Standard 2110—Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization
- Ensuring effective organizational performance management and accountability
- Communicating risk and control information to appropriate areas of the organization
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management

2110.A1

The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

Standard 2120—Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

2120.A1

The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives
- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations
- Safeguarding of assets
- Compliance with laws, regulations, and contracts

2120.A2

The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

Standard 2130—Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives
- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations
- Safeguarding of assets
- Compliance with laws, regulations, and contracts

Standard 2210—Engagement Objectives

Objectives must be established for each engagement.

2210.A1

Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2

Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

The IIA's *IPPF—Practice Guide: Internal Auditing and Fraud*

To help auditors comply with their responsibilities pertaining to fraud, the IIA released *IPPF—Practice Guide: Internal Auditing and Fraud* (Practice Guide). Although not mandatory, the guidance included in the practice guide is strongly recommended. Specifically, the practice guide addresses fraud awareness; potential fraud indicators; roles and responsibilities for fraud prevention and detection; the internal auditor's role during audit engagements; fraud risk assessment; fraud prevention and detection; fraud investigation; and forming an opinion on internal controls related to fraud. The practice guide also includes an appendix that lists IPPF Practice Advisories that pertain to fraud. The following is a discussion of selected topics from the practice guide. The complete guide is available from the IIA's website (www.theiia.org).

Internal Audit's Role in Fighting Fraud

Fighting fraud in an organization requires the combined efforts of many different departments, including internal audit. Internal auditors assist in the prevention and detection

of fraud by evaluating the adequacy and effectiveness of internal controls, assisting management in establishing effective fraud prevention measures, proactively auditing for fraud, and investigating suspected fraud. Specifically, the practice guide states that, in conducting audit engagements, the internal auditor should:

- Consider fraud risks in the assessment of internal control design and determination of audit steps to perform.
- Have sufficient knowledge of fraud to identify red flags indicating fraud might have been committed.
- Be alert to opportunities that could allow fraud, such as control deficiencies.
- Evaluate whether management is actively retaining responsibility for oversight of the fraud risk management program, whether timely and sufficient corrective measures have been taken with respect to any noted control deficiencies or weaknesses, and whether the plan for monitoring the program continues to be adequate for the program's ongoing success.
- Evaluate the indicators of fraud and decide whether any further action is necessary or whether an investigation should be recommended.
- Recommend investigation when appropriate.

The role internal audit plays in fraud investigations varies by organization. Internal audit may have primary responsibility for fraud investigations, may serve as a resource for the investigations, or may have no involvement at all in the investigations. For internal auditors who find themselves involved in fraud investigations, the practice guide discusses the investigation process, the role of the internal auditor, conducting the investigation, reporting the investigation, resolution and communication of fraud incidents, and analysis of lessons learned.

The practice guide also emphasizes that internal auditors must exercise professional skepticism—an attitude that includes a questioning mind and a critical assessment of audit evidence—in all audit work. By exercising professional skepticism and focusing on the effectiveness of internal controls, auditors increase the likelihood that they will uncover possible fraudulent activity.

Other Roles and Responsibilities for Fraud Prevention and Detection

Other typical roles and responsibilities for fraud detection and prevention outlined in the practice guide include the following:

- *Board of directors*: The board of directors is responsible for effective and responsible corporate fraud governance and is tasked with overseeing management's actions to manage fraud risks.
- *Audit committee*: The audit committee's role is to evaluate management's identification of fraud risks and the implementation of anti-fraud measures, and to provide the tone at the top that fraud will not be accepted in any form. The audit committee is also responsible for overseeing controls to prevent or detect management fraud.
- *Management*: Management is responsible for overseeing the activities of employees, assessing the vulnerability of the entity to fraud, and establishing and maintaining an effective internal control system at a reasonable cost.
- *Legal counsel*: Legal counsel advises the organization on legal matters pertaining to fraud.
- *External auditors*: External auditors have a responsibility to comply with professional standards and to plan and perform the audit of the organization's financial statements to obtain reasonable assurance about whether the financial statements are free of material misstatements, whether caused by error or fraud. (For more information on the external auditor's responsibilities for fraud, see the previous discussion on "External Audit Standards Related to Fraud.")
- *Loss prevention manager*: The loss prevention manager deals with crimes, disasters, accidents, waste, and other business risks, and usually works closely with internal auditors to identify areas of weak internal controls within the organization.
- *Fraud investigators*: Fraud investigators are responsible for detecting and investigating fraud, as well as recovering assets.
- *Other employees:* All employees have a responsibility to report suspicious activity to a hotline, the internal audit department, or management.

The IIA's *IPPF—Practice Guide: Auditing Anti-Bribery and Anti-Corruption Programs*

As the risks of bribery and corruption have increased in significance and focus for many organizations, internal auditors are increasingly being tasked with auditing the programs designed to combat these risks. The IIA issued *IPPF—Practice Guide: Auditing Anti-Bribery and Anti-Corruption Programs* as a to complement the *Internal Auditing and Fraud* practice guide (discussed above) to fully support internal auditors in their responsibilities pertaining to fraud and corruption. The full text of Auditing Anti-Bribery and Anti-Corruption Programs can be found at www.iia.nl/SiteFiles/Nieuws/PG-Auditing-Anti-bribery-and-Anti-corruption-Programs.pdf. The following discussion summarizes some of the key points

of this guidance pertaining to the internal auditor's responsibilities regarding bribery and corruption.

Internal Audit's Role in Anti-Bribery and Anti-Corruption Programs

The specific role of internal audit in anti-bribery and anti-corruption programs varies across organizations, depending on the relevant governance structure. Nonetheless, internal audit can play a significant role in reinforcing the program, both through identifying the existence of potential and actual incidents and assessing the effectiveness of the program designed to anticipate and address these risks.

Specifically, internal audit can reinforce each of the following program components in the noted ways:

- Tone at the top/governance structure, by:
  - Understanding the attitude and tolerance of management and the board regarding bribery and corruption risks
  - Assessing whether that attitude is sufficiently restrictive
  - Validating that this attitude has been effectively communicated throughout the organization
  - Scrutinizing the governance structure and oversight of the anti-bribery and anti-corruption program
- Bribery and corruption risk assessment, by:
  - Understanding all aspects of the anti-bribery and anti-corruption program before performing risk assessments
  - Evaluating inherent bribery and corruption risks as part of a comprehensive risk assessment
  - Ensuring the audit plan for assessing the anti-bribery and anti-corruption program is based on the results of risk assessment
- Policies and procedures, by testing whether they are:
  - Documented appropriately
  - Approved by management
  - In compliance with applicable laws and regulations
  - Implemented effectively
- Communication and training, by:
  - Sharing information with other functions or parties (e.g., fraud investigation, legal, compliance, external audit, regulators), as appropriate

  - Assisting in communicating and training employees in anti-bribery and anti-corruption policies (to the extent that doing so does not impair their objectivity)
- Monitoring and auditing, by:
  - Ensuring risk assessments, analyses, and communication are effective in supporting management's monitoring role
- Investigations and reports, by:
  - Participating in investigations as appropriate, based on the team's resources, the organization's governance structure, and formal protocols
  - Understanding the cultural and legal landscape of the jurisdictions involved
  - Being familiar with local protocols for investigating and reporting
  - Following the organization's protocol regarding any audit evidence that might indicate bribery or corruption
  - Performing and document adequate audit actions to support any findings, conclusions, or recommendations pertaining to bribery or corruption
  - Seeking legal advice or recommending management seek legal advice regarding any evidence of illegal activity uncovered during an audit
  - Working with appropriate personnel to determine whether an irregularity or illegal act has occurred and gauge its effect
- Enforcement and sanctions, by:
  - Working with management to adhere to a defined process for evaluating cases of bribery or corruption and, if appropriate, implementing sanctions according to a formal policy

International Standards for Government Auditing

The International Organization of Supreme Audit Institutions[7]

The International Organization of Supreme Audit Institutions (INTOSAI) is an autonomous, independent, and non-political organization. It is a non-governmental organization founded in 1953, with special consultative status with the Economic and Social Council (ECOSOC) of the United Nations. INTOSAI currently has 192 full members and five associate members.

[7] The material in this section is compiled from materials and resources issued by the International Organization of Supreme Audit Institutions. For more information about this organization, please see www.intosai.org.

INTOSAI operates as an umbrella organization for the external government audit community and provides an institutionalized framework for supreme audit institutions (SAIs) to promote development and transfer of knowledge, improve government auditing worldwide, and enhance professional capacities, standing, and influence of member SAIs in their respective countries. INTOSAI considers that the exchange of experience among its members, and the findings and insights which result, are a guarantee that government auditing continuously progresses with new developments.[8]

International Standards of Supreme Audit Institutions (ISSAI) Framework

According to INTOSAI, several different documents combine to form the comprehensive ISSAI framework with the following hierarchy:[9]

- The founding principles of the INTOSAI professional framework are found in the *Lima Declaration of Guidelines on Auditing Precepts,* with its comprehensive precepts on auditing in the public sector.
- The *Prerequisites for the Functioning of Supreme Audit Institutions* form the next level of the framework. This portion of the framework includes the *Mexico Declaration of SAI Independence*, the *Guidelines and Good Practices Related to SAI Independence*, and the *Principles of Transparency and Accountability*. The *Code of Ethics* also represents a critical element of this portion of the framework. Its statement of values and principles that guide the daily work of the auditors form the prerequisites for the functioning of supreme audit institutions. One of the principles outlined in the *Code of Ethics* is the auditor's obligation to apply generally accepted auditing standards.
- The *Fundamental Auditing Principles* at the next level contain the postulates and principles for carrying out the audit work. The standards include basic audit principles and standards for public-sector, financial, performance, and compliance audit engagements.
- *Auditing Guidelines*, which is the fourth level, provides practical assistance to SAIs in implementing the Standards in their individual constituents.

Portions of the first three elements of this framework are summarized in the following sections. The complete version of the professional framework can be found at www.issai.org.

[8] www.intosai.org/about-us.html

[9] For more information about the ISSAI framework, please see www.issai.org.

The Lima Declaration: General Precepts for Auditing in the Public Sector

The *Lima Declaration of Guidelines on Auditing Precepts* is the foundation of the INTOSAI professional framework. It contains a comprehensive yet concise list of all goals and issues relating to government auditing.

The main purpose of the *Lima Declaration* is to call for independent government auditing. However, the demands of the *Lima Declaration* are not satisfied by a SAI just achieving independence; this independence is also required to be anchored in the legislation. For this, however, well-functioning institutions of legal security must exist, and these are only to be found in a democracy based on the rule of law. Rule of law and democracy are, therefore, essential premises for really independent government auditing and are the pillars on which the *Lima Declaration* is founded.

International Code of Ethics for Auditors in the Public Sector

The INTOSAI *Code of Ethics* is a comprehensive statement of the values and principles that should guide the daily work of auditors. The independence, powers, and responsibilities of the public sector auditor place high ethical demands on the SAI and the staff they employ or engage for audit work. A code of ethics for auditors in the public sector should consider the ethical requirements of civil servants in general and the particular requirements of auditors, including the auditors' professional obligations.

APPLICABILITY

The INTOSAI *Code of Ethics* is directed at the individual auditor, the head of the SAI, executive officers and all individuals working for or on behalf of the SAI who are involved in audit work. However, the Code should not be interpreted as having any impact on the organizational structure of the SAI.

Due to national differences of culture, language, and legal and social systems, it is the responsibility of each SAI to develop its own code of ethics which best fits its own environment. Preferably these national codes of ethics should clarify the ethical concepts. The INTOSAI *Code of Ethics* is intended to constitute a foundation for the national codes of ethics. Each SAI has the responsibility to ensure that all its auditors acquaint themselves with the values and principles contained in the national code of ethics and act accordingly.

GENERAL PRINCIPLES

The conduct of auditors should be beyond reproach at all times and in all circumstances. Any deficiency in their professional conduct or any improper conduct in their personal life places the integrity of auditors, the SAI that they represent, and the quality and validity of their audit work in an unfavorable light, and may raise doubts about the reliability and competence of the SAI itself. The adoption and application of a code of ethics for auditors in the public sector promotes trust and confidence in the auditors and their work.

It is of fundamental importance that the SAI is looked upon with trust, confidence and credibility. The auditor promotes this by adopting and applying the ethical requirements of the concepts embodied in the key words Integrity, Independence and Objectivity, Confidentiality and Competence.

Fundamental Auditing Principles

The *Fundamental Auditing Principles* contain common pronouncements of the generally recognized professional principles that underpin effective, independent auditing of public-sector organizations. The principles contain a set of standards for general public-sector audits, as well as standards specific to financial, performance, and compliance audits.

The following discussion focuses on those principles that apply to all public-sector audits, irrespective of their form or context. The full text of these principles, as well as the principles that are specific to financial, performance, and compliance audits, can be found at www.issai.org/3-fundamental-auditing-principles.

FUNDAMENTAL PRINCIPLES OF PUBLIC-SECTOR AUDITING

The principles contained in this section are fundamental to the conduct of an audit. Although auditing is a cumulative and iterative process, for the purposes of presentation, the fundamental principles are grouped by principles related to the SAI's organizational requirements, general principles that the auditor should consider prior to commencement and at more than one point during the audit, and principles related to specific steps in the audit process.

ORGANIZATIONAL REQUIREMENTS

Each SAI should establish and maintain procedures for ethics and quality control on an organizational level that will provide it with reasonable assurance that the SAI and its

personnel are complying with professional standards and the applicable ethical, legal, and regulatory requirements.

GENERAL PRINCIPLES

- *Ethics and independence*—Auditors should comply with the relevant ethical requirements and be independent. Ethical principles should be embodied in an auditor's professional behavior. The SAIs should have policies addressing ethical requirements and emphasizing the need for compliance by each auditor. Auditors should remain independent so that their reports will be impartial and be seen as such by the intended users.
- *Professional judgment, due care, and skepticism*—Auditors should maintain appropriate professional behavior by applying professional skepticism, professional judgment, and due care throughout the audit. The auditor's attitude should be characterized by professional skepticism and professional judgment, which are to be applied when forming decisions about the appropriate course of action. Auditors should exercise due care to ensure that their professional behavior is appropriate.
- *Quality control*—Auditors should perform the audit in accordance with professional standards on quality control. An SAI's quality control policies and procedures should comply with professional standards, the aim being to ensure that audits are conducted at a consistently high level. Quality control procedures should cover matters such as the direction, review and supervision of the audit process and the need for consultation in order to reach decisions on difficult or contentious matters.
- *Audit team management and skills*—Auditors should possess or have access to the necessary skills. The individuals in the audit team should collectively possess the knowledge, skills, and expertise necessary to successfully complete the audit. This includes an understanding and practical experience of the type of audit being conducted, familiarity with the applicable standards and legislation, an understanding of the entity's operations, and the ability and experience to exercise professional judgment. Auditors should maintain their professional competence through ongoing professional development.
- *Audit risk*—Auditors should manage the risks of providing a report that is inappropriate in the circumstances of the audit. The *audit risk* is the risk that the audit report may be inappropriate. The auditor performs procedures to reduce or manage the risk of reaching inappropriate conclusions, recognizing that the limitations inherent to all audits mean that an audit can never provide absolute certainty of the condition of the subject matter.
- *Materiality*—Auditors should consider materiality throughout the audit process. Materiality is relevant in all audits. A matter can be judged material if knowledge of it

would be likely to influence the decisions of the intended users. Determining materiality is a matter of professional judgment and depends on the auditor's interpretation of the users' needs. This judgment may relate to an individual item or to a group of items taken together. Materiality is often considered in terms of value, but it also has other quantitative as well as qualitative aspects.

- *Documentation*—Auditors should prepare audit documentation that is sufficiently detailed to provide a clear understanding of the work performed, evidence obtained, and conclusions reached. Audit documentation should include an audit strategy and audit plan. It should record the procedures performed and evidence obtained and support the communicated results of the audit. Documentation should be sufficiently detailed to enable an experienced auditor, with no prior knowledge of the audit, to understand the nature, timing, scope, and results of the procedures performed, the evidence obtained in support of the audit conclusions and recommendations, the reasoning behind all significant matters that required the exercise of professional judgment, and the related conclusions.
- *Communication*—Auditors should establish effective communication throughout the audit process. It is essential that the audited entity be kept informed of all matters relating to the audit. This is key to developing a constructive working relationship. Communication should include obtaining information relevant to the audit and providing management and those charged with governance with timely observations and findings throughout the engagement. The auditor may also have a responsibility to communicate audit-related matters to other stakeholders, such as legislative and oversight bodies.

PRINCIPLES RELATED TO THE AUDIT PROCESS

- Planning an audit:
  - *Auditors should ensure that the terms of the audit have been clearly established.* Audits may be required by statute, requested by a legislative or oversight body, initiated by the SAI, or carried out by simple agreement with the audited entity. In all cases, the auditor, the audited entity's management, those charged with governance, and others, as applicable, should reach a common formal understanding of the terms of the audit and their respective roles and responsibilities.
  - *Auditors should obtain an understanding of the nature of the entity/program to be audited.* This includes understanding the relevant objectives, operations, regulatory environment, internal controls, financial and other systems, and business processes, and researching the potential sources of audit evidence. Knowledge can be obtained from

regular interaction with management, those charged with governance, and other relevant stakeholders.

- *Auditors should conduct a risk assessment or problem analysis and revise this as necessary in response to the audit findings*. The auditor should consider and assess the risk of different types of deficiencies, deviations, or misstatements that may occur in relation to the subject matter. Both general and specific risks should be considered. The auditor should assess management's response to identified risks, including its implementation and design of internal controls to address them. The identification of risks and their impact on the audit should be considered throughout the audit process.
- *Auditors should identify and assess the risks of fraud relevant to the audit objectives*. Auditors should make enquiries and perform procedures to identify and respond to the risks of fraud relevant to the audit objectives. They should maintain an attitude of professional skepticism and be alert to the possibility of fraud throughout the audit process.
- *Auditors should plan their work to ensure that the audit is conducted in an effective and efficient manner*. Planning for a specific audit includes strategic and operational aspects. Strategically, planning should define the audit scope, objectives, and approach. Operationally, planning entails setting a timetable for the audit and defining the nature, timing, and extent of the audit procedures. Audit planning should be responsive to significant changes in circumstances and conditions. It is an iterative process that takes place throughout the audit.

- Conducting an audit:
  - *Auditors should perform audit procedures that provide sufficient appropriate audit evidence to support the audit report*. The auditor's decisions on the nature, timing, and extent of audit procedures will have an impact on the evidence to be obtained. The choice of procedures will depend on the risk assessment or problem analysis. Evidence should be both sufficient in quantity and appropriate in quality (i.e., relevant, valid, and reliable) to persuade a knowledgeable person that the findings are reasonable. The auditor's assessment of the evidence should be objective, fair, and balanced. Preliminary findings should be communicated to and discussed with the audited entity to confirm their validity. The auditor must respect all requirements regarding confidentiality.
  - *Auditors should evaluate the audit evidence and draw conclusions*. After completing the audit procedures, the auditor will review the audit documentation in order to determine whether the subject matter has been sufficiently and appropriately audited. Before

drawing conclusions, the auditor reconsiders the initial assessment of risk and materiality in light of the evidence collected and determines whether additional audit procedures need to be performed. When evaluating the audit evidence and assessing materiality of findings, the auditor should take both quantitative and qualitative factors into consideration. Based on the findings, the auditor should exercise professional judgment to reach a conclusion on the subject matter or subject matter information.

- Reporting and follow-up:
  - *Auditors should prepare a report based on the conclusions reached*. The audit process involves preparing a report to communicate the results of the audit to stakeholders, others responsible for governance, and the general public. The purpose is also to facilitate follow-up and corrective action. Reports should be easy to understand, free from vagueness or ambiguity, and complete. They should be objective and fair, only including information that is supported by sufficient and appropriate audit evidence and ensuring that findings are put into perspective and context. The form and content of a report will depend on the nature of the audit, the intended users, the applicable standards, and legal requirements.

FRAUD PREVENTION PROGRAMS

Fraud prevention requires a system of policies and procedures, which, in their aggregate, minimize the likelihood of fraud occurring while maximizing the possibility of detecting any fraudulent activity that might transpire. The potential of being caught most often persuades likely perpetrators not to commit the fraud. Because of this principle, the existence of a thorough control system is essential to fraud prevention.

Selling Fraud Prevention to Management

Management might be resistant to supporting investment in fraud prevention measures for one of several reasons, including:

- Management's concerns relate to areas other than audit or fraud. Those in charge don't typically understand that fraud is hidden and that losses go undetected. They also might refuse to believe that their own workers are capable of stealing even when studies suggest that one-third of employees might do such a thing.
- Because of the hidden nature of fraud, managers are understandably reluctant to believe in the presence of fraud. And, if one employee is caught committing fraud, management might too often claim that it is an isolated problem and not worth additional consideration. Management must understand that when instances of fraud are detected, it is too late to do anything about them.
- Management sometimes unreasonably feels that bringing up the issue will alienate the work force. This problem can be addressed by reminding management that the rank-and-file workers appreciate working for an honest company. It is also helpful to point out to management what the losses might be.

Many anti-fraud professionals complain that management does not adequately support fraud prevention efforts. There are generally two reasons behind this complaint: Management either believes that fraud is not really a problem in the company, or it believes that even addressing the subject has a negative impact. In either scenario, it is difficult for the auditor to break down management's built-in resistance to dealing with fraud prevention. Some of the following suggestions might be helpful in "selling" fraud prevention to management.

The Impact on the Bottom Line

One of the best ways to sell management on fraud prevention is by showing the impact on the bottom line. Fraud impacts net sales dollar for dollar. For example, if a company nets 20

percent on sales, it must sell five items at regular prices to recover losses (cost plus lost profit) from the theft of one item. Fraud can be very expensive.

The cost/benefit analysis of investing in fraud prevention should be clear. It is much more cost effective to proactively address fraud risks than to suffer preventable fraud and spend valuable resources on detecting, investigating, prosecuting, and cleaning up after it. In other words, stopping fraud before it occurs directly increases the organization's bottom line.

The Impact of Negative Publicity

Many corporate executives are more sensitive to adverse publicity than almost any other issue. Certainly, one way to convince management of the logic of fraud prevention is to point out that negative publicity can have a devastating impact on the bottom line, even in small cases. This negative impact can be eliminated or reduced by a proactive fraud prevention program.

Procedures to Prevent Fraud

The following are examples of procedures and mechanisms that are specifically designed to detect and prevent fraud.

Increasing the Perception of Detection

Most experts agree that it is much easier to prevent fraud than to detect it. To prevent fraud, we should understand something about the potential perpetrator's mindset. Increasing the perception of detection might be the most effective fraud prevention method. Controls, for example, do little good in preventing theft and fraud if those at risk do not know of the presence of possible detection. In the audit profession, this means letting employees, managers, and executives know that auditors are actively seeking out information concerning internal theft. This can be accomplished in several ways, such as through proactive audit policies, employee anti-fraud education, enforcement of mandatory-vacation and job-rotation policies, strong management oversight, and effective reporting programs.

Proactive Audit Procedures

Implementing proactive audit procedures demonstrates management's intention to aggressively seek out possible fraudulent conduct instead of waiting for instances to come to management's attention. Such techniques include the use of analytical review, fraud assessment questioning, and surprise audits where possible.

Use of Analytical Review Procedures

Some internal fraud is discovered as a result of analytical review procedures performed during a financial statement audit. To uncover fraud using such techniques, however, the scheme must materially impact the financial statements. Auditors should be especially mindful of the following trends:

- Increasing expenses
- Increasing cost of sales
- Increasing receivables/decreasing cash
- Increasing inventories
- Increasing sales/decreasing cash
- Increasing returns and allowances
- Increasing sales discounts

Fraud Assessment Questioning

Fraud assessment questioning is a nonaccusatory interview technique used as a part of a normal audit. It operates on the theory that employees' attitudes are a good indicator of potential problems, and that one of the most effective ways to assess potential fraud is to ask about it.

Below are some suggested questions that can be asked as part of the normal audit. Note that the questions here begin with the general and proceed to the specific.

- Part of my duty as an auditor is to find fraud, waste, and abuse. Do you understand that?
- Do you think fraud is a problem for business in general?
- Do you think this company has any particular problem with fraud?
- Has anyone ever asked you to do anything that you felt was illegal or unethical?
- If you felt that there was a problem in the company with respect to fraud, what would you do?
- Do you have any indication that there is fraud occurring in the company now?

(See the Investigation section of the *Fraud Examiners Manual* for further details on fraud assessment questioning.)

Surprise Audits Where Possible

In addition to regularly scheduled fraud audits, surprise fraud audits of business functions in which fraud is most likely to occur can be effective both in increasing employees' perception of detection and in uncovering actual frauds that have been perpetrated. The surprise

element must be present for this control to be effective; predictability allows perpetrators the time to conceal their acts by altering, destroying, or misplacing records and other evidence.

Employee Anti-Fraud Education

Each entity should have a policy for educating managers, executives, and employees about fraud. This education can be accomplished through memoranda, organization-wide emails and voice mails, formal training programs, and other intercompany communication methods. Any education efforts should be positive and nonaccusatory. The goal is to make others within the company your eyes and ears.

Who Should Attend?

Every employee within the organization should be required to participate in the fraud awareness training program. No individuals—regardless of their position within the organization—should be provided an exemption from receiving an initial orientation and ongoing anti-fraud education.

FRAUD AWARENESS TRAINING FOR MANAGERS AND EXECUTIVES

In addition to the information presented to all employees, managers and executives should receive special training that addresses the added fraud prevention and detection responsibility—and ability—provided by their authority positions. For example, department managers should be trained in the specific warning signs and prevention/detection methods pertinent to their department's functions. Purchasing managers should be well versed in the red flags of bribery schemes; likewise, controllers should understand just how important their vigilance is in preventing and detecting fraudulent disbursements.

Frequency and Length of Fraud Awareness Training

Like any educational efforts, frequent exposure to anti-fraud topics is the key to ensuring employees absorb—and apply—the information provided. Formal fraud awareness training should be an ongoing process that begins at the time of hire. Employees should also participate in refresher training at least annually to help keep the program alive and engrained in their minds. Additionally, all employees should sign an annual statement acknowledging their understanding of and commitment to the program.

Training Delivery Methods

Formal anti-fraud training can take many forms, including live, in-class instruction; recorded video or animated courses; or interactive self-study programs. Of these options, a live class is

preferable, as it allows employees the opportunity to actively participate, interact with other employees, discuss the true fraud risks facing the organization, and seek and provide feedback regarding the anti-fraud program as a whole. Integrating games and role-playing exercises into the training curriculum can make the course more enjoyable—and thus more effective—for participants.

Perhaps most important, however, is that the training be based on the realities of the organization, rather than on generic anti-fraud messages. While providing general information is good and necessary, doing so without addressing the company's specific concerns or providing employees with practical knowledge and ideas on how to apply it will render the training program ineffective.

In addition, the organization can use other informal means to reinforce its anti-fraud stance on a more constant basis. Periodic newsletters, posters in break rooms, and other casual reminders help keep fraud prevention and detection in the front of employees' minds.

CASCADING TRAINING

As messages from an employee's direct supervisor often carry the most weight with an employee, the concept of cascading training can be an especially effective means of anti-fraud education. In cascading training, managers are tasked with and specifically educated on how to provide anti-fraud training to their own staff. This allows training to be customized to each team's own needs, as well as for the message to come directly from the team's own leader.

Topics to Cover

The following topics should form the basis of the training, but the information presented should focus on the specific risks faced by the organization to provide employees with practical, implementable knowledge.

WHAT FRAUD IS AND WHAT IT IS NOT

A good anti-fraud training program informs employees of what behavior is acceptable and what is not. Providing employees with the legal definition of fraud is not enough; effective training includes an interactive discussion and examples of fraud, as well as examples of errors and abuse.

HOW FRAUD HURTS THE ORGANIZATION

Surprisingly, some employees view the theft of a few thousand dollars from a big organization as having a negligible impact on the company as a whole. Others might believe that fudging numbers in the accounting records to help the company reach its goals is actually a helpful act.

Fraud awareness training programs must make clear to employees how such actions harm the organization—how all frauds result in lost resources; decreased productivity; lowered morale; investments of time and money into investigation, punishment, and remediation; and a hit to the company's reputation.

HOW FRAUD HURTS EMPLOYEES

Employees must also be made aware of how a fraud perpetrated by another individual can negatively affect them personally through decreased salaries, loss of bonuses, possible layoffs, increased scrutiny, decreased trust throughout the organization, and the need to clean up after any mess created. Personalizing the fallout in this way helps increase employees' commitment to aiding fraud prevention and detection efforts.

WHO PERPETRATES FRAUD

Anyone who has the combination of sufficient pressure, adequate opportunity, and an ability to rationalize a dishonest act is at risk of committing fraud. Fraudsters come in all age groups, income levels, and from both genders. Further, ACFE research shows that the typical fraudster is college educated and does not have a criminal history. Anti-fraud training should work to dispel any preconceived notions held by employees regarding what a fraud perpetrator looks like and should help employees learn to focus on identifying the warning signs of fraudulent behavior.

HOW TO IDENTIFY FRAUD

Instructing employees that they must help the organization fight fraud does little good without some accompanying information about what to look for. The following are some warning signs of fraud that employees should be aware of.

FINANCIAL/TRANSACTIONAL RED FLAGS

- Structural red flags
- Personnel red flags
- Operational red flags

- Accounting system red flags
- Financial performance red flags
- Professional service red flags

BEHAVIORAL RED FLAGS

- Living beyond their means
- Financial difficulties
- Control issues, unwilling to share duties
- Unusually close relationship with vendor/customer
- Wheeler-dealer attitude
- Divorce/family problems
- Irritability, suspiciousness, defensiveness
- Addiction problems
- Unwilling to take vacation days
- Past employment-related problems
- Complained about inadequate pay
- Excessive pressure from within the organization
- Past legal problems
- Instability in life circumstances
- Excessive family/peer pressure for success
- Complained about lack of authority

HOW TO REPORT FRAUD

As previously discussed, more fraud is uncovered by tips than by any other means, making employees the best possible fraud detection control. But for employees to be able to serve this function, they must be well informed on how to report any suspicious activity, as well as empowered to make such reports without risk of retribution.

THE PUNISHMENT FOR DISHONEST ACTS

The opportunity to commit fraud becomes more attractive when employees believe fraud normally goes undetected and unprosecuted. Consequently, the punishment (termination and possible prosecution) should be spelled out explicitly to all employees in advance. Providing examples of past transgressions that have gone punished can reinforce the stance that such acts will be addressed with certainty, swiftness, and severity.

Enforcement of Mandatory Vacations

Many internal frauds require manual intervention and are discovered when the perpetrator is away on vacation. The enforcement of mandatory vacations will aid in the prevention of some frauds.

Job Rotation Policy

Some frauds are detected when the perpetrator is sick or unexpectedly absent because they require continuous, manual intervention. Requiring employees in certain functions (e.g., accounting clerks) to periodically rotate job duties or accounts reviewed can increase the perception of detection in the potential perpetrator's mind.

EXAMPLE

A manager who embezzled $1.6 million from his company said, "If the company had coupled a two-week vacation with four weeks of rotation to another job function, my embezzlement would have been impossible to cover up." His fraud lasted three years.

Effective Management Oversight

It is common for employees who steal to use the proceeds for lifestyle improvements. Some examples include more expensive cars, extravagant vacations, expensive clothing, new or remodeled homes, expensive recreational property, and outside investments. Managers should be educated to be observant of these signs. To further increase the deterrent effect, employees should know that supervisors are watching for unexplained or suspicious anomalies of this nature.

EXAMPLE

Discovery of a $97,000 embezzlement, which occurred over a two-year period, resulted when an observant manager asked the internal auditors to examine the responsibilities of a seven-year veteran of the company. The manager noticed that this female employee had begun wearing designer clothes (and making a big deal about it), and was driving a new BMW. The manager was also aware of the fact that this employee had no outside income that might explain the upgrade in lifestyle.

Reporting Programs

An anonymous reporting channel, such as an ethics hotline, is an integral part of an anti-fraud control system. Employees must be made aware of the existence of the reporting mechanism, taught how to use it, and be able to trust that they can report suspicious activity

anonymously or confidentially (where permitted by law) without fear of reprisal. In addition, it should be made clear to employees that reports of suspicious activity will be promptly and thoroughly evaluated.

In educating employees about the reporting program, it should be specifically emphasized that:

- Fraud, waste, and abuse occur in nearly all companies.
- Such conduct costs the company jobs and profits.
- The company actively encourages any employee with information to come forward.
- The employee can come forward and provide information anonymously and without fear of retaliation for good-faith reporting.
- There is an exact method for reporting an incident (e.g., a telephone number or online form).
- The report need not be made to one's immediate superiors.

Hotlines

Hotlines have proved to be a very effective reporting mechanism. However, most hotline reports do not result in fraud cases. With careful screening of calls and proper handling, spurious complaints can be effectively weeded out. There are three general types of hotlines. The advantages and disadvantages of each are summarized below.

PART TIME, IN-HOUSE

These hotlines are assigned to an employee with other duties. An audit or security department usually staffs an in-house hotline. When the employee is out, a recorder takes calls. The main advantage is cost. The main disadvantage is that the hotline is not staffed full-time, which can discourage calls. Also, some people might be reluctant to report their concerns directly to the company.

FULL TIME, IN-HOUSE

A full-time, in-house hotline might be feasible depending on the company size. The advantage is that people can make reports at any time, day or night, and talk to a person. The disadvantage is cost and, like the part-time line, some people might be reluctant to report directly to the company.

THIRD PARTY

An outside company that specializes in services of this type most often staffs a third-party hotline. The advantages are cost, efficiency, and anonymity. Some are staffed around the clock and will provide the information immediately to the client subscriber. They also provide anonymity to those who might be more comfortable with it. Their disadvantage is that the operation is beyond the company's control.

Rewards

A reward, such as a cash payment, can provide an incentive for employees to report wrongdoing. Strict criteria should exist for the payment of rewards, and any proposed policies should be reviewed and approved by legal counsel. Although the amount of rewards paid by companies varies from fixed fees to a percentage of the recovery, studies have generally indicated that rewards should not exceed a few thousand dollars.

In addition to or instead of cash payments, employees who provide information on wrongdoing can be rewarded with public recognition (if they wish), lunch with the CEO, or some other non-monetary incentive that focuses on the qualitative value of reporting and highlights management's support of and encouragement for individuals to come forward with tips.

Tone at the Top

A key part of a fraud prevention program is the express commitment of the board and senior management. This commitment forms the basis of the organization's anti-fraud culture. A strong corporate culture can most often be observed by its outcome, rather than by any individual component. Fostering a culture of ethics and compliance runs deeper than simply implementing a checklist of initiatives; similarly, a culture of corruption can exist even in companies with seemingly sound policies in place. However, organizations that cultivate ethical corporate cultures frequently have one thing in common: a strong "tone at the top."

To achieve an organizational culture with a strong value system founded on integrity, management must show employees through its words and actions that dishonest or unethical behavior will not be tolerated. Management must also create an environment in which employees feel safe to challenge management's decisions or speak up if they think something is wrong. Having a general culture where people feel heard when they have concerns can reduce the risk of fraud significantly because employees often feel more loyal

to their superiors. Such a culture also might help to prevent unethical behavior because issues of anger or stress are dealt with before they escalate to the point of a fraud.

Additionally, management must exude ethics in order to model the behavior that is expected of the staff. When management believes and acts as though it is "above the law" with respect to company policies, staff members are much less likely to follow rules. Staff members frequently resent management for expecting them to behave in a certain way when members of management do not need to behave in the same way themselves. However, when management acts ethically and follows organizational policies, the staff tends to respect and appreciate the behavior and copy it.

Organizational Structure

A well-designed organizational structure—with key areas of authority and clear and proper lines of reporting—can be an effective fraud prevention measure. A confused structure, in contrast, makes it easier for a fraudster to perpetrate and conceal his misdeeds. Establishing and communicating the proper flow of information to everyone in the organization is an essential component of a well-designed organizational structure. Flowcharts displaying organizational and departmental hierarchies can be a helpful tool for this purpose. To ensure that information is being properly received and that instructions are being carried out, such checks must be established.

Background Checks

One of the most basic steps in preventing employee fraud is not to hire employees who have previously stolen. Before hiring anyone, management should conduct a background check (where and to the extent permitted by law) to find out as much as possible about the employee's previous experience with employers and law enforcement. Each company must decide whether the time and expense of such background checks is worth the return. It is always a good practice, but, at a minimum, employers should check the background of any employee who will have constant access to cash, checks, credit card numbers, or any other items that are easily stolen.

Background checks should also be run on existing employees who are being promoted or moved to positions that include access to sensitive or valuable company resources. Even if such a check was performed on the employee at the time of hire, an updated background check should be run to identify any significant changes or occurrences that have taken place during the individual's tenure.

In assessing individuals for hire or promotion, employers should conduct as many of the following background checks as possible and as legally permissible.

Past Employment Verification

Even though most employers will only verify position and dates of employment, you can usually tell by their tone of voice what they think of the employee. Also, ask the previous employers whether the applicant is eligible for rehire.

Criminal Conviction Checks

Many public records services have criminal conviction records. Criminal conviction information can also be obtained by searching the criminal conviction records in the jurisdictions in which the employee has resided.

Drug Screening

Many companies are now conducting drug screenings for potential hires, as well as current employees.

Reference Checks

Amazingly, very few employers actually call the references a candidate provides. Most operate under the theory that someone wouldn't provide a bad reference. However, some job applicants will list important-sounding individuals as references with the hope that the hiring organization won't call. In addition, people often just assume, incorrectly, that a former supervisor or coworker will provide a good reference. But obtaining negative information from someone the candidate listed as a recommendation can be very telling and should serve as a serious warning sign to the hiring organization.

Education and Certification Verification

It is always a good idea to verify a person's education. Also, if the person claims he has a license or other certification, call the issuing organization to verify it. It is not that unusual for someone to claim a certification or license that has actually been revoked due to a disciplinary action. Most licensing or certification organizations, including the Association of Certified Fraud Examiners, will tell you if any disciplinary action has been taken against a particular member.

Performance Management and Measurement

In addition to hiring qualified, ethical employees, it is important to place employees in situations where they are able to thrive without resorting to unethical conduct. Organizations should provide employees with well-defined job descriptions and performance goals. Performance goals should be routinely reviewed to ensure that they do not set unrealistic standards.

Training should be provided on a consistent basis to ensure that employees maintain the skills needed to perform their tasks effectively. Regular ethics training will help employees identify potential trouble spots and avoid getting in compromising situations. Management should also quickly determine where deficiencies in an employee's conduct exist and work with the employee to fix the problem.

Additionally, there is a fine line between performance goals that motivate employees to challenge themselves and those that are so ambitious that the only way employees can meet them is to perpetrate fraud. When employee compensation, including bonuses, or job security is tied to unachievable performance goals, employees have the incentive to mastermind creative (read: fraudulent) approaches to meeting them.

Moreover, including ethics-based metrics—those that focus on how employees do business, not just how much business they do—as a component of performance goals and evaluation can be an especially effective way to foster ethical behavior and reinforce the importance of ethics as the guiding factor in making business decisions.

Handling of Known Fraud Incidents

The way that management handles incidents of fraud within the organization plays an important role in its fraud prevention program. Specifically, it must be made clear to all employees that the company maintains a policy of zero tolerance for fraud; otherwise, once an employee learns that small frauds are possible, larger frauds might be committed shortly thereafter. In addition, by not consistently punishing perpetrators, a company renders its fraud prevention program less effective, if not useless. Having a public record of the incident can also be important, so reporting known incidents of fraud to law enforcement can be an effective step in making the organization's zero-tolerance stance clear.

Minimizing Employee Pressures

While most internal controls are designed to reduce the opportunity to commit and conceal fraud, organizations should also be mindful of the pressures, such as financial hardships or family problems, that can lead to fraud. Unfortunately, such pressures can be difficult to detect in employees. However, companies should take steps to increase managers' awareness of such potential problems, as well as to assist an employee who might be having difficult times.

Open-Door Policies

An open-door policy that allows employees to speak freely about pressures can provide management with the opportunity to alleviate such pressures before they become acute, which will help prevent fraud. If employees and others know they can speak freely to their supervisors, they might be more willing to discuss the personal and professional issues that could lead to illicit actions if not dealt with properly. Additionally, managers will have more opportunities to understand the pressures faced by employees and might be able to assist them in addressing those issues.

EXAMPLE

The controller of a small fruit-packing company in California stole $112,000 from the company. When asked why, he said, "Nobody at the company ever talked to me, especially the owners. They were unfair. They talked down to me, and they were rude. They deserve everything they got."

Fair Personnel Policies and Procedures

It is not uncommon for employees who feel that they have been treated unfairly in some way to want to right a perceived injustice. To some disgruntled employees, getting even translates to committing fraud. For example, an employee who receives a pay cut might view walking off with company assets as a way to even the score. Or an employee who feels underappreciated by his employer might get revenge by disclosing classified company information to a competitor in an effort to sabotage the organization.

Efforts of human resources managers to assess and maintain morale at a high level are an important preventive control. Human resource managers can monitor employee morale through observation, anonymous employee surveys, an open-door policy, and other means.

Further, ensuring that personnel policies and procedures are fair and equitably applied can boost morale and thereby reduce fraud risk. Other measures employers can take to boost morale include providing the following:

- Proper management training
- Career development opportunities
- Special events for employees
- Recognition of employees for a job well done

Employee Support Programs

Many progressive companies and agencies have realized the benefit of employee support programs. Some kinds of support programs include alcohol and drug assistance, as well as counseling for gambling, family and marital problems, and financial difficulties. In addition to addressing the direct pressures that might contribute to an individual resorting to fraud, making such programs available to employees who are facing personal problems shows employees that management cares for their well-being, which can reduce the employee's ability to rationalize a dishonest act.

Fraud Prevention Policy

Another important element of an overall fraud prevention program is a written fraud policy that specifically spells out who in an organization handles varying fraud matters under differing circumstances. Instituting a separate, formal anti-fraud policy sends a strong message to employees about the organization's intolerance for employee fraud.

Writing the Fraud Policy

Companies often have an ethics policy that sets forth in detail what is expected in the ethical climate of the company. Other companies have a fraud policy that specifically spells out who handles fraud matters under what circumstances. The components of a fraud policy will differ from company to company. Many fraud policies have some of the following elements.

Policy Statement

The policy statement sets forth that management is responsible for fraud, and each member of the management team should be familiar with the types of signals present within his scope of responsibilities. The policy statement also designates who is in charge of investigating suspected irregularities.

Scope of Policy

This area of the fraud policy statement covers what constitutes an irregularity and the fact that the policy covers everyone, from management to workers.

Actions Constituting Fraud

This area sets forth in detail what actions constitute fraudulent conduct. This is important, as it gives management the legal grounds to investigate and punish violators. The actions listed can include:

- Any dishonest or fraudulent act
- Forgery or alteration of documents
- Misapplication of funds or assets
- Impropriety with respect to reporting financial transactions
- Profiting on insider knowledge
- Disclosing securities transactions to others
- Accepting gifts from vendors
- Destruction or disappearance of records or assets
- Any similar or related irregularity

Non-Fraud Irregularities

This section covers allegations of personal improprieties or irregularities and states that they should be resolved by management and not an auditor.

Investigation Responsibilities

This section deals with who will investigate suspected irregularities, as well as to whom these irregularities will be reported (e.g., management, law enforcement, or legal counsel).

Confidentiality

Under this section, the confidential nature of the investigation is set forth. It states that the investigation will not be disclosed to outsiders except as required.

Authorization for Investigation

This delineates that whoever is in charge of the investigation has the authority to take control of and examine records.

Reporting Procedures

This part states that anyone suspecting fraud should report it and not attempt an investigation. It also states that management and others should not make statements regarding the perpetrator's alleged guilt.

Termination

This section states that any recommendations to terminate employees should be reviewed by counsel and management.

Communicating the Fraud Policy

Management must periodically and appropriately communicate the company's fraud policy to all employees and third parties. It does little good to have a fraud or ethics policy if it is not clearly and thoroughly communicated. Again, in such communications, the policy should be presented in a positive, nonaccusatory manner. Communications regarding the policy can be accomplished in several ways.

Orientation/Annual Training

New employees should be advised of the fraud policy at the time of hire. During initial employee orientation, the fraud policy should be discussed. This is the first opportunity the company has to make its point, and it should be made thoroughly.

Additionally, employees should sign an annual statement acknowledging that they understand the policy. Reminding employees via annual online or live training reinforces the policy and management's expectations that it be followed.

Memoranda

An interoffice memorandum from the chief executive officer detailing the fraud policy is a good idea. Once again, the policy should concentrate on the positive aspects of working for an ethical company.

Posters

Some companies might wish to use posters displayed in common areas. However, this should be carefully considered, as some employees might object to such tactics.

Quizzes/Games

Games can be a fun and informal way to reinforce and communicate the fraud policy in an organization. Quizzes with prizes might also be used to reward those who demonstrate awareness of the policy.

Employee Morale

If an employee is properly instructed, communication of a fraud policy can have a positive impact on morale. Honest workers want to work for an honest company. A fraud policy helps set the proper tone.

Legal Considerations

Many companies have learned that it is best to spell out specific unacceptable conduct. If the type of conduct that is considered unacceptable is not accurately detailed, there might be legal problems in discharging a dishonest employee. Check with legal counsel regarding any legal considerations with respect to a fraud policy. One of the most important legal considerations is to ensure everyone and every allegation is handled in a uniform manner. A sample fraud policy is contained at the end of this chapter.

Ethics Programs

In most social groups, the majority of people share the same values. They typically agree on what is good and bad, what is right and wrong, and what is moral and immoral. Although all group members will not hold the same set of values, the social values of the majority will affect the beliefs and behaviors of all people.

The collection of a person's beliefs and morals makes up a set of principles known as *ethics*. Ethics are the judgments about right and wrong or, more specifically, a person's moral obligations to society that determine his actions. Determining ethical rights and wrongs is complicated by the fact that moral standards and generally accepted social behavior change with time. In addition, different groups in the same society might have conflicting ideas of right and wrong. These individual values and ethics are reflected in employees' actions and influence a wide range of organizational decisions. There are four factors that generally affect employees' ethical decisions:

- The law and other government regulations
- Industry and organizational ethical codes

- Social pressures
- Tension between personal standards and organizational needs

A common fallacy in discussions about ethics is: *If it's legal, it's ethical.* A common defense to charges of unethical behavior is to invoke the law. This legalistic approach to ethics mistakenly implies that actions that are not explicitly prohibited by the law are ethical. The main error in this approach is that legal standards do not establish ethical principles. Although abiding by the law is a part of ethical behavior, laws themselves do not describe how an ethical person should behave. One can be dishonest, unprincipled, untrustworthy, unfair, and uncaring without breaking the law. Ethical people measure their conduct by basic principles rather than rules. Thus, in making personal or occupational decisions, the law is only the minimum threshold in determining what is legally possible, and does not address how people should behave ethically.

A written ethics policy is an excellent method by which management can objectively communicate its philosophy and develop a successful ethics program. The policy should be disseminated among both new and old employees. Additionally, some companies have found it effective to share the ethics policy with their vendors, and many organizations make their ethics policies available for the public, such as by posting them on the company's website. Such exposure helps reinforce the importance the organization places on ethics and provides parties outside the organization with a tool to help identify and report breaches of expected employee conduct.

Origins of Ethics

There are theories that state that, by the time one becomes an adult and enters the workplace, a basic code of ethics is already in place. Ethical character is hardwired into the personality before or during adolescence. Based on this theory, if a person did not learn to be ethical in childhood, there is a slim chance that he will act ethically as an adult.

An opposing theory holds that operational values that guide behavior are not formed until early adulthood and, even after that, they are subject to change. Until one has to make serious, binding decisions, it is not necessary to act according to one's beliefs. Based on this theory, as long as individuals have the capacity to reflect and make value judgments, they can modify their personal ethics and change their behavior.

Business ethics programs rely on the validity of the latter theory. With the hope that adult behavior can be affected or modified, ethics programs are designed to steer employees in the right direction.

Ethics' Current Place in Business

The decline in public attitudes about business in recent years has reinforced the importance of ethics in the workplace. Although there seems to be a further deterioration of public confidence, substantial endeavors have been made by organizations with respect to business ethics. These initiatives include adoption of codes of conduct, introduction of ethics into employee and management training, and the establishment of ethics and compliance offices.

Ethics Program Development

Identifying key organizational characteristics and issues is a start to the development of an ethics program. These considerations include:

- Understanding of why good people can commit unethical acts
- Defining current—as well as desired—organizational values
- Determining if organizational values have been properly communicated
- Producing written ethics policies, procedures, or structures
- Ascertaining how board members, stockholders, management, employees, and any other pertinent members of the organization define success
- Determining if ethics is a leadership issue in the organization

With a good understanding of the aforementioned issues, a more effective ethics program can be built. The following 12 components are necessary to develop, implement, and manage a comprehensive ethics program:

- Focus on ethical leadership
- Vision statement
- Values statement
- Code of ethics
- Designated ethics official
- Ethics task force or committee
- Ethics communication strategy
- Ethics training
- Ethics help and fraud report telephone line
- Ethical behavior rewards and sanctions

- Comprehensive system to monitor and track ethics data
- Periodic evaluation of ethics efforts and data

A sample of a typical Code of Business Ethics and an Annual Compliance Questionnaire are provided at the end of this chapter.

SAMPLE FRAUD POLICY

BACKGROUND

The corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against ABC Corporation. It is the intent of ABC Corporation to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and the conduct of investigations.

SCOPE OF POLICY

This policy applies to any irregularity, or suspected irregularity, involving employees, as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with ABC Corporation (also called the Company).

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

POLICY

Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. Fraud is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his injury. Each member of the management team will be familiar with the types of improprieties that might occur within his area of responsibility, and be alert for any indication of irregularity.

Any irregularity that is detected or suspected must be reported immediately to the Director of _____, who coordinates all investigations with the Legal Department and other affected areas, both internal and external.

ACTIONS CONSTITUTING FRAUD

The terms *defalcation, misappropriation,* and *other fiscal irregularities* refer to, but are not limited to, the following:

- Any dishonest or fraudulent act
- Misappropriation of funds, securities, supplies, or other assets
- Impropriety in the handling or reporting of money or financial transactions
- Profiteering as a result of insider knowledge of company activities
- Disclosing confidential and proprietary information to outside parties
- Disclosing to other persons securities activities engaged in or contemplated by the company
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company (Exception: Gifts less than $50 in value)
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment
- Any similar or related irregularity

OTHER IRREGULARITIES

Irregularities concerning an employee's moral, ethical, or behavioral conduct should be resolved by departmental management and the Employee Relations Unit of Human Resources rather than the _____ Unit.

If there is any question as to whether an action constitutes fraud, contact the Director of _____ for guidance.

INVESTIGATION RESPONSIBILITIES

The _____ Unit has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, the _____ Unit will issue reports to appropriate designated personnel and, if appropriate, to the Board of Directors through the Audit Committee.

Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as will final decisions on disposition of the case.

CONFIDENTIALITY

The _____ Unit treats all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify the _____ Unit immediately and *should not attempt to personally conduct investigations or interviews/interrogations* related to any suspected fraudulent act (see REPORTING PROCEDURES section below).

Investigation results *will not be disclosed or discussed* with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability.

AUTHORIZATION FOR INVESTIGATING SUSPECTED FRAUD

Members of the Investigation Unit will have:

- Free and unrestricted access to all Company records and premises, whether owned or rented
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation

REPORTING PROCEDURES

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

An employee who discovers or suspects fraudulent activity will *contact the* _____ *Unit immediately*. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his attorney or representative, or any other inquirer should be directed to the Investigations Unit or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: "I am not at liberty to discuss this matter." *Under no circumstances* should any reference be made to "the allegation," "the crime," "the fraud," "the forgery," "the misappropriation," or any other specific reference.

The reporting individual should be instructed to do the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with *anyone* unless specifically asked to do so by the Legal Department or _____ Unit.

ACTING IN GOOD FAITH

Anyone reporting any irregularity that is detected or suspected must be acting in good faith and have reasonable grounds for believing the information provided. Allegations made maliciously or with knowledge of their falsity will not be tolerated. People making such allegations may be subject to institutional disciplinary action and/or legal actions by the individuals accused of fraudulent conduct.

WHISTLEBLOWER PROTECTION

Employees of ABC Corporation may not retaliate against a whistleblower for reporting an activity which that person believes to be fraudulent or dishonest with the intent or effect of adversely affecting the terms or conditions of employment (including, but not limited to, threats of physical harm, dismissal, transfer to an undesirable job assignment, demotion, suspension, or impact on salary or wages). A whistleblower is defined as an employee who informs a manager, supervisor, or Director of _____ about an activity which that person believes to be fraudulent or dishonest.

Whistleblowers who believe that they have been retaliated against may file a written complaint with the Director of _____. Any complaint of retaliation will be promptly investigated by the _____ and appropriate remedial measures will be taken if allegations of retaliation are proven. This protection from retaliation is not intended to prohibit managers or supervisors from taking action, including disciplinary action, in the usual scope of their duties and based on valid performance-related factors.

TERMINATION

If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from Human Resources and the Legal Department and, if necessary, by outside counsel, before any such action is taken. The _____ Unit does not have the authority to terminate an employee. The decision to terminate an employee is made by the employee's management. Should the _____ Unit believe the management decision inappropriate for the facts presented, the facts will be presented to executive level management for a decision.

ADMINISTRATION

The Director of _____ is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed.

APPROVAL

_____ _____

(CEO/Senior Vice President/Executive) **Date**

Fraud Policy Decision Matrix

Action Required	Investigation Unit	Internal Audit	Finance/ Accounting	Executive Mgmt	Line Mgmt	Risk Mgmt	Legal	Public Relations	Employee Relations
1. Controls to Prevent Fraud	S	S	S	SR	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S	S
3. Investigation of Fraud	P	S					S		S
4. Referrals to Law Enforcement	P						S		
5. Recovery of Monies Due to Fraud	P								
6. Recommendations to Prevent Fraud	SR	SR	S	S	S	S	S	S	S
7. Internal Control Reviews		P							
8. Handle Cases of a Sensitive Nature	P	S		S		S	S		S
9. Publicity/Press Releases	S	S						P	
10. Civil Litigation	S	S					P		
11. Corrective Action/Recommendation to Prevent Recurrences	SR	SR		S	SR	S	S		
12. Monitor Recoveries	S		P						
13. Proactive Fraud Auditing	S	P							
14. Fraud Education/Training	P	S			S			S	
15. Risk Analysis of Areas of Vulnerability	S	S				P			
16. Case Analysis	P	S							
17. Hotline	P	S							
18. EthicsLine	S	S					P		

P (Primary Responsibility) **S (Secondary Responsibility)** **SR (Shared Responsibility)**

Sample Code of Business Ethics and Conduct

Introduction

This section reaffirms the importance of high standards of business conduct. Adherence to this Code of Business Ethics and Conduct by all employees is the only sure way we can merit the confidence and support of the public.

Many of us came from a culture that provided answers or direction for almost every situation possible. Managing our business was not so complex; the dilemmas we faced were—for the most part—simple, making our choices relatively easy. We would probably all agree that managing in today's environment is not so simple.

This code has been prepared as a working guide and not as a technical legal document. Thus, emphasis is on brevity and readability rather than providing an all-inclusive answer to specific questions. For example, the term *employee* is used in its broadest sense and refers to every officer and employee of the company and its subsidiaries. The word "law" refers to laws, regulations, orders, etc.

In observance of this code, as in other business conduct, there is no substitute for common sense. Each employee should apply this code with common sense and the attitude of seeking full compliance with the letter and spirit of the rules presented.

It is incumbent upon you, as an employee of the company, to perform satisfactorily and to follow our policies and comply with our rules as they are issued or modified from time to time.

These policies and rules are necessary to effectively manage the business and meet the ever-changing needs of the marketplace. Good performance and compliance with business rules lead to success. Both are crucial since our ability to provide you with career opportunities depends totally upon our success in the marketplace. Nonetheless, changes in our economy, our markets, and our technology are inevitable. Indeed, career opportunities will vary between the individual companies. For these reasons, we cannot contract or even imply that your employment will continue for any particular period of time. While you might terminate your employment at any time, with or without cause, we reserve that same right. This relationship might not be modified, except in writing signed by an appropriate representative of the company.

This Code of Business Ethics and Conduct is a general guide to acceptable and appropriate behavior at the company, and you are expected to comply with its contents; however, it does not contain all of the detailed information you will need during the course of your employment. Nothing contained in this code or in other communications creates or implies an employment contract or term of employment. We are committed to reviewing our policies continually. Thus, this code might be modified or revised from time to time.

You should familiarize yourself with this code so that you might readily distinguish any proposal or act that would constitute a violation. Each employee is responsible for his actions. Violations can result in disciplinary action, including dismissal and criminal prosecution. There will be no reprisal against an employee who in good faith reported a violation or suspected violation.

The absence of a specific guideline practice or instruction covering a particular situation does not relieve an employee from exercising the highest ethical standards applicable to the circumstances.

If any employee has doubts regarding a questionable situation that might arise, that employee should immediately consult his supervisor or a higher-level manager.

Competition

Fair Competition

The company supports competition based on quality, service, and price. We will conduct our affairs honestly, directly, and fairly. To comply with the anti-trust laws and our policy of fair competition, employees must:

- Never discuss with competitors any matter directly involved in competition between us and the competitor (e.g., sales price, marketing strategies, market shares, and sales policies)
- Never agree with a competitor to restrict competition by fixing prices, allocating markets, or other means
- Not arbitrarily refuse to deal with or purchase goods and services from others simply because they are competitors in other respects
- Not require others to buy from us before we will buy from them
- Not require customers to take from us a service they don't want just so they can get one they do want

- Never engage in industrial espionage or commercial bribery
- Be accurate and truthful in all dealings with customers and be careful to accurately represent the quality, features, and availability of company products and services

Compliance with Laws and Regulatory Orders

The applicable laws and regulatory orders of every jurisdiction in which the company operates must be followed. Each employee is charged with the responsibility of acquiring sufficient knowledge of the laws and orders relating to his duties in order to recognize potential dangers and to know when to seek legal advice.

In particular, when dealing with public officials, employees must adhere to the highest ethical standards of business conduct. When we seek the resolution of regulatory or political issues affecting the company's interests, we must do so solely on the basis of merit and pursuant to proper procedures in dealing with such officials. Employees may not offer, provide, or solicit, directly or indirectly, any special treatment or favor in return for anything of economic value or the promise or expectation of future value or gain. In addition, there shall be no entertaining of employees of the federal or provincial government.

Conflicts of Interest

There are several situations that could give rise to a conflict of interest. The most common are accepting gifts from suppliers, employment by another company, ownership of a significant part of another company or business, close or family relationships with outside suppliers, and communications with competitors. A potential conflict of interest exists for employees who make decisions in their jobs that would allow them to give preference or favor to a customer in exchange for anything of personal benefit to themselves or their friends and families.

Such situations could interfere with an employee's ability to make judgments solely in the company's best interest.

Gifts and Entertainment

DEFINITION OF GIFTS

Gifts are items and services of value that are given to any outside parties, but do not include items described below.

- Normal business entertainment items, such as meals and beverages, are not to be considered gifts.

- Items of minimal value, given in connection with sales campaigns and promotions or employee service, safety, or retirement awards are not to be considered gifts for purposes of this code.
- Contributions or donations to recognized charitable and nonprofit organizations are not considered gifts.
- Items or services with a total value under $100 per year are excluded.

DEFINITION OF SUPPLIER

Supplier includes not only vendors providing services and material to the company, but also consultants, financial institutions, advisors, and any person or institution that does business with the company.

GIFTS

No employee or member of his immediate family shall solicit or accept from an actual or prospective customer or supplier any compensation, advance loans (except from established financial institutions on the same basis as other customers), gifts, entertainment, or other favors that are of more than token value or that the employee would not normally be in a position to reciprocate under normal expense account procedures.

Under no circumstances should a gift or entertainment be accepted that would influence the employee's judgment. In particular, employees must avoid any interest in or benefit from any supplier that could reasonably cause them to favor that supplier over others. It is a violation of the code for any employee to solicit or encourage a supplier to give any item or service to the employee regardless of its value, no matter how small. Our suppliers will retain their confidence in the objectivity and integrity of our company only if each employee strictly observes this guideline.

REPORTING GIFTS

An employee who receives, or whose family member receives, an unsolicited gift prohibited by these guidelines should report it to his supervisor and either return it to the person making the gift or, in the case of a perishable gift, give it to a nonprofit charitable organization.

DISCOUNTS

An employee might accept discounts on a personal purchase of the supplier's or customer's products only if such discounts do not affect the company's purchase price and are generally offered to others having a similar business relationship with the supplier or customer.

BUSINESS MEETINGS

Entertainment and services offered by a supplier or customer may be accepted by an employee when they are associated with a business meeting and the supplier or customer provides them to others as a normal part of its business. Examples of such entertainment and services are transportation to and from the supplier's or customer's place of business, hospitality suites, golf outings, lodging at the supplier's or customer's place of business, and business lunches and dinners for business visitors to the supplier's or customer's location. The services should generally be of the type normally used by the company's employees and allowable under the applicable company's expense account.

Outside Employment

Employees must not be employed outside the company:

- In any business that competes with or provides services to the company or its subsidiaries
- In a manner that would affect their objectivity in carrying out their company responsibilities
- Where the outside employment would conflict with scheduled hours, including overtime, or the performance of the company assignments; employees must not use company time, materials, information, or other assets in connection with outside employment

Relationships with Suppliers and Customers

Business transactions must be entered into solely for the best interests of the company. No employee can, directly or indirectly, benefit from his position as an employee or from any sale, purchase, or other activity of the company. Employees should avoid situations involving a conflict or the appearance of conflict between duty to the company and self-interest.

An employee who deals with individuals or organizations doing or seeking to do business with the company, or who makes recommendations with respect to such dealings, should not:

- Serve as an officer, director, employee, or consultant.
- Own a substantial interest in any competitor of the company, or any organization doing or seeking to do business with the company. *Substantial interest* means an economic interest that might influence or reasonably be thought to influence judgment or action, but shall not include an investment representing less than 1 percent of a class of outstanding securities of a publicly held corporation. Every employee must complete the included Conflict of Interest Questionnaire.

In addition, an employee who deals with individuals or organizations doing or seeking to do business with the company, or who makes recommendations with respect to such dealings, may not:

- Have any other direct or indirect personal interest in any business transactions with the company (other than customary employee purchases of company products and services as consumers and transactions where the interest arises solely by reason of the employee relationship or that of a holder of securities).
- Provide telecommunications or information service or equipment, either directly or as a reseller, in a manner that would place the objectivity or integrity of the company in question.

Our policy is that employees will not do business on behalf of the company with a close personal friend or relative; however, recognizing that these transactions do occur, they must be reported on the Conflict of Interest Questionnaire.

This policy is applicable equally to the members of the immediate family of each employee, which normally includes your spouse, children and their spouses, and the father, mother, sisters, and brothers of yourself and your household.

Employment of Relatives

Relatives of employees will not be employed on a permanent or temporary basis by the company where the relative directly reports to the employee or the employee exercises any direct influence with respect to the relative's hiring, placement, promotions, evaluations, or pay.

Confidential Information and Privacy of Communications

Confidential Information

Confidential information includes all information, whether technical, business, financial, or otherwise concerning the company, which the company treats as confidential or secret and/or which is not available or is not made available publicly. It also includes any private information of, or relating to, customer records, fellow employees, other persons or other companies, and national security information obtained by virtue of the employee's position.

Company policy and various laws protect the integrity of the company's confidential information, which must not be divulged except in strict accordance with established company policies and procedures. The obligation not to divulge confidential company information is in effect even though material might not be specifically identified as confidential, and the obligation exists during and continues after employment with the company.

A few examples of prohibited conduct are:

- Selling or otherwise using, divulging, or transmitting confidential company information
- Using confidential company information to knowingly convert a company business opportunity for personal use
- Using confidential company information to acquire real estate that the employee knows is of interest to the company
- Using, divulging, or transmitting confidential company information in the course of outside employment or other relationship, or any succeeding employment or other relationship at any time
- Trading in the company stocks, or the stocks of any company, based on information that has not been disclosed to the public or divulging such information to others so that they might trade in such stock. Insider trading is prohibited by company policy and by law.

Employees shall not seek out, accept, or use any confidential company information of or from a competitor of the company. In particular, should we hire an employee who previously worked for a competitor, we must neither accept nor solicit confidential information concerning that competitor from our employee.

Company Assets

Cash and Bank Accounts

All cash and bank account transactions must be handled so as to avoid any question or suspicion of impropriety. All cash transactions must be recorded in the company's books of account.

All accounts of company funds, except authorized imprest funds, shall be established and maintained in the name of the company or one of its subsidiaries and may be opened or closed only on the authority of the company's Board of Directors. Imprest funds must be maintained in the name of the custodian, and the custodian is wholly responsible for these funds. All cash received shall be promptly recorded and deposited in a company or subsidiary bank account. No funds shall be maintained in the form of cash, except authorized petty cash, and no company shall maintain an anonymous (numbered) account at any bank. Payments into numbered bank accounts by the company might leave that company open to suspicion of participation in a possibly improper transaction. Therefore, no disbursements of any nature might be made into numbered bank accounts or other accounts not clearly identified to the company as to their ownership.

No payments can be made in cash (currency) other than regular, approved cash payrolls and normal disbursements from petty cash supported by signed receipts or other appropriate documentation. Further, corporate checks shall not be written to "cash," "bearer," or similar designations.

Company Assets and Transactions

Compliance with prescribed accounting procedures is required at all times. Employees having control over company assets and transactions are expected to handle them with the strictest integrity and ensure that all transactions are executed in accordance with management's authorization. All transactions shall be accurately and fairly recorded in reasonable detail in the company's accounting records.

Employees are personally accountable for company funds over which they have control. Employees who spend company funds should ensure that the company receives good value in return and must maintain accurate records of such expenditures. Employees who approve or certify the correctness of a bill or voucher should know that the purchase and amount are proper and correct. Obtaining or creating "false" invoices or other misleading

documentation or the invention or use of fictitious sales, purchases, services, loans, entities, or other financial arrangements is prohibited.

Employees must pay for personal telephone calls and use, except to the extent that specifically defined benefit programs or allowances otherwise provide.

Expense Reimbursement

Expenses actually incurred by an employee in performing company business must be documented on expense reports in accordance with company procedures. In preparing expense reports, employees should review these procedures for the documentation in order to be reimbursed for business expenses.

Company Credit Card

Company credit cards are provided to employees for convenience in conducting company business. No personal expenses can be charged on company credit cards except as specifically authorized by company procedures. Any charged personal expenses must be paid promptly by the employee. Company credit cards should not be used to avoid preparing documentation for direct payment to vendors. Where allowed by local law, charges on company credit cards for which a properly approved expense report has not been received at the time of an employee's termination of employment might be deducted from the employee's last paycheck. The company will pursue repayment by the employee of any amounts it has to pay on the employee's behalf.

Software and Computers

Computerized information and computer software appear intangible, but they are valuable assets of the company and must be protected from misuse, theft, fraud, loss, and unauthorized use or disposal, just as any other company property.

Employees cannot access company records of any kind for their personal use. Misappropriation of computer space, time, or software includes, but is not limited to, using a computer to create or run unauthorized jobs, operating a computer in an unauthorized manner, or intentionally causing any kind of operational failure.

Company-owned computers can be used for company-sanctioned education programs, as well as personal use incidental to company business use, with the permission of your supervisor. However, personal use is not allowed for personal financial gain.

Political Contributions

The level of contributions that can be made by corporations to political parties or candidates is set out by the applicable jurisdictions' laws. In addition to direct cash contributions, the term *political contributions* includes the donation of property or services and the purchases of tickets to fundraising events.

Where corporate political contributions are legal in connection with federal, provincial, or municipal elections, such contributions shall be made only from funds allocated for that purpose, and with the written approval of the president of the company making the contribution.

Employee Conduct

Conduct on Company Business

Dishonest or illegal activities on company premises or while on company business will not be condoned and can result in disciplinary action, including dismissal and criminal prosecution. The following illustrates activities that are against company policy, and that will not be tolerated on company premises, in company vehicles, or while engaged in company business:

- Consumption and storage of alcoholic beverages, except where legally licensed or authorized by an officer of the company
- The use of controlled substances, such as drugs or alcohol; the unlawful manufacture, distribution, dispensation, possession, transfer, sale, purchase, or use of a controlled substance
- Driving vehicles or operating company equipment while under the influence of alcohol or controlled substances
- Illegal betting or gambling
- Carrying weapons of any sort on company premises, in company vehicles, or while on company business; even employees with permits or licenses cannot carry weapons on company property or while on company business

The company reserves the right to inspect any property that might be used by employees for the storage of their personal effects. This includes desks, lockers, and vehicles owned by the company. It is a violation of company policy to store any contraband, illegal drugs, toxic materials, or weapons on company property.

Reporting Violations

All employees are responsible for compliance with these rules, standards, and principles. In the area of ethics, legality, and propriety, each employee has an obligation to the company that transcends normal reporting relationships. Employees should be alert to possible violations of the code anywhere in the company and are encouraged to report such violations promptly. Reports should be made to the employee's supervisor, the appropriate security, audit, or legal department personnel, or elsewhere as the circumstance dictates. Employees will also be expected to cooperate in an investigation of violations. In addition, any employee who is convicted of a criminal offense, whether related to these rules or not, should also report that fact.

All cases of questionable activity involving the code or other potentially improper actions will be reviewed for appropriate action, discipline, or corrective steps. Whenever possible, the company will keep confidential the identity of employees about or against whom allegations of violations are brought, unless or until it has been determined that a violation has occurred. Similarly, whenever possible, the company will keep confidential the identity of anyone reporting a possible violation. Reprisal against any employee who has, in good faith, reported a violation or suspected violation is strictly prohibited.

All employees are required to notify the company within five (5) days of any conviction of any criminal statute violation occurring on the job. In addition, any employee who is convicted of a felony, whether related to these rules or not, should report that fact.

Discipline

Violation of this code can result in serious consequences for the company, its image, credibility, and the confidence of its customers, and can include substantial fines and restrictions on future operations, as well as the possibility of fines and prison sentences for individual employees. Therefore, it is necessary that the company ensure that there will be no violations. Employees should recognize that it is in their best interest, as well as the company's, to follow this code carefully.

The amount of any money involved in a violation might be immaterial in assessing the seriousness of a violation since, in some cases, heavy penalties might be assessed against the company for a violation involving a relatively small amount of money, or no money.

Disciplinary action should be coordinated with the appropriate Human Resources representatives. The overall seriousness of the matter will be considered in setting the disciplinary action to be taken against an individual employee. Such action, which might be reviewed with the appropriate Human Resources representatives, might include:

- Reprimand
- Probation
- Suspension
- Reduction in salary
- Demotion
- Combination of the above
- Dismissal

In addition, individual cases might involve:

- Reimbursement of losses or damages
- Referral for criminal prosecution or civil action
- Combination of the above

Disciplinary action might also be taken against supervisors or executives who condone, permit, or have knowledge of illegal or unethical conduct by those reporting to them and do not take corrective action. Disciplinary action might also be taken against employees who make false statements in connection with investigations of violations of this code.

The company in its sole discretion will determine the disciplinary action appropriate to a given matter. The listing of possible actions is informative only and does not bind the company to follow any particular disciplinary steps, process, or procedure.

The company's rules and regulations regarding proper employee conduct will not be waived in any respect. Violation is cause for disciplinary action, including dismissal. All employees will be held to the standards of conduct described in this booklet.

The company never has and never will authorize any employee to commit an act that violates this code or to direct a subordinate to do so. With that understood, it is not possible to justify commission of such an act by saying someone directed it in higher management.

Compliance Letter and Conflict of Interest Questionnaire

Annually, all officers of the company will represent in writing that there are no violations of this code known to the officer, after the exercise of reasonable diligence, or if such violations have been committed, to disclose such violations in a format to be specified.

Annually, each employee will review the Code of Business Ethics and Conduct, sign the Code's Acknowledgment form, and complete and sign the Conflict of Interest Questionnaire. If the employee's circumstances change at any time, a new Conflict of Interest Questionnaire or letter of explanation must be completed.

The Code of Business Ethics and Conduct Acknowledgment form should be signed and given to your supervisor for inclusion in your personnel file.

[*COMPANY NAME*]

Code of Conduct Compliance Questionnaire

Managerial employees are being asked to complete this Compliance Questionnaire. [*COMPANY NAME*] and its subsidiaries are committed to providing a workplace where employees can and do act responsibly and ethically. The [*COMPANY NAME*] Code of Conduct sets out specific standards of conduct that should govern our behavior toward our fellow employees, suppliers, and customers. Please answer each of the following questions and, if necessary, provide an explanation. *For any "yes" response, please explain in the extra space provided on the last page.*

Conflict of Interest

1. During fiscal 20XX, did you receive, or are you aware of anyone who received, from any person or company doing business with your employer any loan, gift, trip, gratuity, or other payment that did or could cause prejudice toward or obligation to the giver, or could be perceived by others as creating an obligation to the giver? *(Note: Each item, or the total of items from a single vendor with a value of more than $50, must be reported, except that you do not need to report loans made by financial institutions on normal and customary terms, common stock dividends, or insurance policy payments).*

   ☐ **Yes** ☐ **No**

2. In fiscal 20XX, did you participate in or influence, or are you aware of anyone who participated in or influenced, any transaction between your employer and another entity in which they or any member of their family had a direct or indirect financial interest?

   ☐ **Yes** ☐ **No**

3. In fiscal 20XX, did you have a material financial interest in or hold a position of influence with, or are you aware of anyone who had a material financial interest in or held a position of influence with, any business that furnishes goods or services to your employer? *(Note: The term* material financial interest *means someone who by virtue of their stock ownership or monetary interest in a company is able to direct or to influence business decisions, or a commissioned sales representative;* position of influence *means someone holding an influential position such as a sole proprietor, partner, member of a board of directors, an executive, or a manager.)*

   ☐ **Yes** ☐ **No**

4. For fiscal 20XX, did you use, or are you aware of anyone who used, company assets or other resources (including funds, equipment, supplies, or personnel) for purposes other than company business or company-sponsored activities?

   ☐ **Yes** ☐ **No**

5. During fiscal 20XX, did you receive, or are you aware of anyone who received, gifts or entertainment from individuals or organizations having dealings with the Company, including but not necessarily limited to loans, any form of cash gratuities, private or personal discounts not sanctioned by the Company, or remuneration or service related to illegal activities?

   ☐ **Yes** ☐ **No**

6. During fiscal 20XX, did you accept, or are you aware of anyone who accepted, any consideration or special favors from suppliers or potential suppliers that in fact or appearance could be deemed a bribe, kickback, or reward given to influence your business judgment?

   ☐ **Yes** ☐ **No**

7. Were you involved in, or are you aware of any employee who was involved in, a conflict of interest situation during fiscal year 20XX?

   ☐ **Yes** ☐ **No**

8. I have read the attached Conflict of Interest Policy Statement, which is set forth in the [*COMPANY NAME*] [and Subsidiaries] Code of Conduct and Compliance Program. Accordingly, I have listed below all relationships and outside activities that require disclosure under the policy. I have also listed names, addresses, and the nature of the relationships of all persons or entities doing business with my employer from whom I or any member of my immediate family has received, directly or indirectly, cash or a gift of more than nominal value ($50) during the fiscal year ended May 31, 20XX. *(If there are no persons or entities to be listed, so indicate by writing "NONE" in the first space provided below.)*

Name of Person/Entity	Nature of Relationship/Outside Activity

Political

9. In fiscal 20XX, did you receive, or are you aware of anyone who received, any payments from your employer for the purpose of making a contribution to any political party, candidate, or election committee?

☐ **Yes** ☐ **No**

Securities Trading

10. Did you buy or sell, or are you aware of anyone who may have bought and/or sold, stock based on confidential information, or communicated confidential information to influence [*COMPANY NAME*] stock transactions?

☐ **Yes** ☐ **No**

Financial Integrity

11. Are you aware of any entries made in the books and records of your employer in fiscal 20XX that you believe are false or intentionally misleading?

☐ **Yes** ☐ **No**

12. Are you aware of any assets, liabilities, or transactions that you believe were improperly omitted from the books of your company in fiscal 20XX?

☐ **Yes** ☐ **No**

13. In fiscal 20XX, are you aware of anyone seeking to influence any government official (including foreign officials) or government employee, or individual doing business with your company, by offering money, goods, or services in return for some special consideration?

☐ **Yes** ☐ **No**

Other

14. Are you aware of any incident involving your employer that you feel constituted noncompliance with laws, regulations, policies, guidelines, procedures, or ethical principles, other than those matters referred to in other questions or incidents that have already been reported? *(Note: If you prefer to report an incident or violation anonymously, please answer this question "NO" and contact a member of the Ethics Committee or call the Confidential Ethics Hotline.)*

    ☐ **Yes** ☐ **No**

15. Please provide any explanations for "yes" responses.

    _____

    _____

    _____

16. In the space below, please provide any suggestions you may have for improving the Code of Conduct and Compliance Program.

    _____

    _____

    _____

_____

Printed Name

_____

Signature

_____

Date

[*COMPANY NAME*] AND SUBSIDIARIES

Employee	Company/Subsidiary	Location

Code of Conduct and Conflict of Interest Employee Certification

- I have read the [*COMPANY NAME*] and Subsidiaries Code of Conduct and Compliance Program.

- I understand that the standards and policies in that Code of Conduct represent the policies of [*COMPANY NAME*] and its subsidiaries, and that violating those standards and policies, or any legal and regulatory requirements applicable to my job, may result in penalties set forth in the Code of Conduct or other appropriate sanction.

- I understand that there are several sources within the company, including the Ethics Committee, that I can consult if I have questions concerning the meaning or application of the Code of Conduct or relevant legal and regulatory requirements.

- I understand that it is my responsibility to disclose to an Ethics Officer, a member of the [*COMPANY NAME*] Operations Audit Department, a member of the Ethics Committee, or the Company's Ethics Hotline any situation that might reasonably appear to be a violation of the Code of Conduct.

- I have read the attached Conflict of Interest Policy Statement that is set forth in the [*COMPANY NAME*] and Subsidiaries Code of Conduct and Compliance Program. Accordingly, I have listed below all relationships and outside activities that require disclosure under the policy. I have also listed names, addresses, and the nature of the relationships of all persons or entities doing business with my employer from whom I or any member of my immediate family has received, directly or indirectly, cash or a gift of more than nominal value ($50) during the fiscal year ended May 31, 20XX. *(If there are no persons or entities to be listed, so indicate by writing "NONE" in the first space provided below.)*

Name of Person/Entity	Address	Nature of Business/Relationship

- I am not aware of any exceptions to standards and policies in the Code of Conduct except: *(if none, so indicate by writing "NONE.")*

_____

_____

_____

Signature of Employee **Date**

FRAUD RISK ASSESSMENT

For an organization to be able to effectively manage its fraud risks, the risks must first be identified using a formal risk assessment. If performed and used correctly, a fraud risk assessment can be a powerful proactive tool in the fight against fraud for any business. Additionally, regulators, professional standard-setters, and law enforcement authorities continue to emphasize the crucial role that fraud risk assessment plays in developing and maintaining effective anti-fraud programs and controls.

What Is Fraud Risk?

Cressey's fraud triangle teaches us that there are three interrelated elements that enable someone to commit fraud: the *motive* or pressure that drives a person to want to commit the fraud, the *opportunity* that enables him to commit the fraud, and the *ability to rationalize* the fraudulent behavior. The vulnerability that an organization faces from individuals capable of combining all three of these elements is *fraud risk*. Fraud risk can come from sources both internal and external to the organization, and it is one of the many types of risks managed by an organization.

Inherent and Residual Fraud Risks

When considering the fraud risks faced by an organization, it is helpful to analyze how significant a risk is before and after risk response. Risks that are present before management action are described as *inherent risks*. The risks that remain after management action are described as *residual risks*.

For example, there is an inherent risk that the employee in charge of receiving customer payments at a small company might embezzle incoming cash. Controls, such as segregation of duties and oversight from the company owner, can be implemented to help mitigate this risk; however, even with such controls in place, some residual risk will likely remain that the bookkeeper might still manage to embezzle funds. The objective of the controls is to make the residual risk significantly smaller than the inherent risk.

What Factors Influence Fraud Risk?

Many factors influence how at-risk an organization is to fraud. Some of the main factors are:

- The nature of its business
- The environment in which it operates
- The effectiveness of its internal controls
- The ethics and values of the company and its employees

The Nature of the Business

The types of risks an organization faces are directly connected to the nature of the business in which it is engaged. For example, the inherent fraud risks faced by hospitals and medical practices are vastly different from those faced by banks and financial institutions, construction companies, educational institutions, or retail organizations.

The Operating Environment

The environment in which the organization operates has a direct impact on its vulnerability to fraud. Brick-and-mortar businesses have a very different risk profile than Internet businesses. Likewise, local businesses have different risk profiles than those that operate in the international arena.

The Effectiveness of Its Internal Controls

A good system of internal controls, with the right balance of preventive and detective controls, can greatly reduce an organization's vulnerability to fraud. *Preventive controls* are those manual or automated processes that stop something bad from happening before it occurs. *Detective controls* can also be manual or automated, but are designed to identify something bad that has already occurred. No system of internal controls can fully eliminate the risk of fraud, but well-designed and effective internal controls can deter the average fraudster by reducing the opportunity to commit the fraud and increasing the perception of detection.

The Ethics and Values of the Company and Its Employees

It is extremely difficult, if not impossible, to have a company made up of individuals whose ethics and values are fully aligned with those of the organization. Any significant gaps in alignment can increase an organization's fraud risk.

While many organizations have codes of conduct, those codes are not always clear in drawing a definitive line between acceptable and unacceptable behavior. That lack of clarity

leaves room for fraudsters to rationalize their actions. For example, in most organizations, it is generally understood that manipulating financial records is unacceptable behavior that will result in termination; however, it is not always apparent whether taking a pen or pencil home that belongs to the company is unacceptable behavior, or what the consequence, if any, would be.

An organization that is clear and consistent about its ethics, values, and expectations will reduce the potential fraudster's ability to rationalize his actions. Likewise, an organization that demonstrates consistency and predictability in how it handles and holds accountable unacceptable behaviors can significantly reduce the risk of fraud.

What Is a Fraud Risk Assessment?

Fraud risk assessment is a process aimed at proactively identifying and addressing an organization's vulnerabilities to both internal and external fraud. As every organization is different, the fraud risk assessment process is often more an art than a science. What gets evaluated and how it gets assessed should be tailored to the organization—there is no one-size-fits-all approach. Additionally, organizational fraud risks continually change. It is therefore important to think about a fraud risk assessment as an ongoing, continuous process, rather than just an activity.

A fraud risk assessment starts with an identification and prioritization of fraud risks that exist in the business. The process evolves as the results of that identification and prioritization begin to drive education, communication, organizational alignment, and action around effectively managing fraud risk and identifying new fraud risks as they emerge.

What Is the Objective of a Fraud Risk Assessment?

In the simplest terms, the objective of a fraud risk assessment is to help an organization recognize what makes it most vulnerable to fraud. Through a fraud risk assessment, the organization is able to identify where fraud is most likely to occur, enabling proactive measures to be considered and implemented to reduce the chance that it could happen. The strategic reasoning used in conducting a fraud risk assessment requires a skeptical mindset and involves asking questions such as:

- How might a fraud perpetrator exploit weaknesses in the system of controls?
- How could a perpetrator override or circumvent controls?
- What could a perpetrator do to conceal the fraud?

Why Should Organizations Conduct Fraud Risk Assessments?

Every organization should conduct a fraud risk assessment and build procedures to keep the assessment process current and relevant. Not only is this practice good corporate governance, but it makes good business sense. Additionally, conducting a fraud risk assessment enables the organization to:

- Improve communication and awareness about fraud.
- Identify where the company is most vulnerable to fraud and what activities put it at the greatest risk.
- Know who puts the organization at the greatest risk.
- Develop plans to mitigate fraud risk.
- Develop techniques to investigate and determine if fraud has occurred in high-risk areas.
- Assess internal controls.
- Comply with regulations and professional standards.

Improve Communication and Awareness About Fraud

A fraud risk assessment can be a great vehicle for an organization to open up communication and raise awareness about fraud. When employees are engaged in an open discussion about fraud, the conversations themselves can play a role in reducing fraud vulnerability. Employees are reminded that the organization does care about preventing fraud and they are empowered to come forward if they suspect fraud is occurring. Open communication and awareness about fraud can also deter a potential fraudster by reducing his ability to rationalize bad behavior and increasing his perception that someone might catch on to his actions and report him.

Identify What Activities Are the Most Vulnerable to Fraud

Management must know where the company is most vulnerable to fraud to prevent it from happening. For most companies, the normal course of business generally involves many different activities; however, not all of the activities that the company engages in are equal in terms of increasing the business's exposure to fraud. The fraud risk assessment helps guide the organization to focus on the activities that put the company at greatest risk.

Know Who Puts the Organization at the Greatest Risk

The actions of certain individuals can significantly increase the company's vulnerability to fraud. The risk can be driven from the way in which someone makes decisions, behaves, or treats others within and outside the organization. The fraud risk assessment can help home in on those people and their activities that might increase the company's overall fraud risk.

Develop Plans to Mitigate Fraud Risk

If management knows where the greatest fraud risks are, it can put plans in place to reduce or mitigate those risks. The results of the fraud risk assessment can be used to gain alignment among stakeholders and drive preventive action.

Develop Techniques to Determine If Fraud Has Occurred in High-Risk Areas

Assessing an area as having a high fraud risk does not conclusively mean that fraud is occurring there. Nevertheless, the fraud risk assessment is useful in identifying areas that should be proactively investigated for evidence of fraud. In addition, putting high-risk areas under increased scrutiny can deter potential fraudsters by increasing their perception of detection.

Assess Internal Controls

Many organizations rely heavily on their internal control system to prevent and detect fraud. Although internal control plays a critical role in fraud prevention and detection, it is a dynamic system that requires constant reevaluation of its weaknesses. Performing a fraud risk assessment provides management with the opportunity to review the company's internal control system for effectiveness, taking into account the following considerations:

- Controls that might have been eliminated due to restructuring efforts (e.g., elimination of separation of duties due to downsizing)
- Controls that might have eroded over time due to reengineering of business processes
- New opportunities for collusion
- Lack of internal controls in a vulnerable area
- Nonperformance of control procedures (e.g., control procedures compromised for the sake of expediency)
- Inherent limitations of internal controls, including opportunities for those responsible for a control to commit and conceal fraud (e.g., through management and system overrides)

Comply with Regulations and Professional Standards

Fraud risk assessments can assist management and auditors (internal and external) in satisfying regulatory requirements and complying with professional standards pertaining to their responsibility for fraud risk management.

For example, International Standard on Auditing (ISA) 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment*, requires auditors to

undertake risk assessment procedures during audit engagements and includes key points that should be considered during this process.

What Makes a Good Fraud Risk Assessment?

A good fraud risk assessment is one that fits within the culture of the organization, is sponsored and supported by the right people, encourages everyone to openly participate, and is generally embraced throughout the business as an important and valuable process. Conversely, a fraud risk assessment that is conducted without these conditions will have inferior results.

Collaborative Effort of Management and Auditors

As regulations and professional standards indicate, both management and auditors have a responsibility for fraud risk management. However, each of these parties has unique knowledge and perspective of the fraud risks faced by the organization. Management has intricate familiarity with day-to-day business operations; responsibility for assessing business risks and implementing organizational controls; authority to adjust operations; influence over the organization's culture and ethical atmosphere; and control over the organization's resources (e.g., people and systems). Auditors, conversely, are trained in risk identification and assessment, and have an expertise in evaluating internal controls, which is critical to the fraud risk assessment process. Consequently, the fraud risk assessment is most effective when management and auditors share ownership of the process and accountability for its success.

The Right Sponsor

Having the right sponsor for a fraud risk assessment is extremely important in ensuring its success and effectiveness. The sponsor must be senior enough in the organization to command the employees' respect and elicit full cooperation in the process. The sponsor also must be someone who is committed to learning the truth about where the company's fraud vulnerabilities are; he must be a truth seeker—not someone who is prone to rationalization or denial. In the ideal situation, the sponsor would be an independent board director or audit committee member; however, a chief executive officer or other internal senior leader can be equally as effective.

Organizational culture plays a key role in influencing the organization's vulnerability to fraud. If the company's culture is shaped by a strong and domineering leader, obtaining

candid participation from the people in the business might be difficult with that leader as sponsor of the fraud risk assessment.

The right sponsor is someone who is willing to hear the good, the bad, and the ugly. For example, suppose a fraud risk assessment reveals that one of the greatest fraud risks facing the organization is bribery/corruption based on the close relationship between one of the key business leaders and the company's business partners. For the fraud risk assessment to be effective, the sponsor needs to be independent and open in his evaluation of the situation and, most important, appropriate in his response to the identified risks.

Independence/Objectivity of the People Leading and Conducting the Work

A good fraud risk assessment can be effectively conducted either by people inside the organization or with external resources. Either way, it is critical that the people leading and conducting the fraud risk assessment remain independent and objective throughout the assessment process. Additionally, they must be perceived as independent and objective by others.

The people leading and conducting the work should be mindful of any personal biases they might have regarding the organization and the people within it, and they should take steps to reduce or eliminate all biases that might affect the fraud risk assessment process. For example, if an employee on the fraud risk assessment team had a bad past experience with someone in the accounts payable department, he might allow that experience to affect his evaluation of the fraud risks related to that area of the business. To preclude this possibility, someone else should perform the fraud risk assessment work related to the accounts payable department's activities.

Cultural neutrality is an important aspect of independence and objectivity when leading or conducting a fraud risk assessment. Some organizations have very strong corporate cultures that can play a big role in influencing the way the people inside the organization think about fraud risk. If people within the organization are leading and conducting the fraud risk assessment, they must be able to step outside the corporate culture to assess and evaluate the presence and significance of fraud risks in the business.

A Good Working Knowledge of the Business

The individuals leading and conducting the fraud risk assessment need to have a good working knowledge of the business. Every organization is unique; even companies that

appear similar have characteristics that differentiate them—and their fraud risks—from their competitors. Some of those differences can be obvious, whereas others are more subtle.

To ensure a good working knowledge of the business, the fraud risk assessor must know, beyond a superficial level, what the business does and how it operates. He must also have an understanding of what makes the organization both similar to and different from other companies in related lines of business.

Obtaining information about broad industry fraud risks from external sources can be helpful. Such sources include industry news; criminal, civil, and regulatory complaints and settlements; and professional associations and organizations.

Access to People at All Levels of the Organization

It is often said that perception is reality. In other words, how an individual perceives a situation is his reality of that situation. In an organization, it is important that the perceptions of people at all levels are included in the fraud risk assessment process.

Leaders of a business or function often have very different perspectives from their subordinates on how something is perceived or executed; however, this does not mean that one perspective is right and the other is wrong. What it does mean is that expectations and perceptions within the organization are not aligned, which could increase fraud risk.

Risk assessments created or performed by management and auditors without the input of the staff performing the operational tasks will be ineffective. It is crucial to include members of all levels of the organization in the risk assessment process to ensure that all relevant risks are addressed and reviewed from many different perspectives.

Engendered Trust

If management and employees do not trust the people leading and conducting the fraud risk assessment, they will not be open and honest about the realities of the business, its culture, and its vulnerability to fraud. Trust is not something that can be granted by authority; it must be earned through words and actions. As the people leading and conducting the fraud risk assessment engage with employees throughout the business, they should deliberately and carefully plan the initial contact with an effort to develop a rapport and gain trust.

The Ability to Think the Unthinkable

Most honest people are not naturally inclined to think like a criminal. In fact, many large-scale frauds that have occurred would have been deemed unthinkable by people closest to the events. But a necessary part of conducting an effective fraud risk assessment involves thinking like a fraudster. A good fraud risk assessment has to allow for the people leading and conducting the assessment to be expansive in their consideration and evaluation of fraud risk. Thoughts of "it couldn't happen here" should not be allowed to moderate the evaluation of fraud risk.

A Plan to Keep It Alive and Relevant

The fraud risk assessment should not be treated as a onetime exercise that is executed, reported on, and then put on a shelf to collect dust. The organization should strive to keep the process alive and relevant through ongoing dialogue, active management of action plans, and development of procedures to ensure the assessment is maintained on a current and routine basis.

Considerations for Developing an Effective Fraud Risk Assessment

A fraud risk assessment is only effective if the organization embraces it and uses the results to monitor, change, or influence the factors that put the company at risk for fraud.

Packaging It Right

People do not easily relate to or embrace things they don't understand. Every organization has its own vocabulary and preferred methods of communication. The announcement and execution of the fraud risk assessment, including the reporting of the results, will only be effective if completed in the language of the business. For example:

- In a creative organization where decisions are made based on qualitative assessments and instinct, and where the majority of communication is visual, a quantitative approach to assessing fraud risk—one that is driven by numbers and calculations—would most likely be rejected.
- In an organization where the business is built and run on quantitative decision-making models, a qualitative approach with no quantitative components would most likely be rejected.

The assessor must remain mindful of the language used throughout the fraud risk assessment. Specifically, he should stay away from technical language that won't resonate with people in the business. For example, many people might not easily relate to or

understand the term *cash larceny*. If cash larceny is one of the organization's greatest fraud risks, it might be more effective to explain the concept in layman's terms, such as *theft of cash*.

One Size Does Not Fit All

Do not try to fit a round peg into a square hole; what works in one organization most likely will not easily work in another. Recognizing the nuances and differences of each business and tailoring the approach and execution to the specific organization contributes to the success of the fraud risk assessment. While a generic framework or toolset can be a valuable starting point for the development of the fraud risk assessment, it must be adapted to fit the business model, culture, and language of the organization.

Keeping It Simple

The more complicated the fraud risk assessment is, the harder it will be to execute it and use it to drive action. Whether the assessor uses a generic assessment framework or develops one specifically for the organization, he should focus the effort and time on evaluating the areas that are most likely to have fraud risk.

Preparing the Company for a Fraud Risk Assessment

Properly preparing the company for the fraud risk assessment is critical to the assessment's success. The culture of the organization should influence the approach used in the fraud risk assessment preparation. The goals of the preparation should be to:

- Assemble the right team to lead and conduct the fraud risk assessment.
- Determine the best techniques to use in conducting the fraud risk assessment.
- Obtain the sponsor's agreement on the work to be performed.
- Educate the employees and openly promote the process.

Assemble the Right Team to Lead and Conduct the Fraud Risk Assessment

The organization should build a fraud risk assessment team consisting of individuals with diverse knowledge, skills, and perspectives to lead and conduct the assessment. The size of the team will depend on the size of the organization and the methods used to conduct the assessment. The team should have individuals who are credible and who have experience in gathering and eliciting information.

The team members can include internal and external resources such as:

- Accounting and finance personnel who are familiar with the financial reporting processes and internal controls
- Nonfinancial business unit and operations personnel who have knowledge of day-to-day operations, customer and vendor interactions, and issues within the industry
- Risk management personnel who can ensure that the fraud risk assessment process integrates with the organization's enterprise risk management program
- The general counsel or other members of the legal department
- Members of any ethics or compliance functions within the organization
- Internal auditors
- External consultants with fraud and risk expertise
- Any business leader with direct accountability for the effectiveness of the organization's fraud risk management efforts

Determine the Best Techniques to Use in Conducting the Fraud Risk Assessment

There are many ways to conduct a fraud risk assessment. Picking a method or combination of methods that is culturally right for the organization will help to ensure its success. The assessment team should also consider the best ways to gather candid information from people throughout all levels of the organization, starting by understanding what techniques are commonly and effectively used throughout the organization. The following are some examples of methods that can be used to conduct the fraud risk assessment.

Interviews

Interviews can be an effective way to conduct a candid one-on-one conversation. But their usefulness depends on how willing people in the organization are to be open and honest in a direct dialogue with the interviewer. The assessor must consider whether interviews are commonly and effectively used in the organization to gather and elicit information. He should also speak with individuals who have previously conducted interviews with employees to glean lessons learned. For each potential interviewee, the assessor should gauge the willingness of the interviewee to be open and honest—some people might be good interview candidates, whereas others might need to be engaged through a different approach.

Focus Groups

Focus groups enable the assessor to observe the interactions of employees as they discuss a question or issue. Some topics might lend themselves to being discussed in an open forum in which people feel comfortable among their colleagues. Additionally, when discussing tough

or thorny issues in a group, an anonymous, real-time voting tool can be an effective way of opening up a dialogue among the participants.

The success of a focus group will be highly dependent on the skill of the facilitator. If focus groups are used as part of the fraud risk assessment, they should be led by an experienced facilitator whom the group will relate to and trust. Getting a group to open up and talk honestly can be very difficult. An experienced facilitator will be able to read the group and use techniques, such as group icebreakers, to make the session a success.

Surveys

Surveys can be anonymous or directly attributable to individuals. Sometimes people will share more openly when they feel protected behind a computer or paper questionnaire. In an organization where the culture is not one in which people open up and freely talk, an anonymous survey can be an effective way to get feedback. However, employees can be skeptical about the true anonymity of a survey, especially in organizations that use surveys to solicit feedback anonymously but send follow-up emails to individual delinquent respondents. If the assessor determines that an anonymous survey is an appropriate technique to use in the fraud risk assessment, he should clearly and explicitly explain to employees how anonymity will be maintained.

Anonymous Feedback Mechanisms

In some organizations, anonymous suggestion boxes or similar mechanisms are used to encourage and solicit frequent employee feedback. In these companies, information pertaining to the fraud risk assessment can be requested in the same way. Additionally, use of an anonymous feedback mechanism can be effective in an environment where people are less likely to be open and honest through other methods and techniques.

One approach to effectively using the anonymous feedback technique involves establishing a question of the day that is prominently displayed above a collection box. A sample question is: "If you thought fraud were occurring in the company, would you come forward? Why or why not?"

Another approach involves using a table lineup of five to ten opaque boxes, each with a statement posted above it. Employees are provided with poker chips in two different colors and told that one color indicates "I agree" and the other indicates "I disagree." Employees

are then encouraged to respond to each statement by putting a corresponding chip in each box to indicate their response.

Obtain the Sponsor's Agreement on the Work to Be Performed

Before the fraud risk assessment procedures begin, the sponsor and the assessment team need to agree on:

- The scope of work that will be performed
- The methods that will be used (e.g., surveys, interviews, focus groups, or anonymous feedback mechanisms)
- The individuals who will participate in the chosen methods
- The content of the chosen methods
- The form of output for the assessment

Educate the Organization and Openly Promote the Process

The fraud risk assessment process should be visible and communicated throughout the business. Employees will be more inclined to participate in the process if they understand its purpose and the expected outcomes.

Sponsors should be strongly encouraged to openly promote the process. The more personalized the communication from the sponsor, the more effective it will be in encouraging employees to participate. Whether through a video, town-hall meeting, or companywide email, the communication should be aimed at eliminating any reluctance employees have about participating in the fraud risk assessment process.

Fraud Risk Assessment Frameworks

Fraud risk assessments can be executed in many ways. To ensure the assessment's success, the approach should be structured, rational, and tailored to the organization. Consequently, when conducting a fraud risk assessment, it is helpful to use a framework for performing, evaluating, and reporting on the results of the work. Fraud risk can be analyzed and reported both qualitatively and quantitatively using a consistent framework. In adopting a framework, however, the fraud risk assessment team must ensure that the specific needs and culture of the organization are considered and accounted for. Without tailoring the fraud risk assessment approach to the specific organization, the team encounters the risk of missing important factors or obtaining results that are unreliable or meaningless.

The following sample fraud risk assessment frameworks illustrate how the elements of fraud risk assessment are applied under different approaches.

Sample Fraud Risk Assessment Framework #1[1]

Using this framework, the fraud risk assessment team incorporates the following steps into the fraud risk assessment strategy:

1. Identify potential inherent fraud risks.
2. Assess the likelihood of occurrence of the identified fraud risks.
3. Assess the fraud risks' significance to the organization.
4. Evaluate which people and departments are most likely to commit fraud and identify the methods they are likely to use.
5. Identify and map existing preventive and detective controls to the relevant fraud risks.
6. Evaluate whether the identified controls are operating effectively and efficiently.
7. Identify and evaluate residual fraud risks resulting from ineffective or nonexistent controls.

The following table provides a visual representation of the steps involved in this framework, and can be filled in as the fraud risk assessment is performed.

[1] This framework is based on information contained in *Managing the Business Risk of Fraud: A Practical Guide*, sponsored by the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners. The full text of this publication is available at: www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf.

Fraud Risk Assessment Framework[2]

Identified Fraud Risks and Schemes	Likelihood	Significance	People and/or Departments	Existing Anti-Fraud Controls	Controls' Effectiveness Assessment	Residual Risks	Fraud Risk Response
Financial Reporting:							
Misappropriation of Assets:							
Corruption:							
Other Risks:							

Identify Potential Inherent Fraud Risks

One of the first steps in a fraud risk assessment involves identifying potential fraud risks inherent to the organization. The fraud risk assessment team should brainstorm to identify the fraud risks that could apply to the organization. Brainstorming should include discussions regarding the topics discussed in the following sections.

INCENTIVES, PRESSURES, AND OPPORTUNITIES TO COMMIT FRAUD

When assessing incentives, pressures, and opportunities to commit fraud, the fraud risk assessment team should evaluate:

- Opportunities to commit fraud that arise from a person's position (i.e., given his responsibilities and authority)
- Incentive programs and how they might affect employees' behavior when conducting business or applying professional judgment

[2] *Managing the Business Risk of Fraud: A Practical Guide*, sponsored by the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners, 21.

- Pressures on individuals to achieve performance or other targets and how such pressures might influence employees' behavior
- Opportunities to commit fraud that arise from weak internal controls, such as a lack of segregation of duties
- Highly complex business transactions and how they might be used to conceal fraudulent acts
- Opportunities for collusion (intrinsic to schemes such as bribery or kickbacks)

RISK OF MANAGEMENT'S OVERRIDE OF CONTROLS

When considering the potential for management's override of controls, the fraud risk assessment team should keep in mind that:

- Management personnel within the organization generally know the controls and standard operating procedures that are in place to prevent fraud.
- Individuals who are intent on committing fraud might use their knowledge of the organization's controls to do it in a manner that will conceal their actions.

POPULATION OF FRAUD RISKS

The fraud risk identification process requires an understanding of the universe of fraud risks and the subset of risks that apply to a particular organization. It includes gathering information about the business itself, including its business processes, industry, and operating environment, as well as all associated potential fraud risks. Such information can be obtained from external sources—such as industry news outlets; criminal, civil, and regulatory complaints and settlements; and professional organizations and associations—and from internal sources by interviewing and brainstorming with personnel, reviewing complaints on the whistleblower hotline, and performing analytical procedures.

Although the specific fraud risks an organization faces will be unique to that organization, they generally can be classified into the following major areas: fraudulent financial reporting, asset misappropriation, corruption, and external fraud. Potential fraud risks to consider in each category are discussed below.

FRAUDULENT FINANCIAL REPORTING

Potential fraudulent financial reporting risks include:

- Inappropriately reported revenues, expenses, or both
- Inappropriately reflected balance sheet amounts, including reserves
- Inappropriately improved or masked disclosures

- Concealed misappropriation of assets
- Concealed unauthorized receipts, expenditures, or both
- Concealed unauthorized acquisition, use, or disposition of assets

ASSET MISAPPROPRIATIONS

Potential asset misappropriation risks include misappropriation of:

- Tangible assets
- Intangible assets
- Proprietary business opportunities

CORRUPTION

Potential corruption risks include:

- Payment of bribes or gratuities to companies, private individuals, or public officials
- Receipt of bribes, kickbacks, or illegal gratuities
- Aiding and abetting of fraud by outside parties, such as customers or vendors

EXTERNAL FRAUD

External fraud risks include:

- Fraud committed by customers (e.g., fraudulent customer payments)
- Fraud committed by vendors (e.g., overbilling by a vendor or collusion between bidding contractors to inflate contract price)
- Fraud committed by competitors (e.g., corporate espionage)
- Fraud committed by unrelated third parties (e.g., hacking)

RISK OF REGULATORY AND LEGAL MISCONDUCT

Regulatory and legal misconduct includes a wide range of risks, such as conflicts of interest, insider trading, theft of competitor trade secrets, anti-competitive practices, environmental violations, and trade and customs regulations in areas of import and export. Depending on the particular organization and the nature of its business, some or all of these risks might be applicable and should be considered in the fraud risk assessment process.

REPUTATION RISK

Reputation risk must be considered as part of the organization's risk assessment process because fraudulent acts can damage an organization's reputation with customers, suppliers,

capital markets, and others. For example, fraud leading to a financial restatement can damage an organization's reputation in capital markets, which can increase the organization's cost of borrowing and depress its market capitalization.

RISK TO INFORMATION TECHNOLOGY

Information technology (IT) is a critical component of fraud risk assessment. Organizations rely on IT to conduct business, communicate, and process financial information. A poorly designed or inadequately controlled IT environment can expose an organization to threats to data integrity, threats from hackers to system security, and theft of financial and sensitive business information. Whether in the form of hacking, economic espionage, Web defacement, sabotage of data, viruses, or unauthorized access to data, IT fraud risks can result in significant financial and information losses.

Assess the Likelihood and Significance of the Identified Fraud Risks

Assessing the likelihood and significance of each potential fraud risk is a subjective process that allows the organization to manage its fraud risks and apply preventive and detective controls rationally. The fraud risk assessment team should first consider fraud risks to the organization on an inherent basis, without consideration of known controls. By approaching the assessment in this manner, the team will be better able to consider all relevant fraud risks and then evaluate and design controls to address those risks.

ASSESS THE LIKELIHOOD OF OCCURRENCE OF THE IDENTIFIED FRAUD RISKS

The likelihood of occurrence of each fraud risk can be classified *as remote, reasonably possible,* or *probable*. The fraud risk assessment team should consider the following inherent factors in assessing the likelihood of occurrence of each fraud risk:

- Prevalence of the fraud risk in the organization's industry
- Number of individual transactions involved
- Complexity of the fraud risk
- Number of people involved in reviewing or approving a relevant process
- Information from fraud surveys such as the ACFE's *Report to the Nations on Occupational Fraud and Abuse*

In addition, the team should evaluate the likelihood of the identified risks based on organization-specific factors, such as:

- The organization's internal control environment
- Management's ethical standards

- Management's support of fraud prevention efforts
- Resources available to address fraud
- Past instances of the particular fraud at the organization
- Complaints by customers or vendors
- Unexplained losses

ASSESS THE SIGNIFICANCE TO THE ORGANIZATION OF THE FRAUD RISKS

The fraud risk assessment team should consider qualitative and quantitative factors when assessing the significance of identified fraud risks to the organization. For example, a particular fraud risk that might only pose an immaterial direct financial risk to the organization, but that could greatly affect its reputation, would be deemed a significant risk to the organization.

The significance of each potential fraud can be classified as *immaterial*, *significant*, or *material*. In assessing the significance of each fraud risk, the fraud risk assessment team should consider the following factors:

- Financial statement and monetary significance
- Financial condition of the organization
- Value of the threatened assets
- Criticality of the threatened assets to the organization
- Revenue generated by the threatened assets
- Significance to the organization's operations, brand value, and reputation
- Criminal, civil, and regulatory liabilities

Evaluate Which People and Departments Are Most Likely to Commit Fraud and Identify the Methods They Are Likely to Use

In identifying potential fraud risks, the risk assessment team will have evaluated the incentives and pressures on individuals and departments to commit fraud. The team should use the information gained in that process to identify the individuals and departments most likely to commit fraud and the methods they are likely to use. This knowledge will assist the organization in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.

Identify and Map Existing Preventive and Detective Controls to the Relevant Fraud Risks

After identifying and assessing fraud risks for likelihood of occurrence and for significance, the fraud risk assessment team should identify and map existing preventive and detective controls to the relevant fraud risks.

PREVENTIVE CONTROLS

Preventive controls, which are intended to prevent fraud before it occurs, include:

- Bringing awareness of the fraud risk management program to personnel throughout the organization
- Performing background checks on employees (where permitted by law)
- Hiring competent personnel and providing them with anti-fraud training
- Conducting exit interviews
- Segregating duties
- Ensuring proper alignment between an individual's authority and his level of responsibility
- Reviewing third-party and related-party transactions

DETECTIVE CONTROLS

Detective controls, which are intended to detect fraud if it does occur, include:

- Establishing and marketing the presence of a confidential reporting system, such as a whistleblower hotline
- Implementing proactive controls for the fraud detection process, such as independent reconciliations, reviews, physical inspections/counts, analysis, and audits
- Implementing proactive fraud detection procedures, such as data analysis and continuous auditing techniques
- Performing surprise audits

Evaluate Whether the Identified Controls Are Operating Effectively and Efficiently

The fraud risk assessment team must ensure that there are adequate controls in place, that the controls are mitigating fraud risk as intended, and that the benefit of the controls exceeds the cost. Such an assessment requires:

- Review of the accounting policies and procedures in place
- Consideration of the risk of management's override of controls
- Interviews with management and employees
- Observation of control activities

- Sample testing of controls compliance
- Review of previous audit reports
- Review of previous reports on fraud incidents, shrinkage, and unexplained shortages

Identify and Evaluate Residual Fraud Risks Resulting from Ineffective or Nonexistent Controls

Consideration of the internal control structure might reveal certain residual fraud risks, including management's override of established controls, that have not been adequately mitigated due to:

- Lack of appropriate prevention and detection controls
- Noncompliance with established prevention and control measures

The likelihood and significance of occurrence of these residual fraud risks should be evaluated by the fraud risk assessment team in the development of the fraud risk response.

Sample Fraud Risk Assessment Framework #2—Fraud Risk Index

The following is a suggested framework that has two components: the Fraud Risk Index, which looks at indicators of areas that put the organization at risk for fraud, and the Leadership Risk Profile, which examines the way business leaders operate to help determine if they behave or conduct business in a way that can increase the company's risk of fraud.

Fraud Risk Index

The Fraud Risk Index is the overall assessment of fraud risk for the organization based on three components:

- The Environmental Risk Index
- The Culture Quotient
- The Prevent/Detect Index

THE ENVIRONMENTAL RISK INDEX

The Environmental Risk Index is an assessment of macro-level fraud risk indicators that can affect the organization's vulnerability to fraud. These include factors such as pressures on the business, the organization's system of internal controls, the tone at the top, and the overall quality of the mechanisms that the company has in place to prevent and detect fraud.

THE CULTURE QUOTIENT

The Culture Quotient is an assessment of how the organization and its people behave or are perceived to behave. The Culture Quotient includes:

- Tolerance Index—an assessment of the organization's tolerance for bad behavior. An organization that has a high tolerance for bad behavior can significantly increase the company's vulnerability to fraud risk.
- Entitlement Index—an assessment that helps determine whether people in the company display or promote a sense of entitlement. An organization that sustains a strong sense of entitlement from its employees or leaders can have a higher risk of fraud.
- Notification Index—an assessment of how likely it is that employees will come forward when they suspect something is wrong. An organization where there is a low probability that employees will come forward is at significantly greater risk of fraud than an organization where it is likely that employees will come forward.

Both the Environmental Risk Index and Culture Quotient are elements of the Fraud Risk Index that are aimed at identifying and evaluating macro-level indicators of fraud risk to which the company might be exposed. The content and approach for performing these parts of the assessment should be tailored for the organization under review.

THE PREVENT/DETECT INDEX

The Prevent/Detect Index assesses the quality of the specific mechanisms that the organization has in place to prevent or detect potential fraud, particularly those fraud schemes for which the company is at the greatest risk. This component of the assessment can be used to identify the company's greatest fraud risks by pinpointing areas and methods that provide opportunities for potential fraudsters to get something—of either real or perceived value—out of the business.

To calculate the Prevent/Detect Index, a standard, comprehensive population of fraud schemes, such as the ACFE Occupational Fraud Classification System, is used to evaluate each scheme that applies to the business and determine which schemes are the high-risk schemes that the organization should focus on. For those fraud schemes that apply to the company, an evaluation of each scheme should be performed to identify:

- The likelihood that the scheme could be perpetrated
- The significance of the fraud risk to the company
- Whether there are preventive or detective internal controls in place to moderate the risk to a sufficient level

Leadership Risk Profile

The Leadership Risk Profile is developed to provide a macro-level organizational view of which business leaders, if any, increase the organization's vulnerability to fraud through their:

- Leadership style
- Operating behaviors
- Decision-making practices

The fraud risk assessment team should develop or obtain an organizational chart that shows the organizational structure of the business and identifies its leaders. The team should then develop a profile of each of the leaders and evaluate the fraud risk associated with their leadership styles, operating behaviors (including how they interact with their team and partners across the business), and decision-making practices.

As part of this evaluation, the team should consider any information that indicates unique pressures on or incentives for each leader that could increase the organization's fraud risk. Such pressures and incentives can include, but are not limited to:

- A significant amount of personal net worth invested in the company
- A large portion of compensation tied to activities that the leader can manipulate (e.g., sales volumes or other business performance measures)
- A pending divorce
- Recent organizational changes that have either greatly expanded or reduced/eliminated the leader's span of control
- Living larger than life
- Dependence on drugs or alcohol
- Gambling problems

Note that a comprehensive approach to conducting a fraud risk assessment using this framework would include the assessment of both the Fraud Risk Index and the Leadership Risk Profile. However, due to the sensitive nature of the Leadership Risk Profile, the sponsor may decide to focus the assessment on only the Fraud Risk Index.

Addressing the Identified Fraud Risks

Establishing an Acceptable Level of Risk

Because it is neither practical nor cost effective for an organization to eliminate all fraud risk, management must establish an acceptable level of fraud risk—often referred to as a *risk tolerance*—based on the business objectives and risk tolerance of the organization. In responding to fraud risks identified during the fraud risk assessment, management must determine how the fraud risks affect business objectives and, using cost/benefit analysis, decide where to best allocate resources for fraud prevention and detection.

Ranking and Prioritizing Risks

Once risks are identified, they need to be prioritized. There are two basic frameworks for prioritizing risk:

- Estimating the likely cost of a risk
- Using a quadrant graph, called a heat map, to identify those risks that are both likely and significant

Estimating Likely Cost of a Risk

Estimating the likely cost of a risk involves determining a quantitative value for the expected loss based on the risk's potential cost and likelihood of occurrence. Both of these factors are estimates—and are far from objective—but by engaging in a process to estimate and quantify these elements of risk, an organization can prioritize its risks from the highest to lowest expected cost and focus on the outcomes that would be the most expensive.

Under this model, Risk = Likelihood x Cost.

Consider the following risk scenarios:

1. Risk of lost business and reputation damage from a disruption in data processing:
   Likely cost (in lost revenue) = $100,000
   Likelihood of occurrence = 2%
   Potential loss = $2,000 (2% x $100,000)

2. Risk of lost revenues from losing a major client:
   Likely cost (in lost revenue) = $500,000
   Likelihood of occurrence = 15%
   Potential loss = $75,000 (15% x $500,000)

3. Risk of employee embezzlement:
   Likely cost = $150,000
   Likelihood of occurrence = 7%
   Potential loss = $10,500 (7% x $150,000)

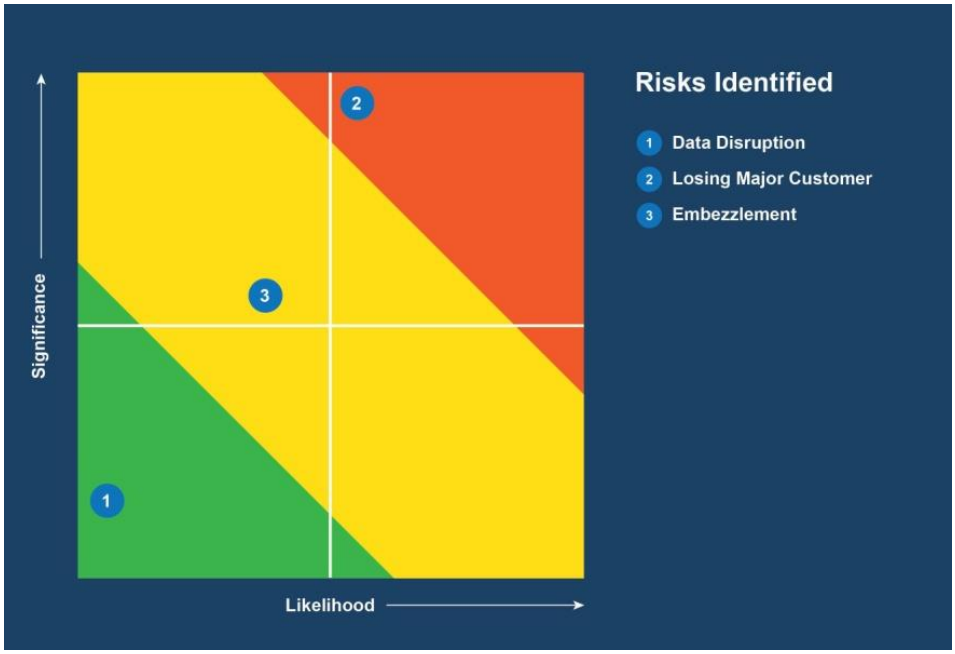
This analysis could then be used to rank these three risks by listing them from highest to lowest potential loss:

Risk	Potential Loss
Loss of a major client	$75,000
Employee embezzlement	$10,500
Data process disruption	$2,000

Based on this listing, the assessment team would be equipped with an awareness of the most expensive losses and could allocate their compliance resources accordingly to mitigate, share, or abandon the highest cost risks.

Plotting Risks on a Heat Map

With a heat map, the risk assessment team is seeking to focus its attention on those risks that are both likely and significant. The risk assessment team goes through the list of risks and places each in a quadrant of the heat map, based on its assessed significance and likelihood. The following analysis prioritizes those risks that are in the red and yellow areas.



Responding to Residual Fraud Risks

Regardless of the framework used to conduct the fraud risk assessment, management will need to address the identified risks to ensure that the organization is within its established tolerance level for fraud risk.

Larry Cook, CFE, who is the principal author of the ACFE Fraud Risk Assessment Tool (www.acfe.com/fraud-risk-assessment.aspx), suggests that management can use one or a combination of the following approaches to respond to the organization's residual fraud risks:[3]

- Avoid the risk.
- Transfer the risk.
- Mitigate the risk.
- Assume the risk.

Avoid the Risk

Management may decide to avoid the risk by eliminating an asset or discontinuing an activity if the control measures required to protect the organization against an identified threat are

[3] Larry E. Cook, "Risky Business: Conducting the Internal Fraud Risk Assessment," *Fraud Magazine,* March/April 2005.

too expensive. This approach requires the fraud risk assessment team to complete a cost-benefit analysis of the value of the asset or activity to the organization compared to the cost of implementing measures to protect the asset or activity.

Transfer the Risk

Management may transfer some or all of the risk by purchasing fidelity insurance or a fidelity bond. The cost to the organization is the premium paid for the insurance or bond. The covered risk of loss is then transferred to the insurance company.

Mitigate the Risk

Management can mitigate the risk by implementing appropriate countermeasures, such as prevention and detection controls. The fraud risk assessment team should evaluate each countermeasure to determine whether it is cost effective and reasonable given the probability of occurrence and impact of loss.

Assume the Risk

Management may choose to assume the risk if it determines that the probability of occurrence and impact of loss are low. Management may decide that it is more cost effective to assume the risk than it is to eliminate the asset or discontinue the activity, buy insurance to transfer the risk, or implement countermeasures to mitigate the risk.

Combination Approach

Management may also elect a combination of these approaches. For example, if the probability of occurrence and impact of loss are high, management may decide to transfer part of the risk through the purchase of insurance, as well as to implement preventive and detective controls to mitigate the risk.

Reporting the Results of the Fraud Risk Assessment

The success of the fraud risk assessment process hinges on how effectively the results are reported and what the organization then does with those results. A poorly communicated report can undermine the entire process and bring all established momentum to a halt. The report should be delivered in a style most suited to the language of the business. If management prefers succinct PowerPoint presentations, the fraud risk assessment team should not deliver a 50-page Word document.

Considerations When Reporting the Assessment Results

To maximize the effectiveness of the process, the team should consider the following points when developing the report of the results.

Report Objective—Not Subjective—Results

Much instinct and judgment goes into performing the fraud risk assessment. When reporting the results of the assessment, the team must stick to the facts and keep all opinions and biases out of the report. A report that is interspersed with the assessment team's subjective perspective will dilute and potentially undermine the results of the work.

Keep It Simple

The assessment results should be reported in a way that is easy to understand and that resonates with management. The reader of the report should be able to quickly view and comprehend the results. A simple one-page visual can sometimes make the most impact.

Focus on What Really Matters

Less is often more when it comes to reporting the results of the fraud risk assessment. The team should take care not to turn the report into a laundry list of things that management will have to sort through and prioritize. Instead, the report should be presented in a way that focuses on what really matters, clearly highlighting those points that are most important and that will make the most impact on the organization's fraud risk management efforts.

Identify Actions That Are Clear and Measurable to Drive Results

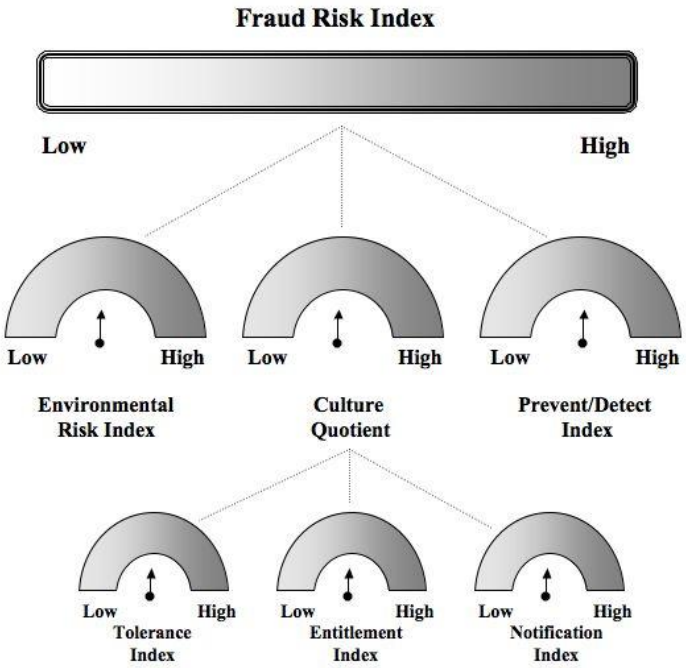
The report should include key recommendations for action that are clear and measurable and that will decrease fraud risks. The actions should be presented in a way that makes apparent exactly what needs to be done. The report should not include recommendations that are vague or that wouldn't reduce the risk of fraud. Additionally, management and those affected by the suggested actions should have already vetted and agreed to the recommendations.

Sample Report Formats

The following are two examples of simple formats that can be used or adapted to report on the results of a fraud risk assessment based on the Fraud Risk Index framework discussed earlier in this chapter.

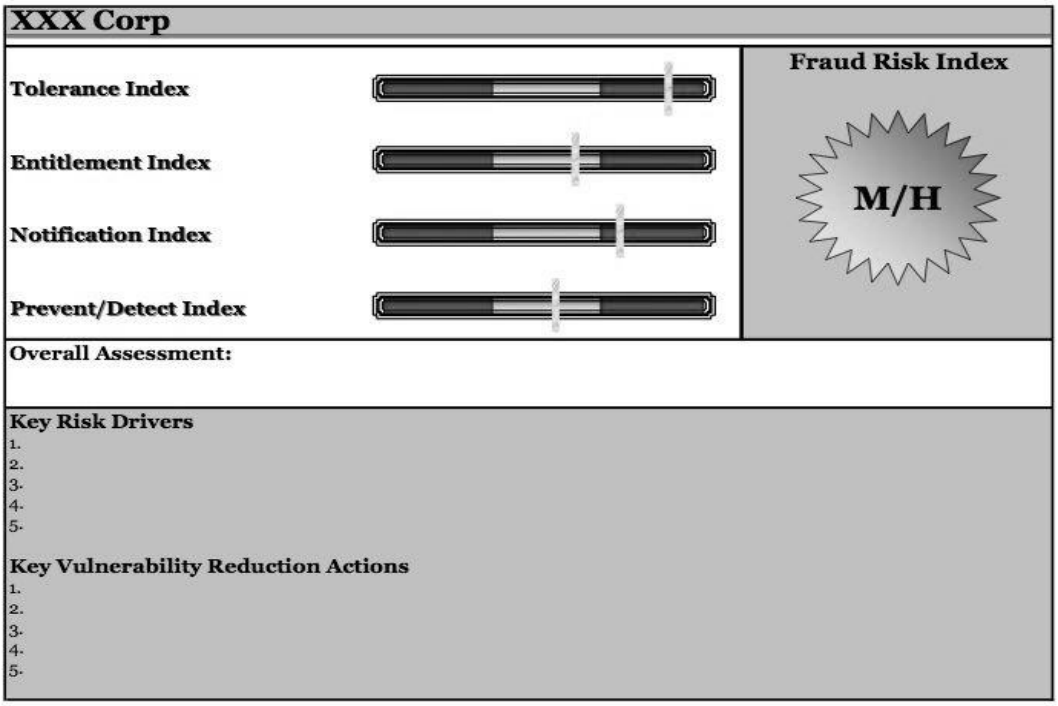
Graphic Report Format

The first sample report format, shown below, would work well in an organization that uses dashboards or tends to be visually oriented. The gauges can be substituted with any type of visual representation that the organization uses in the normal course of business. This report should be accompanied by a one- or two-page action plan.



Executive Summary Report Format

The following report format is a simple one-page, executive-summary-type report. It gives the reader a snapshot view of the results of the work, along with insight into what is driving the results and what actions can be taken to reduce the fraud risk. Using a simple format like this forces the assessment team to focus on what really matters and what will make the most impact.



Reporting the Leadership Risk Assessment Results

The results of the Leadership Risk Profile should be treated with great sensitivity. The fraud risk assessment team should discuss with the sponsor what the best method is for conveying the results of that work. If a formal report is requested, a color-coded organization chart can be used as a quick visual to convey the fraud risk associated with each leadership area across the business.

Making an Impact with the Fraud Risk Assessment

To make the most of the fraud risk assessment process, management should use the results to:

- Begin a dialogue across the company.
- Look for fraud in high-risk areas.
- Hold responsible parties accountable for progress.
- Keep the assessment process alive and relevant.
- Monitor key controls.

Begin a Dialogue Across the Company

The results of the initial fraud risk assessment can be used to begin a dialogue across the company that promotes awareness, education, and action planning aimed at reducing the risk

of fraud. Engaging in an active dialogue is an effective way to further establish boundaries of acceptable and unacceptable behavior. Open communication about fraud risks also increases the chance that employees will come forward if they believe they have witnessed potential fraud.

Look for Fraud in High-Risk Areas

An internal audit or investigative team within the organization can use the results of the fraud risk assessment to identify high-risk processes or activities and unusual transactions that might indicate fraud. This practice can also provide some reassurance if the subsequent search for fraud reveals that, despite the assessed risk, fraud does not appear to be occurring at that point in time. Management should remember, however, that just because there is no evidence that fraud is occurring in the present, the risk that it could occur in the future is not eliminated.

Hold Responsible Parties Accountable for Progress

It is often said that what gets measured gets done. To effectively reduce identified fraud risk, management must hold employees accountable for driving results. The organization should track and measure progress against agreed-upon action plans. Publicly celebrating successes can be as or more effective in encouraging the right behaviors as providing negative consequences for failing to deliver results.

Keep It Alive and Relevant

Since there are so many factors that can affect an organization's vulnerability to fraud risk, management must ensure that the fraud risk assessment stays current and relevant. Someone within the organization should be assigned ownership of the fraud risk assessment process. That person or team should build processes to ensure that all changes in the business model, company operating environment, and personnel are considered relative to their impact on the company's risk of fraud.

Monitor Key Controls

At the culmination of a fraud risk assessment, the organization should have a clear view of both the areas where the organization is susceptible to fraud and the controls that are designed and implemented to address those weak spots. To effectively manage the i dentified fraud risks, management should use the results of the fraud risk assessment to monitor the performance of key internal controls. Such proactive attention will allow for

the identification and correction of deficiencies in control design or operation as quickly as possible.

The Fraud Risk Assessment and the Audit Process

The fraud risk assessment should play a significant role in informing and influencing the audit process. In addition to being used in the annual audit planning process, the fraud risk assessment should drive thinking and awareness in the development of audit programs for areas that have been identified as having a moderate to high risk of fraud. Although auditors should always be on guard for things that might be indicators of fraud risk, the results of the fraud risk assessment can help them design audit procedures in a way that enables them to look for fraud in known areas of high risk.

In the course of their work, auditors should validate that the organization is appropriately managing the moderate-to-high fraud risks identified in the fraud risk assessment by:

- Identifying and mapping the existing preventive and detective controls that pertain to the moderate-to-high fraud risks identified in the fraud risk assessment
- Designing and performing tests to evaluate whether the identified controls are operating effectively and efficiently
- Identifying within the moderate-to-high fraud risk areas whether there is a moderate-to-high risk of management override of internal controls
- Developing and delivering reports that incorporate the results of their validation and testing of the fraud risk controls

The following template can be used by auditors to evaluate how effectively the moderate-to-high fraud risks are being managed by the business:

Identiified Fraud Risks	Existing Prevent Controls	Existing Detect Controls	Controls are Effective and Efficient?	Risk of Management Override?	Is the fraud risk effectively managed?

The Fraud Risk Assessment Tool

Introduction

The ACFE's Fraud Risk Assessment Tool can be used by fraud examiners to identify their clients' or employers' vulnerabilities to fraud.

The Fraud Risk Assessment Tool consists of 15 modules, each containing a series of questions designed to help organizations zoom in on areas of risk. The fraud professional and the client or employer should begin the risk assessment process by working together to answer the questions in each module. It is important that the client or employer select people within the organization who have extensive knowledge of company operations, such as managers and internal auditors, to work with the fraud professional. Upon completion of all of the questions, the fraud professional should review the results of the assessment with the client or employer in order to:

- Identify the potential inherent fraud risks.
- Assess the likelihood and significance of occurrence of the identified fraud risks.
- Evaluate which people and departments are most likely to commit fraud and identify the methods they are likely to use.
- Identify and map existing preventive and detective controls to the relevant fraud risks.
- Evaluate whether the identified controls are operating effectively and efficiently.

- Identify and evaluate residual fraud risks resulting from ineffective or nonexistent controls.
- Respond to residual fraud risks.

The Fraud Risk Assessment Tool may reveal certain residual fraud risks that have not been adequately mitigated due to lack of, or noncompliance with, appropriate preventive and detective controls. The fraud professional should work with the client to develop mitigation strategies for any residual risks with an unacceptably high likelihood or significance of occurrence. Responses should be evaluated in terms of their costs versus benefits and in light of the organization's level of risk tolerance.

Be aware, however, that this assessment only provides a snapshot of a particular point in time. The dynamic nature of organizations requires routine monitoring and updating of their financial risk assessment processes in order for them to remain effective.

Module #1—Employee Assessment

The employee assessment questions are designed to assess the probability of a fraudulent event occurring within the organization based on:

- Internal controls
- Internal control environment
- Resources available to prevent, detect, and deter fraud

1. Are employees provided formal written job descriptions?

In addition to clarifying what employees are responsible for, job descriptions signify what employees are not responsible for. Employees who perform duties outside of their job descriptions represent a significant red flag.

2. Are employees provided with an organizational chart that shows lines of responsibility?

Organizational charts provide employees with a snapshot of an organization's division of work, levels of management, and reporting relationships.

3. Does the company have written accounting policies and procedures?

Accounting policies and procedures, including those related to fraud, should be documented, implemented, and communicated to employees.

4. Is there a formal policy covering approval authority for financial transactions, such as purchasing or travel?
In order to safeguard assets and financial reporting, companies should develop and implement policies for determining how financial transactions are initiated, authorized, recorded, and reviewed.

5. Does the company have an ethics statement?
The company should implement a formal ethics statement that (1) defines conduct that is unethical, (2) states that unethical acts will be punished, and (3) provides information on reporting unethical conduct.

6. Does senior management exhibit and encourage ethical behavior?
Senior management sets the tone for ethical conduct throughout the organization. The tone should signal that fraud will not be tolerated.

7. Does the company have written fraud policies and procedures?
The company should document and implement fraud policies and procedures that describe (1) fraudulent conduct, (2) punishment for engaging in fraudulent conduct, and (3) how to report fraudulent conduct.

8. Is a senior member of management responsible for compliance with fraud policies?
The responsibility for compliance with fraud and ethics policies should be assigned to a senior member of management.

9. Does the organization educate employees about the importance of ethics and anti-fraud programs?
All employees should receive training on the ethics and anti-fraud policies of the company. The employees should sign an acknowledgment that they have received the training and understand the policies.

10. Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud programs?
Organizations should provide employees, vendors, and customers with a confidential system for reporting suspected violations of the ethics and anti-fraud policies.

11. Are fraud incidents promptly and thoroughly investigated?
Promptly and thoroughly investigating all reported incidents of fraud can minimize losses.

12. Does the company maintain a record of fraud incidents?

A formal record of all reported incidents of fraud, including documentation of investigative activities and final disposition of each incident, should be maintained.

13. Does the company conduct pre-employment background checks?

Before offering employment to an applicant, a company should conduct a pre-employment background check (where permitted by law).

14. Does the company have a loss prevention function?

Responsible personnel should be trained to perform loss prevention functions.

15. Does the company have an internal audit function?

Internal audits that focus on high-risk areas for fraud can identify new vulnerabilities, measure the effectiveness of internal controls, and signal that fraud prevention is a high priority for the company.

16. Are the duties related to authorization, custody of assets, and recording or reporting of transactions segregated?

The company should segregate the duties related to authorization, custody of assets, and recording or reporting of transactions.

17. Is compliance with internal controls audited periodically?

Periodic audits of compliance with internal controls send the message to employees that the company is proactive in its anti-fraud efforts.

18. Do employees feel they are treated and compensated fairly?

Management should establish appropriate lines of communication with employees (e.g., surveys, exit interviews, and open-door policies) to assess their attitudes toward the organization.

19. Do any employees have large personal debts or credit problems?

Employees with large personal debts or credit problems are a red flag of potential fraud and should be monitored by management.

20. Do any employees appear to be spending far more than they are earning?
Management should be observant of signs of employees spending far more than they are earning. It is common for employees who steal to use the proceeds for lifestyle improvements, including expensive cars and extravagant vacations.

21. Do any employees gamble excessively?
Employees who gamble excessively pose a potential fraud risk to the company and should be monitored by management. Employee assistance programs can be made available to help employees with gambling addictions.

22. Do any employees use alcohol or drugs excessively?
Employees who use alcohol or drugs excessively pose a potential fraud risk to the company and should be monitored by management. Employee assistance programs can be made available to help employees with alcohol or drug addictions.

23. Do any employees resent their superiors?
Employees who resent their superiors should be monitored by management, as they pose a potential fraud risk to the company.

24. Do any employees have a close association with vendors or competitors?
Employees with a close relationship to a vendor or competitor should be monitored for potential conflict of interest.

25. Do any employees have outside business interests that might conflict with their duties at the company?
Employees should be required to provide annual financial disclosures that list outside business interests. Outside interests that conflict with the organization's interests should be prohibited.

26. Is the company experiencing high employee turnover?
High employee turnover, especially in areas particularly vulnerable to fraud, is a warning sign of fraud that should be investigated.

27. Are employees required to take annual vacations?
Requiring employees to take annual vacations can aid an employer in detecting an ongoing fraud scheme because the employer is more likely to discover a perpetrator running such a scheme when the perpetrator is removed from the scene.

28. Is the company dominated by a small group of individuals?

If control is centered in the hands of a few key employees, those individuals should be under heightened security for compliance with internal controls and other policies and procedures.

29. Does the company have unrealistic productivity measurements and expectations?

Unrealistic productivity measurements and expectations can place undue pressure on employees and result in employees committing fraudulent acts in order to meet them.

30. Does management fail to give employees positive feedback and recognition for job performance?

Providing positive feedback and recognition to employees helps to reduce the likelihood of internal fraud and theft through boosting morale. Employees with positive feelings about an organization are less likely to commit fraud against the organization.

31. Are employees afraid to deliver bad news to supervisors or management?

Management should promote a culture in which employees aren't afraid to deliver bad news. After all, the sooner management receives the bad news, the sooner it can respond.

32. Is there a lack of communication between employees and management?

Management can improve communication with employees by creating an atmosphere that encourages open communication. Employees should feel safe in sharing any thoughts, comments, complaints, or suggestions.

33. Is there a lack of clear organizational responsibilities in the company?

A lack of clear organizational responsibilities can lead to confusion and frustration for employees. Organizational charts and job descriptions can be used to clarify organizational responsibilities.

34. Does management not seem to care about or reward appropriate employee behavior?

Management that does not seem to care about or reward appropriate employee behavior can contribute to low employee morale and increased risk of fraud against the company by employees.

Module #2—Management/Key Employee Assessment

The management/key employee assessment questions are designed to assess the probability of a fraudulent event occurring within the organization based on:

- Internal controls
- Internal control environment
- Resources available to prevent, detect, and deter fraud

1. Is the board of directors composed of mainly officers of the company or related individuals?

The board of directors should include independent board members that are not associated with or employed by the company. In theory, independent directors are not subject to the same pressures as management and, therefore, are more likely to act in the best interest of shareholders.

2. Is there an independent audit committee?

Independent audit committee members with financial and accounting expertise can be instrumental in preventing and detecting financial fraud.

3. Has there been high turnover of managers and members of the board of directors?

Management should investigate the reasons for high turnover and implement measures to reduce it.

4. Have an unusually high number of key employees left the company recently?

Management should investigate the reasons for their departure and implement measures to reduce turnover.

5. Is the company involved in any litigation?

Management should determine the reason for the litigation, monitor the filings, and take corrective action where necessary.

6. Does the company have offshore activities or bank accounts?

Management should determine the reason for the offshore activities and accounts, ascertain compliance with U.S. laws, and monitor activity closely.

7. Do any of the senior managers have offshore bank accounts or business interests?

The organization should require senior managers to file annual financial disclosure reports and explain the purpose of any offshore bank accounts or business interests.

8. Are any key employees experiencing financial pressures, such as debts, gambling, medical bills, or divorce?
Key employees who are experiencing financial pressures represent a potential fraud risk to the company and should be monitored by management. Employee assistance programs can be made available to help employees with alcohol, drug, and other problems.

9. Do any key employees appear to be living beyond their means?
Management should be observant of signs of employees spending far more than they are earning. It is common for employees who steal to use the proceeds for lifestyle improvements, including expensive cars, extravagant vacations, or expensive clothing.

10. Do any key employees have civil judgments or bankruptcies on record?
Key employees who have civil judgments or bankruptcies on record represent a potential fraud risk to the company and should be monitored by management.

11. Do any key employees have a criminal conviction?
Key employees with known criminal convictions should be subjected to increased review by management for compliance with internal controls and other policies and procedures.

12. Do one or two key employees appear to dominate the company?
If control is centered in the hands of one or two key employees, then those individuals should be under heightened scrutiny for compliance with internal controls and other policies and procedures.

13. Do any key employees have friends or relatives reporting directly to them?
Organizations should prohibit key employees from having friends or relatives report directly to them.

14. Do any of the key employees appear to have a close association with a vendor?
Key employees who have a close association with a vendor should be monitored for potential conflict of interest.

15. Do any key employees have outside business interests that might conflict with their duties at the company?
Key employees should be required to provide annual financial disclosures that list outside business interests. Interests that conflict with the organization's interests should be prohibited.

16. Do any key employees own a portion of any company that does business with this company?
Organizations should require key employees to disclose any potential conflicts of interest and should closely monitor any such conflicts of interest.

17. Has any key employee failed to take vacation?
Requiring key employees to take annual vacations can aid an employer in detecting an ongoing fraud scheme because the employer is more likely to discover a perpetrator running such a scheme when the perpetrator is removed from the scene.

18. Do any key employees have a significant amount of their net worth invested in the company?
Management should subject key employees with a significant amount of their net worth invested in the company to increased review for compliance with internal controls, especially those controls related to financial reporting.

19. Does the company have unusually high debts?
Management should determine the reason for debt levels and monitor internal controls for financial reporting.

20. Is key employee compensation primarily based on company performance?
Organizations should monitor employees whose compensation is based primarily on company performance for compliance with internal controls, especially controls related to financial reporting.

21. Is there an incentive to use inappropriate means to minimize earnings for tax reasons?
Companies should remove any incentive to use inappropriate means to manipulate financial information.

22. Is there excessive pressure to increase the company's stock price?
Excessive pressure to increase the company's stock price can result in management manipulating financial results in order to meet expectations.

23. Has the company recently experienced large operating or investment losses?
Large operating or investment losses can place undue pressure on management to manipulate results in order to cover up the losses.

24. Does the organization have sufficient working capital?

Insufficient working capital can place undue pressure on management to manipulate financial results.

25. Does the organization have sufficient credit?

A lack of sufficient credit can place undue pressure on management to manipulate financial results in order to obtain credit.

26. Is the organization under pressure to report favorable earnings?

Excessive pressure to report favorable earnings can result in management committing fraudulent acts in order to meet expectations.

27. Does the company depend heavily on only a limited number of products or customers?

Dependence on only a limited number of products or customers places a company at greater risk for fraudulent acts to occur.

28. Has the company experienced difficulty in collecting receivables?

Cash flow problems, which are a warning sign of possible fraud, can arise when a company experiences difficulty in collecting receivables.

29. Has the company recently expanded rapidly into new business or product lines?

Rapid expansion into new business or product lines can place tremendous financial pressure on a company.

30. Has the company experienced a reduction in sales volume?

A reduction in sales volume can place undue pressure on management to manipulate financial results.

31. Does the company have strong competitors that are outperforming?

Strong competition can place a company at greater risk for fraudulent acts to occur.

32. Is the company under pressure to sell or merge with another company?

Situational pressures that might lead to fraudulent acts can arise when a company is under pressure to sell or merge with another company.

33. Does the company change auditors often?

A frequent change in auditors is a red flag of fraud.

34. Does the company delay or avoid supplying auditors with the information necessary to complete the audits?

Delaying or avoiding supplying auditors with the information necessary to complete audits is an indicator of fraudulent activity.

35. Does the company have problems with regulatory agencies?

The company should determine the reasons for the problems with regulatory agencies and implement measures to encourage compliance with regulations.

36. Does the company have poor accounting records?

The company should implement proper accounting records.

37. Does the accounting department appear to be inadequately staffed?

The accounting department should be adequately staffed to allow for proper segregation of duties.

38. Does the organization fail to disclose questionable or unusual accounting practices?

Questionable or unusual accounting practices should be disclosed.

39. Does the company have a number of large year-end or unusual transactions?

Large year-end or unusual transactions should be investigated.

40. Does the organization lack an adequate internal audit staff?

The internal audit department should be adequately staffed.

41. Does the organization lack an internal control system, or does it fail to enforce the existing internal controls?

Organizations should establish and enforce an internal control system.

Module #3—Physical Controls to Deter Employee Theft and Fraud

The physical controls assessment questions are designed to assess the probability of a fraudulent event occurring within the organization based on:

- Physical controls in place to control access to accounting records and information
- Physical controls in place to protect the assets of the organization

1. Does the organization conduct pre-employment background checks to identify previous dishonest or unethical behavior?

Before offering employment to an applicant, a company should conduct a pre-employment background check (where permitted by law).

2. Are there policies and procedures that address dishonest or unethical behavior?

The company should document and implement policies and procedures that describe (1) unethical conduct, (2) punishment for engaging in unethical conduct, and (3) how to report unethical conduct.

3. Does management support the ethics and anti-fraud policies?

Senior management sets the tone for ethical conduct throughout the organization. The tone should signal that fraud will not be tolerated.

4. Does the organization educate employees about the importance of ethics and anti-fraud programs?

All employees should receive training on the ethics and anti-fraud policies of the company. The employees should sign an acknowledgment that they have received the training and understand the policies.

5. Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies?

Organizations should provide a system for anonymous reporting of suspected violations of the ethics and anti-fraud policies.

6. Does the organization restrict access to areas containing sensitive documents (e.g., invoices, receipts, journals, ledgers, and checks) and maintain a system for providing an audit trail of access?

Access to areas containing sensitive documents should be restricted to those individuals who need the information to carry out their jobs. Also, an audit trail of access should be maintained.

7. Does the organization restrict access to computer systems with sensitive documents (e.g., accounting software, inventory, and payroll) and create a system to provide an audit trail of access?
Access to computer systems should be restricted to those individuals who need the information to carry out their jobs. Also, an audit trail of access should be maintained.

8. Does the organization restrict access to areas with high value assets, such as shipping, receiving, storerooms, and cash?
Organizations should restrict access to areas with high value assets and should maintain a log of persons accessing such areas.

9. Does the organization use CCTV and recording equipment to monitor entries, exits, areas with sensitive or high value assets, and sales areas?
Entries, exits, areas with sensitive or high value assets, and sales areas can be monitored using CCTV and recording equipment.

10. Does the organization conduct random, unannounced audits of inventory, cash, expense, purchasing, billing, and other accounts by internal or external auditors?
Random, unannounced audits help prevent fraud perpetrators from having time to alter, destroy, and misplace records and other evidence of their offenses.

11. Does the organization use professional loss prevention or security personnel to monitor physical controls?
Professional loss prevention or security personnel can be used to monitor physical controls.

12. Does the organization promptly investigate incidents of suspected or reported fraud?
Promptly investigating incidents of suspected or reported fraud can minimize losses.

Module #4—Skimming Schemes

Skimming schemes include:

- Collecting cash, but not recording the sale
- Collecting cash, keeping a portion of the cash, and underreporting the sale amount
- Collecting a customer's payment, but not crediting the amount to the customer's account
- Collecting cash and holding it in a personal interest-bearing account before depositing it into the company account

1. Is there periodic analytical review of sales accounts using vertical, horizontal, and ratio analysis?
Periodic analytical review of sales accounts using vertical, horizontal, and ratio analysis can highlight discrepancies that point to skimming.

2. Is there periodic review of the inventory and receiving records using statistical sampling?
Periodic review of the inventory and receiving records using statistical sampling can highlight discrepancies that point to skimming.

3. Is there periodic review of the inventory and receiving records using trend analysis?
Periodic review of the inventory and receiving records using trend analysis can highlight discrepancies that point to skimming.

4. Is there periodic review of the inventory and receiving records using physical inventory counts?
Periodic review of the inventory and receiving records using physical inventory counts can highlight discrepancies that point to skimming.

5. Is there periodic review of the inventory and receiving records using verification of shipping and requisition documents?
Periodic review of the inventory and receiving records using verification of shipping and requisition documents can highlight discrepancies that point to skimming.

6. Is there periodic review of inventory accounts for write-offs?
Inventory accounts should be reviewed periodically for write-offs.

7. Is there periodic review of accounts receivable and allowance for uncollectible accounts to look for write-offs of accounts receivable?
Accounts receivable and allowance for uncollectible accounts should be reviewed periodically for write-offs of accounts receivable.

8. Is there periodic review of cash accounts for irregular entries?
Cash accounts should be reviewed periodically for irregular entries.

9. Is the company mail opened by someone other than bookkeepers, cashiers, or other accounting employees who make journal entries?
Company mail should be opened by someone other than bookkeepers, cashiers, or other accounting employees who make journal entries.

10. Do vouchers for credit and sales receipts contain serial numbers?

Vouchers for credit and sales receipts should contain serial numbers.

11. Is the accounts receivable bookkeeper restricted from preparing the bank deposit?

The accounts receivable bookkeeper should be restricted from preparing the bank deposit.

12. Is the accounts receivable bookkeeper restricted from collecting cash from customers?

The accounts receivable bookkeeper should be restricted from collecting cash from customers.

13. Is the accounts receivable bookkeeper restricted from access to the cash receipts?

The accounts receivable bookkeeper should be restricted from access to the cash receipts.

14. Is the cashier restricted from accessing accounts receivable records?

The cashier should be restricted from accessing accounts receivable records.

15. Is the cashier restricted from accessing bank and customer statements?

The cashier should be restricted from accessing bank and customer statements.

16. Is each of the following responsibilities assigned to a separate employee: general ledger entries, cash receipt entries, and accounts receivable billing?

Having different employees perform these tasks helps minimize the potential for the concealment of theft.

17. Does the employee who opens incoming checks place restrictive endorsements on all checks received?

The employee who opens incoming checks should immediately stamp all incoming checks with the company's restrictive endorsement to protect against unintended parties cashing the checks.

18. Does the person who opens the mail prepare a list of all checks and cash received?

A list of all checks and cash received should be prepared and reconciled daily against the bank deposit receipt and the cash receipts report.

19. Does the person who opens the mail deliver all checks and cash to the person responsible for the daily bank deposit?

The person who opens the mail should deliver all checks and cash to the person responsible for the daily bank deposit.

20. Does an employee perform an independent verification of the bank deposit ticket to the remittance list generated by the employee who opened the mail?

An employee should perform an independent verification of the bank deposit ticket to the remittance list generated by the employee who opened the mail.

21. Does the company use a lockbox service for cash receipts?

Lockboxes decrease the potential for fraud and error by reducing employee handling of each transaction.

22. Does the company have a safe with restricted access?

A safe can be used to physically secure excess cash on hand. Access to the safe should be restricted and an access log should be maintained.

23. Is cash deposited daily?

Daily bank deposits should be made so that excess cash does not remain on the premises.

24. Are there pre-numbered cash receipts for cash sales?

Pre-numbered cash receipts should be used for cash sales.

25. Are employees who handle cash bonded?

Employees who handle cash should be bonded in order to protect against theft.

26. Is there a written policy and procedure for turning over delinquent accounts for collection?

The company should document and implement policies and procedures for turning over delinquent accounts for collection.

27. Is the person who handles customer complaints independent of the cashier or accounts receivable function?

The person who handles customer complaints should be independent of the cashier or accounts receivable function.

28. Is physical access to the accounting system restricted to only authorized persons?

Physical access to the accounting system should be restricted to those who require it to perform their job functions.

Module #5—Cash Larceny Schemes

Cash larceny schemes include:

- Stealing cash at the point of sale or register
- Stealing cash receipts posted to sales and receivable journals
- Stealing cash from bank deposits

1. Are cash register totals reconciled to the amount in the cash drawer?

Cash register totals should be reconciled to the amount in the cash drawer. Any discrepancies should be investigated.

2. Is an employee other than the register worker responsible for preparing register count sheets and agreeing them to register totals?

An employee other than the register worker should be responsible for preparing register count sheets and agreeing them to register totals.

3. Is access to registers or the cash box closely monitored? Are access codes kept secure?

Access to registers or the cash box should be closely monitored and access codes should be kept secure.

4. Are customer complaints regarding short change or improper posting handled by someone other than the employee who receives the cash?

Customer complaints regarding short change or improper posting should be handled by someone other than the employee who receives the cash.

5. Are register workers properly supervised?

Register workers should be properly supervised by on-duty supervisors or CCTV recording of register activity.

6. Are CCTV cameras and digital recorders used to monitor register areas?

CCTV cameras and digital recorders can be used to monitor register areas.

7. Is each receivable transaction reviewed for legitimacy and supporting documentation?

Receivable transactions should be reviewed for legitimacy and supporting documentation.

8. Is an independent listing of cash receipts prepared before the receipts are submitted to the cashier or accounts receivable bookkeeper?

An independent listing of cash receipts should be prepared before the receipts are submitted to the cashier or accounts receivable bookkeeper.

9. Does a person independent of the cash receipts and accounts receivable functions compare entries to the cash receipts journals with the bank deposit slips and bank deposit statements?

Companies should assign a person independent of the cash receipts and accounts receivable functions to compare entries to the cash receipts journals with the bank deposit slips and bank deposit statements.

10. Are the cash receipts, cash counts, bank deposits, deposit receipt reconciliations, bank reconciliations, posting of deposits, and cash disbursements duties segregated?

The primary way to prevent cash larceny is to segregate duties.

11. Does an employee other than the cashier or accounts receivable bookkeeper make the daily bank deposit?

Having an employee other than the cashier or accounts receivable bookkeeper make the daily bank deposit is an important segregation of duties that can help to prevent cash larceny.

12. Is job or assignment rotation mandatory for employees who handle cash receipts and accounting duties?

Many internal fraud schemes are continuous in nature and require ongoing efforts by the employee to conceal defalcations. By establishing mandatory job or assignment rotation, the concealment element is interrupted.

13. Are vacations mandatory for employees who handle cash receipts and accounting duties?

Many internal fraud schemes are continuous in nature and require ongoing efforts by the employee to conceal defalcations. By establishing mandatory vacations, the concealment element is interrupted.

14. Are surprise cash counts conducted?

Surprise cash counts help prevent fraud perpetrators from having time to alter, destroy, and misplace records and other evidence of their offenses.

15. Are journal entries made to the cash accounts reviewed and analyzed on a regular basis?
Journal entries made to the cash accounts should be reviewed and analyzed on a regular basis.

16. Does the company use a point of sale (POS) system?
A POS system will allow the organization to gather sales information in a comprehensive and timely format.

17. Does the POS system track perpetual inventory?
The POS system should be configured to track perpetual inventory.

18. Does the POS system track exceptions, such as voids, refunds, no sales, overages, and shortages?
The POS system should be configured to track exceptions, such as voids, refunds, no sales, overages, and shortages.

19. Are register exception reports reviewed on a regular basis?
Register exception reports should be reviewed on a regular basis by management.

20. Are all employees, except for managers, prohibited from making changes to the POS system?
All employees, except for managers, should be prohibited from making changes to the POS system.

21. Is access to the accounts receivable subledger and the general ledger restricted to authorized employees? Does access leave an audit trail?
Access to the accounts receivable subledger and general ledger should be restricted to authorized employees. An audit trail of who accessed the ledgers, including time and date of access, should be kept.

Module #6—Check Tampering Schemes

Check tampering schemes include:

- Forged maker schemes involve forging an authorized signature on a company check.
- Forged endorsement schemes consist of forging the signature endorsement of an intended recipient of a company check.

- Altered payee schemes involve changing the payee designation on the check to the perpetrator or an accomplice.
- Authorized maker schemes occur when employees with signature authority write fraudulent checks for their own benefit.

1. Are unused checks stored in a secure container with limited access?

Blank checks, which can be used for forgery, should be stored in a secure area such as a safe or vault. Security to this area should be restricted to authorized personnel.

2. Are unused checks from accounts that have been closed promptly destroyed?

Companies should promptly destroy all unused checks from accounts that have been closed.

3. Are electronic payments used where possible to limit the number of paper checks issued?

Companies can minimize the possibility of check tampering and theft by using electronic payment services to handle large vendor and financing payments.

4. Are printed and signed checks mailed immediately after signing?

Printed and signed checks should be mailed immediately after signing.

5. Are new checks purchased from reputable check vendors?

All new checks should be purchased from reputable, well-established check producers.

6. Do company checks contain security features to ensure their integrity?

Companies can reduce their exposure to physical check tampering by using checks containing security features, such as high-resolution microprinting, security inks, and ultraviolet ink.

7. Has the company notified its bank to not accept checks over a predetermined maximum amount?

Companies should work in a cooperative effort with banks to prevent check fraud, establishing maximum dollar amounts above which the company's bank will not accept checks drawn against the account.

8. Has the company established positive pay controls with its bank by supplying the bank with a daily list of checks issued and authorized for payment?

One method for a company to help prevent check fraud is to establish positive pay controls by supplying its banks with a daily list of checks issued and authorized for payment.

9. Is the employee who prepares the check prohibited from signing the check?

Check preparation should not be performed by a signatory on the account.

10. Are detailed comparisons made between the payees on the checks and the payees listed in the cash disbursements journal?

Companies should perform detailed comparisons of the payees on the checks and the payees listed in the cash disbursements journal.

11. Are employees responsible for handling and coding checks periodically rotated?

Periodic rotation of personnel responsible for handling and coding checks can be an effective check disbursement control.

12. Are bank reconciliations completed immediately after bank statements are received?

Companies should complete bank reconciliations immediately after bank statements are received. The Uniform Commercial Code states that discrepancies must be presented to the bank within 30 days of receipt of the bank statement in order to hold the bank liable.

13. Are bank statements and account reconciliations independently audited to confirm accuracy?

Bank statements and account reconciliations should be independently audited for accuracy.

14. Are canceled checks independently reviewed for alterations and forgeries?

Canceled checks should be independently reviewed for alterations and forgeries.

15. Are checks for a material amount matched to the supporting documentation?

Checks for material amounts should be matched to the supporting documentation.

16. Are voided checks examined for irregularities and to ensure they haven't been processed?

The list of voided checks should be verified against physical copies of the checks. Bank statements should be reviewed to ensure that voided checks have not been processed.

17. Are missing checks recorded and stop payments issued?

Missing checks might indicate lax control over the physical safekeeping of checks. Stop payments should be issued for all missing checks.

18. Do questionable payees or payee addresses trigger review of the corresponding check and support documentation?

Questionable payees or payee addresses should trigger a review of the corresponding check and support documentation.

19. With the exception of payroll, are checks issued to employees reviewed for irregularities?

Checks payable to employees, with the exception of regular payroll checks, should be closely scrutinized for schemes such as conflicts of interest, fictitious vendors, or duplicate expense reimbursements.

20. Are two signatures required for check issuance?

Requiring dual signatures on checks can reduce the risk of check fraud.

21. Are all company payments made by check or other recordable payment device?

Making payments by check or other recordable payment device can reduce the risk of disbursement frauds.

22. Are handwritten checks prohibited?

Handwritten checks are especially vulnerable to check fraud and should be prohibited.

Module #7—Cash Register Schemes

The following are types of cash register schemes:

- False refund schemes occur when an employee (1) issues a refund for fictitious merchandise and keeps the money or (2) overstates the amount of merchandise returned and skims the excess money.
- False void schemes occur when a register worker retains a customer receipt, processes a fictitious voided sale, and keeps the money.

1. Are refunds, voids, and discounts evaluated on a routine basis to identify patterns of activity among employees, departments, shifts, merchandise, etc.?

Companies should routinely evaluate refunds, voids, and discounts to search for patterns of activity that might signal fraud.

2. Is there a sign posted at the register asking the customer to request and examine a sales receipt?

Signs asking customers to request and examine sales receipts should be posted at registers.

3. Are cash disbursements recorded on a pre-numbered form and reconciled daily?

Cash disbursements should be recorded on pre-numbered forms and reconciled daily.

4. Do the cash disbursement forms have an explanation section or code?

An explanation section or code should be included on cash disbursement forms.

5. Are customers that are involved in voided sales and refunds randomly contacted to verify the accuracy of the transaction?

Customers involved in voided sales and refunds should be randomly contacted to verify the accuracy of the transactions.

6. Is access to the necessary control keys for refunds and voids restricted to supervisors?

Access to the necessary control keys for refunds and voids should be restricted to supervisors.

7. Do void or refund transactions have to be approved by a supervisor and documented?

All void or refund transactions should be approved by a supervisor and documented.

8. Is documentation of void and refund transactions maintained on file?

Documentation of void and refund transactions should be maintained on file.

9. Is missing or altered register tape thoroughly investigated?

Companies should thoroughly investigate any missing or altered register tape.

10. Are gaps in the register tape investigated?

Companies should investigate any gaps in the register tape.

11. Are multiple voids or refunds for amounts just under any review limit investigated?

Multiple voids or refunds for amounts just under review limits should be investigated.

12. Is an employee other than the register worker responsible for preparing register count sheets and comparing them to register totals?

An employee other than the register worker should be responsible for preparing register count sheets and comparing them to register totals.

13. Are customer complaints regarding payment errors thoroughly investigated?

Customer complaints regarding payment errors should be thoroughly investigated.

14. Does each cashier have a separate access code to the register?

Each cashier should be assigned a separate access code to the register.

15. Does each cashier have a separate cash drawer?

Each cashier should have a separate cash drawer.

16. Is an over and short log kept for each person and/or register?

An over and short log should be kept for each person and/or register.

17. Are over and short incidents thoroughly investigated and monitored?

Over and short incidents should be thoroughly investigated and monitored.

18. Are all "no sale" receipts accounted for and attached to a daily cashier's report?

All "no sale" receipts should be accounted for and attached to a daily cashier's report.

19. Is access to the register area restricted to authorized employees and supervisors?

Companies should restrict access to register areas to authorized employees and supervisors.

20. Are all cashiers periodically integrity shopped?

Companies should periodically conduct integrity shopping on all cashiers.

Module #8—Purchasing and Billing Schemes

The following are types of purchasing and billing schemes:

- Shell company schemes occur when an employee submits invoices for payment from a fictitious company controlled by the employee.
- Pay-and-return schemes occur when an employee arranges for overpayment of a vendor invoice and pockets the overpayment amount when it is returned to the company.
- Personal purchase schemes occur when an employee submits an invoice for personal purchases to the company for payment, or when an employee uses a company credit card for personal purchases.

1. Does the organization have a purchasing department?
The organization should have a purchasing department that is separate from the payment function.

2. Is the purchasing department independent of the accounting, receiving, and shipping departments?
The purchasing department should be independent of the accounting, receiving, and shipping departments.

3. Do purchase requisitions require management approval?
Management should approve all purchase requisitions.

4. Do purchase orders specify a description of items, quantities, prices, and dates?
Purchase orders should specify a description of items, quantities, prices, and dates.

5. Are purchase order forms pre-numbered and accounted for?
Purchase order forms should be pre-numbered and accounted for.

6. Does the company maintain a master vendor file?
The company should maintain a master vendor file.

7. Are competitive bids required for all purchases?
Companies should require competitive bids for all purchases.

8. Does the receiving department prepare receiving reports for all items received?
The receiving department should prepare receiving reports for all items received.

9. Does the receiving department maintain a log of all items received?
The receiving department should maintain a log of all items received.

10. Are copies of receiving reports furnished to the accounting and purchasing departments?
Copies of receiving reports should be furnished to the accounting and purchasing departments.

11. Are purchasing and receiving functions separate from invoice processing, accounts payable, and general ledger functions?

Purchasing and receiving functions should be segregated from invoice processing, accounts payable, and general ledger functions.

12. Are vendor invoices, receiving reports, and purchase orders matched before the related liability is recorded?

Companies should match vendor invoices, receiving reports, and purchase orders before recording the related liability.

13. Are purchase orders recorded in a purchase register or voucher register before being processed through cash disbursements?

Purchase orders should be recorded in a purchase register or voucher register before being processed through cash disbursements.

14. Are procedures adequate to ensure that merchandise purchased for direct delivery to the customer is promptly billed to the customer and recorded as both a receivable and a payable?

Companies should implement procedures adequate to ensure that merchandise purchased for direct delivery to the customer is promptly billed to the customer and recorded as both a receivable and a payable.

15. Are records of goods returned to vendors matched to vendor credit memos?

Records of goods returned to vendors should be matched to vendor credit memos.

16. Is the accounts payable ledger or voucher register reconciled monthly to the general ledger control accounts?

The accounts payable ledger or voucher register should be reconciled monthly to the general ledger control accounts.

17. Do write-offs of accounts payable debit balances require approval of a designated manager?

Write-offs of accounts payable debit balances should require approval of a designated manager.

18. Is the master vendor file periodically reviewed for unusual vendors and addresses?

The master vendor file should be reviewed periodically for unusual vendors and addresses.

19. Are vendor purchases analyzed for abnormal levels?

Vendor purchases should be analyzed for abnormal levels.

20. Are control methods in place to check for duplicate invoices and purchase order numbers?

Companies should implement control methods to check for duplicate invoices and purchase order numbers.

21. Are credit card statements reviewed monthly for irregularities?

Credit card statements should be reviewed monthly for irregularities.

22. Are vendors with post office box addresses verified?

All vendors with post office box addresses should be verified.

23. Are voucher payments reviewed regularly for proper documentation?

Voucher payments should be reviewed regularly for proper documentation.

24. Is access to the accounts payable subledger and the general ledger restricted? Does access create an audit trail?

Access to the accounts payable subledger and the general ledger should be restricted and an audit trail should be created.

Module #9—Payroll Schemes

The following are types of payroll schemes:

- Ghost employee schemes occur when a person not employed by the company is on the payroll.
- Overpayment schemes occur when a company pays an employee based on falsified hours or rates.
- Commission schemes occur when the amount of sales made or the rate of commission is fraudulently inflated.

1. Is the employee payroll list reviewed periodically for duplicate or missing government identification numbers?

Organizations should check the employee payroll list periodically for duplicate or missing government identification numbers, such as Social Security numbers, that might indicate a ghost employee or overlapping payments to current employees.

2. Are personnel records maintained independently of payroll and timekeeping functions?

Personnel records should be maintained independently of payroll and timekeeping functions.

3. Are references checked on all new hires?

Organizations should perform reference checks on all new hires.

4. Are sick leave, vacations, and holidays reviewed for compliance with company policy?

Sick leave, vacations, and holidays should be reviewed for compliance with company policy.

5. Are appropriate forms completed and signed by the employee to authorize payroll deductions and withholding exemptions?

Employees should complete and sign appropriate forms to authorize payroll deductions and withholding exemptions.

6. Is payroll periodically compared with personnel records for terminations?

Payroll should periodically be compared with personnel records for terminations to ensure that terminated employees have been removed from the payroll.

7. Are payroll checks pre-numbered and issued in sequential order?

Payroll checks should be pre-numbered and issued in sequential order.

8. Is the payroll bank account reconciled by an employee who is not involved in preparing payroll checks, does not sign the checks, and does not handle payroll distribution?

The payroll bank account should be reconciled by an employee who is not involved in preparing payroll checks, does not sign the checks, and does not handle payroll distribution.

9. Are payroll registers reconciled to general ledger control accounts?

Payroll registers should be reconciled to general ledger control accounts.

10. Are canceled payroll checks examined for alterations and endorsements?

Canceled payroll checks should be examined for alterations and endorsements.

11. Is access restricted to payroll check stock and signature stamps?

Access to payroll check stock and signature stamps should be restricted.

12. Are payroll withholdings for taxes, insurance, etc., examined to determine if any employees are not having these items deducted from their paychecks?

Payroll checks that do not have withholdings for taxes, insurance, etc., should be investigated.

13. Is the employee payroll list reviewed periodically for duplicate or missing home addresses and telephone numbers?

The employee payroll list should be reviewed for duplicate or missing home addresses and telephone numbers.

14. Is the account information for automatically deposited payroll checks reviewed periodically for duplicate entries?

Account information for automatically deposited payroll checks should be reviewed periodically for duplicate entries.

15. Is an employee separate from the payroll department assigned to distribute payroll checks?

An employee separate from the payroll department should be assigned to distribute payroll checks.

16. Are new employees required to furnish proof of immigration status?

Companies must require new employees to furnish proof of immigration status.

17. Does any change to an employee's salary require more than one level of management approval?

Changes to an employee's salary should require more than one level of management approval.

18. Does overtime have to be authorized by a supervisor?

Overtime should be authorized by a supervisor.

19. Do supervisors verify and sign timecards for each pay period?

Supervisors should verify and sign timecards for each pay period.

20. Are commission expenses compared to sales figures to verify amounts?

Comparing commission expenses to sales figures to verify amounts is an important control procedure that can help to detect payroll fraud.

21. Does someone separate from the sales department calculate sales commissions?

Someone separate from the sales department should calculate sales commissions.

Module #10—Expense Schemes

The following are types of expense schemes:

- Mischaracterized expense schemes occur when an employee requests reimbursement for a personal expense, claiming the expense to be business related.
- Overstated expense schemes occur when an employee overstates the cost of actual expenses and seeks reimbursement.
- Fictitious expense schemes occur when an employee invents a purchase and seeks reimbursement for it.
- Multiple reimbursement schemes occur when an employee submits a single expense for reimbursement multiple times.

1. Are the expense accounts reviewed and analyzed periodically using historical comparisons or comparisons with budgeted amounts?

Companies should periodically review and analyze expense accounts using historical comparisons or comparisons with budgeted amounts.

2. Do employee expense reimbursement claims receive a detailed review before payment is made?

Employee expense reimbursement claims should receive a detailed review before payment is made.

3. Are employees required to submit detailed expense reports?

Employees should be required to submit detailed expense reports containing receipts, explanations, amounts, etc.

4. Is a limit placed on expenses such as hotels, meals, and entertainment?

Companies should place a spending limit on expenses such as hotels, meals, and entertainment.

5. Are receipts required for all expenses to be reimbursed?

Companies should require receipts for all expenses to be reimbursed.

6. Are supervisors required to review and approve all expense reimbursement requests?

All expense reimbursement requests should be reviewed and approved by supervisors.

7. Is there a random authentication of expense receipts and expenses claimed?

A policy requiring the periodic review of expense reports, coupled with examining the appropriate detail, can help deter employees from submitting personal expenses for reimbursement.

Module #11—Theft of Inventory and Equipment

The following are types of schemes that involve the theft of inventory and equipment:

- Fake sale schemes occur when an accomplice of an employee "buys" merchandise, but the employee does not ring up the sale and the accomplice takes the merchandise without making any payment.
- Purchasing schemes occur when an employee with purchasing authority uses that authority to purchase and misappropriate merchandise.
- Receiving schemes occur when an employee misappropriates assets purchased by the company as they are received at the company.
- False shipment schemes occur when an employee creates false sales documents and false shipping documents to make it appear that missing inventory was not actually stolen, but rather sold.
- Misuse of company assets occurs when an employee borrows company assets for personal use without authorization.
- Larceny schemes occur when an employee takes inventory from the company premises without attempting to conceal the theft in the accounting records.

1. Has a recent inventory of company equipment, listing serial numbers and descriptions, been completed?

Companies should inventory company equipment and maintain a list of the equipment, serial numbers, and descriptions.

2. Does the company assign an individual from outside of the department to conduct the department's inventory?

An employee who doesn't work in the department should be assigned to conduct the department's inventory.

3. Are unexplained entries to the inventory records examined for source documentation?

Unexplained entries to the inventory records should be examined for source documentation.

4. Is the company experiencing sizeable inventory increases without comparable sales increases?
Sizeable inventory increases without comparable sales increases might indicate an inventory overstatement fraud scheme and should be investigated.

5. Are analytical reviews of beginning inventory, sales, cost of goods sold, and ending inventory conducted periodically to look for unexplained differences?
Analytical reviews of beginning inventory, sales, cost of goods sold, and ending inventory should be conducted periodically. Any discrepancies should be investigated.

6. Is there an unusual volume of inventory adjustments, write-offs, or disposals?
Any unusual volume of inventory adjustments, write-offs, or disposals should be investigated.

7. Does the organization have written inventory instructions and orders?
Organizations should document and implement inventory instructions and orders.

8. Does someone independent of the purchasing, receiving, and warehousing functions physically count the inventory?
Physical inventory counts should be conducted by someone independent of the purchasing, receiving, and warehousing functions.

9. Are pre-numbered inventory tags used?
Pre-numbered inventory tags should be used.

10. Are the inventory tags controlled and accounted for?
Inventory tags should be controlled and accounted for.

11. Do the inventory procedures prevent double counting?
Organizations should implement inventory procedures that prevent double counting.

12. Are inventory counts subject to independent recounts?
Inventory counts should be subject to independent recounts.

13. Is the inventory reasonably identifiable for proper classification in the accounting system, such as description, condition, or stage of completion?
The inventory should be reasonably identifiable for proper classification in the accounting system, such as description, condition, or stage of completion.

14. Are differences between physical counts and inventory records investigated before inventory records are adjusted?
Differences between physical counts and inventory records should be investigated before inventory records are adjusted.

15. Is scrap inventoried and is scrap disposal accounted for?
Scrap should be inventoried and scrap disposal should be accounted for.

16. Are the following duties segregated: requisition of inventory, receiving of inventory, disbursement of inventory, writing off of inventory as scrap, and receipt of proceeds from the sale of scrap inventory?
The following duties should be segregated: requisition of inventory, receiving of inventory, disbursement of inventory, writing off of inventory as scrap, and receipt of proceeds from the sale of scrap inventory.

17. Is a receiving report prepared for all purchased goods?
A receiving report should be prepared for all purchased goods.

18. Are copies of receiving reports sent directly to the purchasing and accounting departments?
Copies of receiving reports should be sent directly to the purchasing and accounting departments.

19. Is the receiving department provided with a copy of the purchase order on all items to be received?
The receiving department should be provided with a copy of the purchase order on all items to be received.

20. Are partial shipments annotated on purchase orders or attached as separate sheets?
Partial shipments should be annotated on purchase orders or attached as separate sheets.

21. Are overage, shortage, and damage reports completed and sent to the purchasing and accounting departments?

Overage, shortage, and damage reports should be completed and sent to the purchasing and accounting departments.

22. Are quantities of materials received counted and compared to purchase orders?

Quantities of materials received should be counted and compared to purchase orders.

23. Is there a written policy allowing management to inspect all desks, file cabinets, and other containers on company property?

Companies should document and implement a written policy allowing management to inspect all desks, file cabinets, and other containers on company property.

24. Is there an equipment removal authorization policy requiring written management approval to remove any company equipment from the company premises?

Companies should document and implement an equipment removal authorization policy requiring written management approval to remove any company equipment from the company premises.

25. Is there a policy requiring the inspection of packages, boxes, and other containers before they leave the company premises?

Companies should document and implement a policy requiring the inspection of packages, boxes, and other containers before they leave the company premises.

26. Is the removal of trash and trash receptacles periodically monitored?

Companies should periodically monitor the removal of trash and trash receptacles.

27. Are the shipping and receiving areas adequately supervised to prevent theft?

Shipping and receiving areas should be adequately supervised to prevent theft.

28. Are high value items stored in secure or continuously monitored areas?

High value items should be stored in secure or continuously monitored areas.

29. Is the shipping function separate from the purchasing and inventory functions?

The shipping function should be separate from the purchasing and inventory functions.

30. Are shipping documents pre-numbered and accounted for?
Shipping documents should be pre-numbered and accounted for.

31. Are shipping orders matched with sales orders and contracts?
Shipping orders should be matched with sales orders and contracts to prevent inventory and vendor schemes.

32. Are shipments of goods required to have authorized sales orders and contracts prior to shipping?
Shipments of goods should be required to have authorized sales orders and sales contracts prior to shipping.

33. Are shipping documents forwarded directly to the accounting department for recording inventory reduction and cost of sales?
Shipping documents should be forwarded directly to the accounting department for recording inventory reduction and cost of sales.

Module #12—Theft of Proprietary Information
Theft of proprietary information involves theft or disclosure of confidential or trade secret information for financial gain.

1. Are there policies and procedures addressing the identification, classification, and handling of proprietary information?
The company should implement policies and procedures addressing the identification, classification, and handling of proprietary information.

2. Are employees who have access to proprietary information required to sign nondisclosure agreements?
Employees who have access to proprietary information should be required to sign nondisclosure agreements.

3. Are employees who have access to proprietary information required to sign noncompete agreements to prevent them from working for competitors within a stated period of time and location?
Employees who have access to proprietary information should be required to sign noncompete agreements to prevent them from working for competitors within a stated period of time.

4. Are employees provided with training to make them aware of proprietary information, their responsibility to protect the information, and the company policies and procedures relating to proprietary information?

Employees should be provided with training to make them aware of proprietary information, their responsibility to protect proprietary information, and company policies and procedures relating to proprietary information.

5. Is there an established procedure to identify what information should be classified as sensitive and for how long?

Companies should implement a procedure to identify what information should be classified as sensitive and for how long.

6. Are sensitive documents properly classified and marked as confidential?

Sensitive documents should be properly classified and marked as confidential.

7. Is sensitive information properly secured when not being used?

Sensitive information should be properly secured when not being used.

8. Is access to sensitive information physically controlled and accounted for?

Access to sensitive information should be physically controlled and accounted for.

9. Is sensitive information promptly destroyed when it is no longer needed?

Organizations should promptly destroy sensitive information when it is no longer needed.

10. Are compromises to the security of proprietary information promptly investigated to determine the source?

Companies should promptly investigate any compromises to the security of proprietary information to determine the source.

11. Are employees required to use screensaver and/or server passwords to protect unattended computer systems?

Employees should be required to use screensaver and/or server passwords to protect unattended computer systems.

12. Are confidential documents shredded when discarded?

Confidential documents should be shredded when discarded.

Module #13—Corruption

The following are types of schemes that involve corruption:

- Bribery schemes involve the offering, giving, receiving, or soliciting of a thing of value to influence a business decision.
- Kickback schemes occur when vendors make undisclosed payments to employees of purchasing companies in order to enlist the employees in overbilling schemes.
- Bid-rigging schemes occur when an employee fraudulently assists a vendor in winning a contract through the competitive bidding process.
- Economic extortion schemes occur when an employee demands payment from a vendor for decisions made in the vendor's favor. Refusal to pay the extorter results in harm to the vendor.
- Illegal gratuities schemes involve giving or receiving something of value to reward a business decision.

1. Is there a company policy that addresses the receipt of gifts, discounts, and services offered by a supplier or customer?

Organizations should implement a policy that addresses the receipt of gifts, discounts, and services offered by a supplier or customer.

2. Is there an established bidding policy?

Organizations should establish a bidding policy.

3. Are purchases reviewed to detect out of line costs?

Organizations should review purchases for costs that are out of line.

4. Are purchases reviewed to identify favored vendors?

Purchases should be reviewed to identify favored vendors.

5. Are purchases reviewed to identify excessive amounts?

Purchases should be reviewed and any excessive amounts should be investigated.

6. Are pre-bid solicitation documents reviewed for any restrictions on competition?

Pre-bid solicitation documents should be reviewed for any restrictions on competition.

7. Are bid solicitation packages numbered and controlled?

Bid solicitation packages should be numbered and controlled.

8. Is communication between bidders and purchasing employees restricted?

Companies should restrict and monitor communication between bidders and purchasing employees.

9. Are the bids received kept confidential?

All bids received should be kept confidential.

10. Are bidders' qualifications verified?

Companies should verify bidders' qualifications.

11. Are contracts awarded based on predetermined criteria?

Companies should establish predetermined criteria upon which to award contracts.

12. Are purchasing account assignments rotated?

Periodic rotation of purchasing account assignments can be an effective corruption control.

13. Are vendors surveyed periodically regarding company purchasing practices?

Organizations should periodically survey vendors regarding company purchasing practices.

Module #14—Conflicts of Interest

The following are types of schemes that involve conflicts of interest:

- Purchase schemes involve the overbilling of a company for goods or services by a vendor in which an employee has an undisclosed ownership or financial interest.
- Sales schemes involve the underselling of company goods by an employee to a company in which the employee maintains a hidden interest.

1. Are there periodic comparisons of vendor information with employee information, such as addresses and telephone numbers?

Organizations should conduct periodic comparisons of vendor information with employee information, such as addresses and telephone numbers.

2. Are vendors who employ former company employees under increased scrutiny?

Vendors who employ former company employees should be under increased scrutiny for potential conflicts of interest.

3. Does the organization have a reporting procedure for personnel to report their concerns about vendors receiving favored treatment?

Organizations should provide personnel with a confidential system for reporting concerns about vendors receiving favored treatment.

4. Are employees required to complete an annual disclosure document that includes business ownership, income, and investment information?

Employees should be required to provide annual disclosures that list business ownership, income, and investment information.

5. Does the organization require vendors to sign an agreement allowing vendor audits?

Organizations should require vendors to sign an agreement allowing vendor audits.

6. Are vendor audits conducted by someone independent of the purchase, sales, billing, and receiving departments?

Vendor audits should be conducted by someone independent of the purchase, sales, billing, and receiving departments.

Module #15—Fraudulent Financial Reports

The following are schemes involving fraudulent financial reports:

- Fictitious revenue schemes involve recording fictitious revenue from the sale of goods or services.
- Improper timing schemes involve recording revenues or expenses in improper accounting periods.
- Understating liabilities schemes involve concealing or understating liabilities and expenses, capitalizing expenses, or expensing capital expenses.
- Improper disclosure schemes involve the improper disclosure of material information, such as contingent liabilities, significant events, management fraud, related-party transactions, or accounting changes.
- Improper asset valuation schemes involve the improper valuation of inventory, accounts receivable, fixed assets, intangibles, or other assets.

1. Are the organization's accounting records in proper form?

Organizations should maintain accounting records in proper form.

2. Does the organization employ an adequate number of accounting employees?
The accounting department should be adequately staffed to allow for proper segregation of duties.

3. Does the organization have an effective internal audit staff?
An effective internal audit staff can focus on high-risk areas for fraud and can identify new vulnerabilities, measure the effectiveness of internal controls, and signal that fraud prevention is a high priority for the company.

4. Are proper internal controls established and maintained?
Organizations should establish and enforce an internal control system.

5. Does the organization embrace the concept of internal controls?
Embracing the concept of internal controls requires that senior managers and employees understand why internal controls are important and what adopting such measures means to them.

6. Are senior managers visible in their support of internal controls?
Senior managers should be visible in their support of internal controls.

7. Are the organization's financial goals and objectives realistic?
Unrealistic financial goals and objectives can result in managers and employees committing fraudulent acts in order to meet them.

8. Does the organization consistently achieve its financial goals and objectives?
Any failure to meet financial goals and objectives should be researched.

9. Is the organization's reported financial performance stable or increasing?
Management should investigate any unstable or decreasing financial performance.

10. Does the company have stable relationships with its banks?
The company should strive to have stable relationships with its banks.

11. Are there unrealistic changes or increases in financial statement account balances?
Management should determine the reasons for any unrealistic changes or increases in financial statement account balances.

12. Are the account balances realistic given the nature, age, and size of the company?
Management should investigate any unrealistic account balances.

13. Do actual physical assets exist in the amounts and values indicated on the financial statements?
An inventory of physical assets should be conducted to verify that the physical assets exist in the amounts and values indicated on the financial statements.

14. Have there been significant changes in the nature of the organization's revenues or expenses?
The organization should determine the reasons for any significant changes in the nature of its revenues or expenses.

15. Do one or a few large transactions account for a significant portion of any account balance or amount?
Situations in which one or a few large transactions account for a significant portion of any account balance or amount should be researched.

16. Are there significant transactions that occur near the end of a period that positively impact results of operations, especially transactions that are unusual or highly complex?
Any significant transactions that occur near the end of a period and positively impact results of operations should be scrutinized for legitimacy, especially if the transactions are unusual or highly complex.

17. Are financial results fairly consistent across periods?
The company should be able to explain any variances in financial results across periods.

18. Is there an inability to generate cash flows from operations while experiencing earnings growth?
Any inability to generate cash flows from operations while experiencing earnings growth should be investigated.

19. Is there significant pressure to obtain additional capital necessary to stay competitive?
Insufficient working capital can place undue pressure on management to manipulate financial results.

20. Are reported assets, liabilities, revenues, or expenses based on significant estimates that involve unusually subjective judgments or uncertainties?
Significant estimates, especially those that involve unusually subjective judgments or uncertainties, should be reviewed for reasonableness.

21. Are reported assets, liabilities, revenues, or expenses based on significant estimates that are subject to potential significant change in the near term in a manner that might have a financially disruptive effect on the organization?

Significant estimates that are subject to potential significant change in the near term in a manner that might have a financially disruptive effect on the organization should be scrutinized.

22. Is the company experiencing unusually rapid growth or profitability, especially when compared with that of other companies in the same industry?

Unusually rapid growth or profitability, especially when compared with that of other companies in the same industry, is a red flag of fraud and should be investigated.

23. Is the organization highly vulnerable to changes in interest rates?

The organization should increase review of its financial reporting during periods of high vulnerability.

24. Are there unrealistically aggressive sales or profitability incentive programs?

Unrealistically aggressive sales or profitability incentive programs can place undue pressure on employees and result in employees committing fraudulent acts in order to meet them.

25. Is there a threat of imminent bankruptcy, foreclosure, or hostile takeover?

A threat of imminent bankruptcy, foreclosure, or hostile takeover places a company at increased risk for fraudulent activity to occur.

26. Is there a high possibility of adverse consequences on significant pending transactions, such as business combinations or contract awards, if poor financial results are reported?

A high possibility of adverse consequences on significant pending transactions, such as business combinations or contract awards, if poor financial results are reported can place extreme pressure on management to manipulate results.

27. Is there a poor or deteriorating financial position when management has personally guaranteed significant debts of the entity?

The existence of a poor or deteriorating financial position when management has personally guaranteed significant debts of the entity can result in management committing fraudulent acts in order to protect itself from financial harm.

28. Does the firm continuously operate on a crisis basis or without a careful budgeting and planning process?
A careful budgeting and planning process can help a firm to monitor progress toward its goals, control spending, and predict cash flow and profit.

29. Does the organization have difficulty collecting receivables or have other cash flow problems?
Management should determine the reasons for any collection or cash flow problems.

30. Is the organization dependent on one or two key products or services, especially products or services that can become quickly obsolete?
Dependence on one or two key products can place tremendous pressure on a company, exposing it to increased risk of fraud.

31. Do the footnotes contain information about complex issues?
Any complex issues should be explained in the footnotes.

32. Are there adequate disclosures in the financials and footnotes?
Generally accepted accounting principles concerning disclosures require that financial statements (1) include all relevant and material information in the financials or footnotes and (2) not be misleading.

FRAUD RISK MANAGEMENT[1]

What Is Risk Management?

Among the numerous available definitions of *risk management*, perhaps the most broadly recognized is that provided by the Committee of Sponsoring Organizations (COSO) for *enterprise risk management*: "a process . . . designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[2]

Risk management involves the identification, prioritization, treatment, and monitoring of risks that threaten an organization's ability to provide value to its stakeholders, whether increasing profitability and shareholder value for a for-profit entity or achieving program-specific goals for a nonprofit or governmental agency. More specifically, risk management balances risk appetite—how much risk management is willing to accept—with the ability to meet the organization's strategic, operational, reporting, and compliance objectives.

The Current State of Risk Management Initiatives

In 2015, the Enterprise Risk Management Initiative released a report on the current state of enterprise risk oversight initiatives.[3] Among the findings outlined in the report were:

- Organizations face an increasing volume and complexity of risks, with 65 percent of survey respondents admitting that they were caught off guard by an operational surprise in the last five years.
- Almost one-quarter of the organizations surveyed had no formal ERM processes in place even though 57 percent of the organizations described their risk culture as "strongly risk averse" or "risk averse."
- For the majority of the organizations surveyed, the board of directors is asking for increased senior involvement in risk oversight.

---

[1] Portions of the material in this chapter are taken from *Managing the Business Risk of Fraud: A Practical Guide*, a resource jointly published by the ACFE, AICPA, and IIA. For more information or to read the full text of this publication, please visit the following website: www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf.

[2] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management—Integrated Framework: Executive Summary*, 2004. www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

[3] Mark Beasely, Bruce Branson, and Bonnie Hancock, *2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities*, 2015. http://erm.ncsu.edu/library/article/current-state-erm-2015.

- In addition to requests from the board of directors, the three most frequently cited factors for increasing senior management involvement in risk oversight are (1) regulator demands, (2) emerging corporate governance requirements, (3) and a desire to better anticipate unexpected risk events.
- While the number of organizations embracing ERM is on the rise, the level of risk management initiatives is still immature based on responses from surveyors, with only 23 percent describing their organization's risk management maturity as "robust" or "mature."
- Only 32 percent of respondents indicated that an individual had been formally assigned to serve as the Chief Risk Officer (CRO) or an equivalent designation.
- While one-third of respondents indicated that their risk inventories are maintained at the enterprise level, more than 70 percent of the organizations did not have defined guidelines or measures on how to assess the probability and impact of risks.
- 43 percent of respondents stated that their organizations either had no structured process for identifying and reporting risk exposures to the board or track risks by silos with minimal reporting of aggregate risk exposures to the board.
- One of the more notable areas needing improvement in risk oversight is the integration of risk management with strategic planning; 36 percent of organizations do not conduct any formal risk assessments of emerging strategic, market, or industry risks.
- Barriers to progress still exist that restrict the effectiveness of a risk management process, with the most common being the belief that "risks are monitored in other ways besides ERM."

Risk Management Frameworks

Every organization faces a unique set of risks based upon its industry, financial condition, regulatory environment, culture, and a host of other factors. Consequently, an entity's risk management program must be tailored to the specifics of the organization for it to be effective. Nevertheless, an established risk management framework can be very helpful in providing guidance and structure in developing such a program. The following are some examples of widely accepted risk management frameworks; however, others exist and might be more applicable to the specifics of particular organizations.

COSO *Enterprise Risk Management—Integrated Framework*

The COSO *Enterprise Risk Management—Integrated Framework* (ERM Framework) is among the most widely recognized risk management frameworks, and it is the chosen framework for implementing risk management processes within many organizations.

COSO's ERM Framework builds upon the five components first identified as part of COSO's *Internal Control—Integrated Framework* and includes an additional three components. The eight components of the ERM Framework are:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

COSO provides the following explanations for each of the eight components:[4]

Internal Environment

The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

Objective Setting

Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives, and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

[4] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management — Integrated Framework: Executive Summary*, 2004. www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

Event Identification

Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

Risk Assessment

Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

Risk Response

Management selects risk responses—avoiding, accepting, reducing, or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

Control Activities

Policies and procedures are established and implemented to help ensure that the risk responses are effectively carried out.

Information and Communication

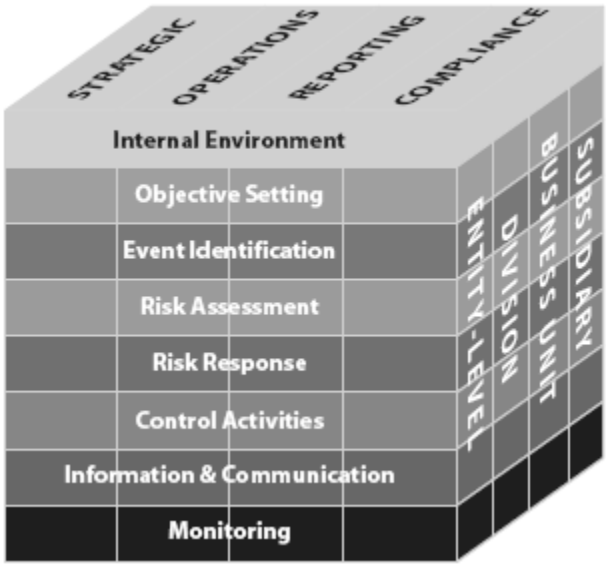
Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

Monitoring

The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Relationship of ERM Framework Components

The ERM Framework presents the relationships of these eight components to each other, as well as to the organization's objectives and operating units, in the form of a three-dimensional matrix, as illustrated here:



(Source: *COSO Enterprise Risk Management—Integrated Framework Executive Summary, 2004*.)

ISO 31000

The International Organization for Standardization (ISO) has developed ISO 31000, a set of international standards providing principles and guidance on risk management. Most organizations with a risk management function that do not follow the COSO ERM model follow the ISO model. Some organizations have developed a customized model that incorporates elements of both the COSO and ISO models.

The ISO 31000 family of standards includes:

- ISO 31000:2009, *Risk Management—Principles and Guidelines*
- ISO/IEC 31010:2009, *Risk Management—Risk Assessment Techniques*, which focuses on risk assessment concepts, processes, and techniques
- ISO Guide 73:2009, *Risk Management Vocabulary*, which includes terms and definitions related to risk management

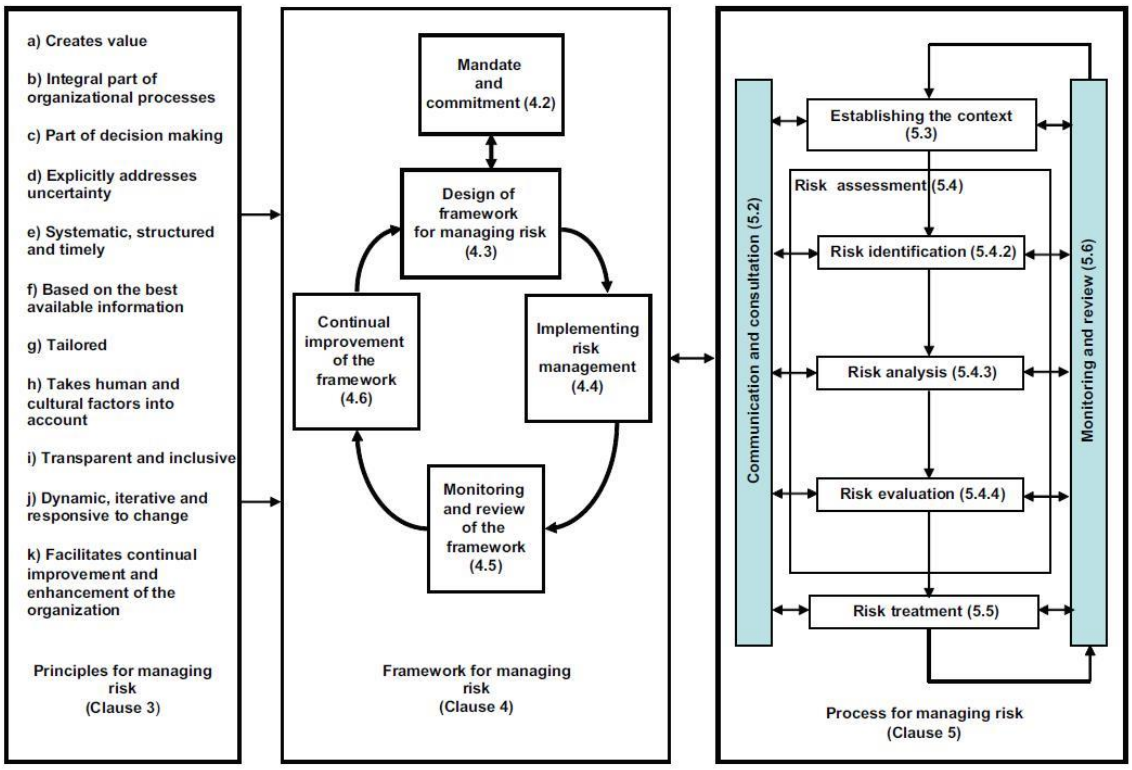
According to ISO, "using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment. … Organizations using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance."[5]

[5] www.iso.org/iso/home/standards/iso31000.htm

ISO 31000 lays out the following 11 principles of an effective risk management program.

- Creates value
- Is an integral part of organizational processes
- Is part of decision making
- Explicitly addresses uncertainty
- Is systematic, structured, and timely
- Is based on the best available information
- Is tailored to the organization
- Takes human and cultural factors into account
- Is transparent and inclusive
- Is dynamic, iterative, and responsive to change
- Facilitates continual improvement and enhancement of the organization

The standard also provides guidance on developing both a framework and a process for managing risk that is based on those principles. The standard shows the relationship between these components as illustrated in the following diagram:



(Source: ISO 31000:2009, *Risk Management—Principles and Guidelines*)

Integrating Anti-Fraud Initiatives into Risk Management

The spectrum of risks faced by organizations is extremely broad, encompassing natural disasters, global economic shifts, product obsolescence, employee strikes, new competitors, regulatory changes, incompetent management, and everything in between.

However, every organization is vulnerable to fraud—no entity is immune to that risk. The key to reducing this vulnerability is to be consciously aware of and realistic about the organization's weaknesses. Only then can management establish mechanisms that effectively prevent or detect fraudulent activities. In fact, it is those organizations that deny the true possibility of fraud that are placing themselves at the greatest risk.

The Business Case for Managing Fraud Risk

According to the ACFE's 2014 *Report to the Nations on Occupational Fraud and Abuse*, the typical organization stands to lose an estimated 5 percent of its annual revenues to fraud. That's 5 percent of gross income lost without any direct benefit to the business. Furthering the damage, most organizations recover very little, if any, of the amounts lost to fraud. Additionally, if and when a fraud is detected, the organization must invest additional time and money in investigating how it happened, pursuing action against the perpetrator, and taking steps to remediate the system weaknesses that allowed the malfeasance to occur. The results of a poor fraud risk management program have brought about the downfall of countless organizations.

The cost/benefit analysis of investing in fraud risk management should be clear: It is much more cost effective to proactively address fraud risks than to suffer preventable fraud and spend valuable resources to detect, investigate, prosecute, and clean up after it. In other words, stopping fraud before it occurs directly increases the organization's bottom line.

In addition to the financial benefits, effective fraud risk management:

- Sends a clear message that fraudulent actions will be proactively sought out and will not be tolerated
- Demonstrates a sound business strategy to employees and third parties
- Enhances the organization's public image and reputation
- Promotes goodwill with other organizations and the general public
- Ensures compliance with certain laws and regulations

Even the most honest and trusted employees can one day become dishonest. Lives change, needs change, situations change, motivations change, and rationalizations change. Effective fraud risk management is a continuous process of reviewing and addressing the significant risks of fraud.

Who Is Responsible for Managing Fraud Risk?

According to *Managing the Business Risk of Fraud: A Practical Guide*, "personnel at all levels of the organization—including every level of management, staff, and internal auditors, as well as the organization's external auditors—have responsibility for dealing with fraud risk."

While everyone within the organization has the duty to help fight fraud, the practical implementation of fraud risk management must start somewhere. The organization must have a team of specific individuals—or a dedicated department—that is made explicitly responsible for executing, monitoring, and ensuring the success of its fraud management initiatives.

Depending on the size and structure of the organization, the following individuals and groups may have key roles in ensuring effective fraud risk management:

- Executive management
- The audit committee
- The investigations group
- The compliance function
- The controller's group
- Internal audit
- IT
- Security
- The legal department
- Human resources

Without clear assignment of the fraud-related roles and responsibilities to the parties overseeing the organization, any fraud risk management program will be ineffective. The following discussion highlights the duties of specific parties involved in the fraud risk management process.

Board of Directors

To ensure that the fraud risk management program is effective in both operation and design, it must be fully embraced by those charged with governing and overseeing the organization. Specifically, the board of directors must recognize the true and specific risks of fraud to the organization, as well as their potential impact, and respond by:

- Setting an appropriate tone and realistic expectations of management to enforce an anti-fraud culture
- Raising awareness of the risks of fraud throughout the organization
- Developing a strategy to assess and manage fraud risks that aligns with the organization's risk appetite and strategic plans
- Overseeing the organization's fraud risk management activities

Audit Committee

As a sub-group of the board of directors, the audit committee is often delegated oversight of the organization's financial, accounting, and audit matters. As part of this responsibility, the committee must take an active role in overseeing the assessment and monitoring of the organization's fraud risks. This involves:

- Receiving regular reports on the status of reported or alleged fraud
- Meeting regularly with key internal parties (e.g., the chief audit executive or other senior financial persons) to discuss identified fraud risks and the steps being taken to prevent and detect fraud
- Understanding how internal and external audit strategies address fraud risk
- Providing external auditors with evidence that the audit committee is dedicated to effective fraud risk management
- Engaging in open conversations with external auditors about any known or suspected fraud

Management

Management holds the primary responsibility for designing, implementing, monitoring, and improving the fraud risk management program. As part of this, management should:

- Be intimately familiar with the organization's fraud risks.
  - Perform (or oversee the performance of) a fraud risk assessment and update it regularly.
  - Form a risk management team within the organization to stay actively abreast of emerging risks.

- Ensure that the organization has specific and effective internal controls in place to prevent and detect fraud. This function may be performed by an outsourced firm if internal resources are unavailable.
  - Perform a cost/benefit analysis so as not to "over-control" the organization such that important business processes cannot occur or will suffer.
  - Perform routine checks to ensure that internal controls are adequate and performing as intended.
- Set a tone at the top and monitor the company culture to ensure that it appropriately supports the organization's fraud prevention and detection strategies. Senior management must exude ethics for staff to be inspired and feel obligated to follow suit.
- Clearly communicate—both in words and actions—that fraud is not tolerated.
  - Send regular blast voice mails and/or emails to staff about the importance of ethics and controls.
  - Give annual refresher training on company policies and expectations.
  - Discuss expectations at new hire orientation training so that staff understands expectations from the very beginning.
- Take seriously all reports of fraud and undertake investigations for any such reports deemed reliable. Management might not be the optimal group to perform investigations but should ensure investigations occur for all allegations of fraud deemed reliable. Investigations might be best performed by other departments or outsourced companies.
  - Ensure open channels for communication of fraudulent activity to investigators.
  - Implement mechanisms through which fraud allegations can be reported confidentially and are handled according to a defined protocol.
- Punish perpetrators of discovered fraud appropriately. Punishing perpetrators reinforces the culture of ethics and the fact that fraud will not be tolerated.
- Take any steps necessary to remediate weaknesses that allowed frauds to occur.

Staff Members

According to *Managing the Business Risk of Fraud*, all levels of staff, including management, should:

- Have a basic understanding of fraud and be aware of the red flags.
- Understand:
  - Their roles within the organization's internal control framework
  - How their job procedures are designed to manage fraud risks
  - When noncompliance might create an opportunity for fraud to occur or go undetected

- Read and understand policies and procedures such as the organization's fraud policy, code of conduct, whistleblower policy, procurement manuals, etc.
- As required, participate in:
  - Creating a strong control environment
  - Designing and implementing fraud control activities
  - Monitoring activities
- Report suspicions or incidences of fraud.
- Cooperate in investigations.

Internal Auditors

Part of the internal audit function's role is to evaluate and improve the effectiveness of the organization's risk management, control, and governance processes. Clearly, each of these organizational components—risk management strategies, internal controls, and governance processes—serves an important function in the fight against fraud. According to *Managing the Business Risk of Fraud*, internal auditors should:

- Devote adequate time and attention to assessing—so that they can provide objective assurance to the board and management—that fraud controls are sufficiently designed and operating effectively to address identified fraud risks.
- Review the comprehensiveness and adequacy of the fraud risks identified by management (giving particular consideration to fraud risks related to management override of controls).
- Consider the organization's fraud risk assessment when developing its audit plan.
- Periodically review management's fraud risk management strategy and capabilities.
- Communicate regularly with those responsible for the fraud risk assessment to ensure all fraud risks have been appropriately considered.
- Maintain an attitude of professional skepticism and be on guard for signs of fraud.
- Take an active role in supporting the organization's ethical culture.

Additionally, depending on the organization's structure and the internal audit charter, the internal audit function may be explicitly responsible for investigating suspected fraud, analyzing factors that contributed to the occurrence of known fraud, recommending improvements to anti-fraud controls, monitoring incoming reports of suspected fraud, and providing ethics training for employees.

Forming the Fraud Risk Management Team

In formulating the fraud risk management team, a cross-departmental approach allows a diverse skill set and holistic perspective to be incorporated into the anti-fraud team's initiatives. However, the group should have a designated leader—such as the chief compliance officer or chief ethics officer—to guide the team and monitor achievement of its objectives. Additionally, each member's roles and responsibilities must be clearly outlined and explicit expectations must be set.

The Objectives of a Fraud Risk Management Program

Fraud risk management programs must address fraud before, during, and after it occurs. Consequently, effective fraud risk management programs must incorporate policies and procedures designed to do all of the following:

- Prevent fraud.
- Detect fraud.
- Respond to identified fraud.

Fraud Prevention

Fraud prevention activities focus on proactively identifying and assessing fraud risks and taking steps to address those risks. These are the first line of defense against fraud in the organization and generally include policies, procedures, training, and communication.

Fraud Detection

Fraud detection activities seek to identify fraud occurrences as soon as possible after they begin in order to limit the damage done.

Fraud Response

Responding to suspected fraud occurrences includes:

- Investigating the allegation to determine the party or parties responsible, the means of the infraction, and the extent of the resulting damage
- Punishing the perpetrator, whether through employment sanctions or legal action
- Remediating the control weaknesses that allowed the fraud to be undertaken
- Rebuilding stakeholders' confidence in the organization

Steps in Developing a Fraud Risk Management Program

Define Program Objectives

While the broad objectives of a fraud risk management program include the prevention of, detection of, and response to fraud, because the fraud risks and strategic initiatives of each organization differ, the detailed objectives of the fraud risk management program should be tailored to the organization's specific needs and goals.

Like any corporate initiative, without a clear, explicit definition of what the organization intends to accomplish through its fraud risk management program, the program will have limited or no success. Consequently, management must balance the following factors in determining the program's objectives:

- The investment in anti-fraud controls
- The prevention of frauds that are material in nature and/or amount
- Management's risk appetite

For example, a "zero-tolerance" approach—which generally indicates that management will take action against any fraud, regardless of size or nature—prioritizes the prevention of frauds over the costs involved, and indicates a very low appetite to take on fraud risks.

Define Risk Appetite

No fraud risk management program will prevent all fraud; some risk of fraud will always remain. Consequently, an important component in defining the objective of the fraud risk management program is determining management's risk appetite. Without an adequate understanding of just how much risk those charged with governance are willing to accept, any stated objectives of the fraud risk management program will be inaccurate.

Risk appetite can be measured and expressed either qualitatively—low, medium, or high, for example—or quantitatively, using a numeric scale. For example, a company's management might decide that it prefers to reduce the residual risk of fraud down to a "low" level, implying a desire for strong controls and monitoring of such controls over a particular area of the business. Another company might decide that any risk rated three or higher is unacceptable (for a risk scale between one and five). Risk appetite can also be broken down into specific types or sources of fraud, which allows for prioritization of fraud risk management strategies based on the assessed components.

Whatever means of measuring risk appetite that management chooses to use, the results should be a continuous focus on developing an effective fraud risk management strategy.

Examine Previous Fraud Incidents

Another helpful starting point in determining the fraud risk management strategy is to examine previous occurrences of fraud and explore how management's ideal fraud risk management program would have prevented, detected, and responded to them. In examining such incidents, management should consider the factors that allowed such frauds to occur. Specifically, management should assess the following:

- Were the fraud risks not fully understood?
- Were internal controls insufficient in design or operation?
- Were the applicable internal controls overridden?
- Were there any warning signs that were missed?

Such analysis can be extremely useful in guiding management's definition of program objectives and determining which areas of the fraud risk management program will need significant attention.

Assess Fraud Risks

Before a program to effectively manage fraud risks can be developed, management must first identify and thoroughly understand the risks faced by the organization. Any program components developed based on an insufficient understanding of the company's specific fraud risks will likely be ineffective in preventing fraud, a waste of resources, and potentially counter-productive.

The fraud risk assessment process, although cumbersome and time-consuming, is very important in developing a fraud risk management program. There are many ways to go about this process, but the overall goal is to detail the fraud risks to the organization and determine the likelihood of their occurrence, as well as their potential damage. Only after the risks have been defined and well-understood can management make an educated decision about how best to reduce the risks, while taking into consideration the productivity and costs to the business.

The previous chapter on "Fraud Risk Assessment" contains more detailed information on how and why such assessments should be conducted.

Design Program Components

The specific components of the fraud risk management program must be designed, taking into consideration the organization's culture, operating environment, and specific risks, as well as management's defined program objectives and risk appetite. Additionally, the design of the program components should be undertaken by individuals with adequate knowledge of both fraud risk management tactics in general and the company's specific risks and operations.

Components of the customized fraud risk management program will generally include:

- Initiatives to increase the anti-fraud culture and tone of the organization
- Fraud prevention controls
- Fraud detection controls
- Formalized policies, processes, and procedures for investigating and responding to known instances of fraud

Implement Program Components

Even the best-designed fraud risk management program will be worthless if it is not implemented effectively. For example, the ethical tone of the organization must be clearly, openly, and consistently demonstrated in the actions of upper management, rather than simply being mandated to lower-level employees through ethics policies that do not apply to those at the top. Likewise, any internal controls will only work to prevent or detect fraud if those responsible for performing and monitoring the control functions are effectively fulfilling their duties.

Communicate Expectations

The purpose and expectations of the fraud risk management program must be communicated, both formally and informally, to employees at all levels throughout the organization. Employees who are told to perform a certain task a certain way will likely not understand the full impact of the anti-fraud control if they are not educated about how that task helps protect the organization from being defrauded. Additionally, employees must be informed about their responsibility to report suspected fraud and be empowered with the means and confidence to do so without concern for retaliation.

Ensure Compliance

The fraud risk management program must include mechanisms specifically designed to monitor, identify, and address breaches in compliance. Such breaches might include failures

in the design or operation of anti-fraud controls, as well as outright occurrences of fraud. A specific individual or team should be designated as responsible for monitoring compliance with the fraud risk management program and for handling suspected instances of noncompliance. Formal sanctions for intentional noncompliance must be well-publicized and carried out in a consistent and firm manner.

Identify and Investigate Violations

Even the most well-designed fraud risk management program will not thwart all attempts to defraud the organization. Consequently, organizations must have in place clearly defined processes and protocols for investigating suspected frauds.

Measure, Evaluate, and Report the Program's Performance and Effectiveness (Benchmarking)

The success of any initiative depends greatly on management's ability to adapt the program to its changing needs and to new information that is uncovered. Consequently, the fraud risk management program's performance will need to be periodically evaluated, with the results of such evaluations reported to senior management and the board of directors. Benchmarking against internal expectations as well as best practices can be extremely helpful in measuring the program's effectiveness.

Fraud Risk Management Program Components

Most organizations have controls designed to prevent and detect fraud; many also have written policies and procedures, such as a code of ethics or fraud investigation policy, that reinforce an anti-fraud stance. However, a proactive fraud risk management program is greatly benefited by formally compiling these activities and documents, assessing and refining how they work together, and communicating the totality of the program to employees, management, directors, vendors, customers, and other stakeholders.

According to *Managing the Business Risk of Fraud*, the following ten components are important to effectively manage fraud risk:

- Commitment
- Fraud awareness
- Affirmation process
- Conflict disclosure
- Fraud risk assessment

- Reporting procedures and whistleblower protection
- Investigation process
- Corrective action
- Process evaluation and improvement (quality assurance)
- Continuous monitoring

Commitment

The board of directors and senior management should communicate, in writing, their commitment to proactively preventing, detecting, and addressing fraud. This communication can be made as part of the organization's written statement of values and principles, as part of the code of conduct, or in a separate short document, such as a letter, that is provided to all employees, vendors, and customers.

The statement of commitment should:

- Be endorsed or authored by a senior executive or board member.
- Be provided to employees as part of the orientation process and be reissued periodically.
- Stress the importance of fraud risk mitigation.
- Acknowledge the organization's vulnerability to fraud.
- Establish the responsibility of each person within the organization to support fraud risk management efforts.
- Reinforce management's "no tolerance" stance on fraudulent behavior.

Fraud Awareness

To help convey fraud risk management expectations and to effectively prevent fraud, management should include a formal fraud awareness program as part of the fraud risk management initiative. The fraud awareness program should include periodic assessment, training, and frequent communications that:

- Define fraud.
- Describe pertinent fraud risks.
- Provide examples of types of fraud that might occur.
- Identify potential perpetrators of fraud.

When designing such programs, management should consider:

- Who should attend
- The frequency and length of training sessions
- Cultural sensitivities

- The inclusion of guidance on how to solve ethical dilemmas
- The appropriate delivery method(s)
- The training needs of individuals at different levels of authority (i.e., staff, supervisors, upper management, and board members)

Affirmation Process

An affirmation process is the requirement for directors, employees, and contractors to explicitly affirm (typically via electronic or manual signature) that they have read, understood, and complied with the organization's code of conduct, fraud control policy, and other such documentation that supports the fraud risk management program. In determining whether to enact an affirmation process, management must weigh any potential legal issues involved with having such a process with the increased fraud risk of not having one.

If an affirmation process is enacted, it should include consistent sanctions for individuals who refuse to sign-off on the acknowledgement. Additionally, the affirmation process might include requiring individuals to acknowledge that they have a fiduciary duty to report any known instances of fraud.

Ways to extend the affirmation process for further fraud protection include:

- Incorporating terms in contracts that require vendors to agree to abide by the organization's code of conduct
- Requiring senior management to sign a code of conduct specific to higher-level employees
- Requiring vendors to sign separate agreements on specific topics, such as confidentiality or use of company technologies

Conflict Disclosure

An important component of a fraud risk management program involves a mechanism for directors, employees, and contractors to self-disclose to the organization any potential or actual conflicts of interest.

All disclosures of potential or actual conflicts of interest—as well as management's decision regarding the situation—should be documented and reported to legal counsel. Additionally, any waivers of conflict of interest policy provisions should be—and, under certain securities regulations, might be required to be—disclosed. Management should also consider the

benefits of and any legal requirements for disclosing the organization's code of conduct, anti-fraud policy, and related statements to the public.

Fraud Risk Assessment

As previously discussed, a thorough fraud risk assessment that accurately identifies the organization's fraud risks is the foundation for an effective fraud risk management program. Such an assessment is not a onetime endeavor, but rather should be performed on a systematic and recurring basis. In addition, the assessment should consider all relevant fraud schemes and scenarios, and the results should be used to map mitigating controls to those fraud schemes and scenarios determined to put the organization at risk.

The previous chapter on "Fraud Risk Assessment" contains more detailed information on how and why such assessments should be conducted.

Reporting Procedures and Whistleblower Protection

Fraud is detected more often by tips than by any other means. Consequently, to be fully effective, a fraud risk management program must include mechanisms for receiving fraud allegations from employees and other parties.

The organization's reporting policies and procedures should:

- Be thoroughly and openly communicated to employees, customers, and vendors.
- Set the expectation that suspected fraud should be immediately reported.
- Clearly define and communicate the channels to use to make such reports (e.g., a hotline, ombudsman, or specific page on the organization's website).
- Provide explicit support and protection for whistleblowers.

Investigation Process

Part of an effective fraud risk management program is a formal investigation process that is performed when suspected fraud is reported. The protocol for this process should be properly documented, and should include consideration of:

- Who should conduct the investigation (internal parties or outside experts)
- Rules of evidence
- Chains of custody
- Reporting mechanisms
- Regulatory requirements
- Legal actions

Corrective Action

Organizations should enact policies that reflect the consequences and processes for individuals who commit or condone fraudulent activity. Such consequences might include termination of employment (or a contract, for non-employees), reporting of the incident to law enforcement or regulatory authorities, and pursuit of civil or criminal action against the perpetrator(s). It is important for management to ensure that any corrective action taken is applied consistently for all involved in the fraudulent act.

The organization should also have specific policies in place to identify and remediate any control deficiencies that allowed fraudulent conduct to occur.

Process Evaluation and Improvement (Quality Assurance)

Management should determine and document specifically how it will periodically evaluate the fraud risk management program's effectiveness. It should also include specific provisions for monitoring changes to the program, obtaining measurements of program effectiveness, and analyzing statistics, benchmarks, resources, and survey results. The results of this process evaluation should be used by the board and management to improve the fraud risk management program.

Continuous Monitoring

All aspects of the fraud risk management program should be continuously reviewed and revised to ensure they are addressing the organization's current needs and risks, as well as to reflect management's ongoing commitment to preventing, detecting, and investigating fraud.

ETHICS FOR FRAUD EXAMINERS

As a fraud examiner, the decisions you make will be extremely important to your client or company, as well as to the individuals you might be called upon to investigate. Therefore, Certified Fraud Examiners are held to a very high ethical standard. The following material is designed to accomplish more than a mere recitation of rules of professional ethics for fraud examiners; it also contains discussion and explanation of many features of ethics in general. The first portion deals with broad principles of moral philosophy, while the latter portion deals more specifically with rules of behavior in situations that characterize fraud examiners' work. The applications of the ACFE Code of Professional Ethics are also discussed.

What Is Ethics?

Ethics is concerned with what is right and wrong. In *A Critical Introduction to Ethics*, Philip Wheelwright defined *ethics* as:

> *[The] branch of philosophy which is the systematic study of reflective choice, of the standards of right and wrong by which it is to be guided, and of the goods toward which it may ultimately be directed.*

This definition contains three key elements:

- Ethics involves questions requiring reflective choice (decision problems).
- Ethics involves guides of right and wrong (moral principles).
- Ethics is concerned with values (goods) inherent in ethical decisions.

Codes of Ethical Conduct

Why does an individual or a group need a code of ethical conduct? While it has been said that a person should *be* upright and not be *kept* upright, a code of conduct serves a useful purpose as a reference and a benchmark for ethical guidance. A code makes explicit some of the criteria for conduct particular to a profession. In this way, codes of professional ethics are able to provide some direct solutions that might not be available from general ethics theories.

Furthermore, an individual is better able to know what the profession expects when a code of ethical conduct is in place. From the viewpoint of an organized profession, a code is a public declaration of principled conduct and a means of facilitating enforcement of

standards of conduct. Practical enforcement and profession-wide internal discipline would be much more difficult if members were not first put on notice of the standards.

An Ethical Decision Maker's Role

While one of the main purposes of ethics is to guide the actions of individual decision makers, the role of decision maker does not fully describe a professional person's entire obligation. Each person acts not only as an individual but also as a member of a profession and as a member of society. Hence, fraud examiners also are *spectators* (observing the decisions of colleagues), *advisors* (counseling with coworkers), *instructors* (teaching students or new employees on the job), *judges* (serving on disciplinary committees), and *critics* (commenting on the ethical decisions of others). All of these roles are important in the practice of professional ethics.

In considering general ethics, the fraud examiner's primary goal is to arrive at a set of acceptable methods for making ethical decisions to fulfill all his roles. Consequently, an understanding of some of the general principles of ethics can serve as background in understanding the ethical decisions faced by fraud examiners, as well as the ethical guidelines provided in the ACFE Code of Professional Ethics.

Ethical Decisions

One of the key elements in ethics is reflective choice. *Reflective choice* refers to the process whereby an individual identifies a decision problem, analyzes the situation—collects information, considers rules of behavior, and thinks about consequences of alternative actions—and takes action. In short, reflective choice refers to decision making.

Ethical problems almost always involve projecting yourself in a future in which you have to live with your decisions. Professional ethics decisions usually turn on these questions: "What written and unwritten rules govern my behavior?" and "What are the possible consequences of my choices?"

We could dispense with any discussion of ethical theories and rules if we were willing to accept a simple proposition: "Let conscience be your guide." Such a rule is appealing because it calls upon an individual's own judgment, which might be based on wisdom, insight, adherence to custom, or an authoritative code. However, it might also be based on caprice, immaturity, ignorance, stubbornness, or misunderstanding.

In a similar manner, reliance on the opinions of others or on the weight of opinion of a particular social group is not always enough. Another person or a group of people might perpetuate a custom or habit that is wrong. To adhere blindly to custom or group habits is to abdicate individual responsibility. Thus, the function of ethical principles and rules is not to provide a simple and sure answer to all your problems, but to provide some guidelines for individual decisions and actions.

Morality, Ethics, and Legality

The concepts of morality, ethics, and legality are related, but they each represent different things. To illustrate, consider the following question: Is it all right to lie to catch a crook? The answer is not immediately clear, and it depends on the underlying facts and a number of factors, including moral, ethical, and legal concerns. For further illustration, consider the following story about a fraud examination.

> *Management at Megacorp, Inc., suspected that its stockroom employees were stealing electronic parts from inventory and hired Abel, a fraud examiner, to discover if and how the thefts were occurring. Abel went undercover to investigate the matter, but only the president of Megacorp knew Abel's true identity. Abel applied for a job at Megacorp, and his application was processed through the personnel department in the normal manner. Ultimately, Abel was hired as a stockroom clerk. While working in the stockroom, Abel preserved his false identity, infiltrated the group responsible for the thefts, and gathered sufficient evidence to prove their misconduct. Consequently, the culpable employees were indicted and charged with theft by state prosecutors.*

This scenario illustrates the moral, ethical, and legal issues facing fraud examiners. These issues involve principles of moral philosophy, rules of ethics, legal considerations, values, and—above all—the problem of distinguishing right from wrong. *Morality* refers to the underlying codes of right and wrong. But the difficulty with morality is that it is relative, not absolute. For example, although lying generally is wrong, Abel would likely argue that his deceptive acts are morally justified under the circumstances.

In contrast, *ethics* refers to the appropriateness of a decision in light of morality. That is, ethics stress standards or codes of behavior expected by the group to which the individual belongs. To illustrate the difference between morals and ethics, consider a criminal defense lawyer who is hired to represent the stockroom employees charged with theft. Though the

lawyer's personal moral code likely finds theft immoral, ethics demand that the accused be defended, even though the lawyer knows the individuals are guilty. Accordingly, the ethics override the lawyer's personal morals that find theft immoral.

Legality refers to lawfulness by conformity to a legal statute. Although there might be overlap between ethics and the law, they are not always in line with each other. For instance, even though speeding is illegal, many drivers would claim that it is not always unethical.

The High Road

Most public and many private discussions of ethics quickly become philosophical, reaching toward lofty principles and broad generalizations about desirable behavior. People easily cite well-known guides and believe the ideas in them should never be violated. Such discussions often take place in a vacuum, apart from real-world situations. People generally exhort themselves and others to observe the highest principles of moral behavior. That is, they urge each other to take the high road, but often, promoting the high road is easier than taking it. Moreover, the idealistic nature of this level of discussion is often not sufficient to help people cope with a problem immediately at hand.

The *high road* is the realm of moral philosophy where philosophical principles guide the process of thinking about problems and distinguishing right from wrong. Such principles are necessary in the process of everyday life. Even though an individual might not know them in all the twists and turns familiar to philosophers, their fundamental precepts are well understood in our concept of *common sense*.

Moral Philosophy, Ethics, and Law

Moral philosophy is the branch of philosophy that involves systematizing, championing, and advocating concepts of right and wrong. It exists at a global level, permeating all facets of the problems of distinguishing right from wrong. Moral philosophy is a field that deals with human judgments based on standards that identify *good* and *evil*. These words mean more than just *right* and *wrong*, but they convey essentially the same idea.

There are two aspects of moral philosophy that fraud examiners should consider. The first is the human judgment process, which deals with ways people analyze problems. The second is the standards or values—such as honesty, faithfulness, and unselfishness—that people can use to make moral principles useful.

Ethics can be distinguished from moral philosophy by considering the role that each have in society. People are usually more comfortable talking about ethics than moral philosophy because ethics seems practical while moral philosophy seems intellectual and impractical. Ethics generally refers to a specific setting—a society, culture, nation, profession, or small group. In this context, ethics refers to behavior that conforms to some societal norms or to a written code of ethics, such as the ACFE Code of Professional Ethics.

When faced with an ethics-related problem, it is appropriate to begin analyzing the issue by asking: Is it legal? Such analysis is at the most practical level. The law deals with actions that are permitted and actions that are prohibited, but it is the lowest reference level for moral decisions.

Again, ethics and the law are not always in line with each other; the law might permit an action that is prohibited by a profession's code of ethics. Laws, rules, and regulations function as standards by which to judge whether an action is acceptable or illegal, but not whether the behavior is right. For instance, if you have promised an individual that you will honor a contract, you are ethically bound to do so, regardless of your legal responsibility; under these facts, keeping your word is the right thing to do, no matter what the law says.

Similarly, morality, ethics, and the law are not always in line with each other. A profession's code of ethics might permit actions that are immoral, or the law might prohibit actions that are moral.

For example, the American Institute of Certified Public Accountants had rules of ethics that prohibited advertising, with the exception of broadly based institutional advertising. The profession believed that professional dignity and objectivity were enhanced by keeping practitioners out of this aspect of the commercial world. The U.S. Federal Trade Commission and the U.S. Department of Justice, however, reached a different conclusion. They decided that the prohibitions against advertising were against the laws barring restraint of trade. The government forced the profession to eliminate the rules against advertising. This example illustrates the triumph of one set of values (the government's belief that competition through advertising would benefit consumers) over another set (the profession's belief that professional dignity should be preserved).

All three areas—morality, ethics, and legality—are important for everyday decisions. When faced with an ethical decision, fraud examiners should consider whether a contemplated

action is legal, is permitted by the written code of ethics, and is moral. Thus, it is important to know the distinctions between morality, ethics, and legality (i.e., between the philosophy, the rules, and the law). Only with this knowledge can a fraud examiner know where he stands when deciding upon and justifying a course of action.

This material observes one important limitation. It confines its consideration of ethics for fraud examiners to matters of moral philosophy, rules of ethics, and general values. It does not deal with detailed matters of the law or with questions about the legality or illegality of actions a fraud examiner might take. By taking this approach, this material does not state that the law is unimportant; instead, the law is beyond the scope of this part of the materials.

Means and Ends

Means-and-ends analysis is an approach to ethical problem solving. In assessing the ethicality of certain actions under this approach, we must look at the means (the techniques used) and the ends (the results sought). Ethics provide a measure through which the relationship between means and ends can be clarified.

Everyone knows some saying like "The ends justify the means," or "Fight fire with fire." And often, people promote such claims when trying to justify actions that could otherwise be considered immoral, unethical, or illegal. Fraud examiners can be particularly influenced by such ideas because they need to deal with people who do not exercise moral reasoning, follow ethical rules, or keep within the law.

Is It All Right to Lie? No, Except …

Even if a moral rule appears to be inflexible, people can think of situations in which they could justify breaking the rule. For example, some people think that lying is okay if done to catch a crook. After all, if the moral rules were followed by everyone, then there would be no crooks; thus, the fraudster's dishonesty made it necessary for the fraud examiner to lie in return. Thus, under such analysis, the ends (catching crooks and upholding justice) justify the means (lying).

The means-end analysis evaluates how well an action—often in comparison with an alternative course of action—accomplishes its intended ends. The action itself is not judged as ethical or unethical; rather, the outcome is the deciding factor in whether the act is justified.

The problem with means-ends analyses is that they are often superficial, ending with the needed justification but failing to consider other aspects and consequences of the actions. To illustrate, consider the facts in the previous case study involving Megacorp. Megacorp's president must think about the moral, ethical, and legal climate of the company once it becomes known that an undercover agent was employed. (How many more are around? What happened to trust?)

Some Concluding Remarks

This brief discussion of ethics provides some guide to the ways many people approach difficult decision problems. When facing difficult decision problems, individuals should take general principles of moral philosophy and apply them to a real decision. But the application of these principles through an individual's codes of professional ethics is where the challenge lies.

Codes of professional ethics and statutory law have two things in common. They are both based, more or less, on pervasive moral principles and values, and they both represent the aspects of behavior that a committee or legislature has chosen to put in writing. Neither codes of professional ethics nor the law provide guidance for every situation. Therefore, professional people, including fraud examiners, often must decide on a course of action without guidance.

Two types of ethics operate in the professional environment—general ethics (the spirit) and professional ethics (the rules). In their book *The Philosophy of Auditing*, Robert K. Mautz and Hussein A. Sharaf contributed the following thoughts to the association of general ethics and professional ethics:

> *The theory of ethics has been a subject of interest to philosophers since the beginnings of recorded thought. Because philosophers are concerned with the good of all mankind, their discussions have been concerned with what we might call general ethics rather than the ethics of small groups such as the members of a given profession. We cannot look, therefore, to their philosophical theories for direct solutions to our special problems. Nevertheless, their work with general ethics is of primary importance to the development of an appropriate concept in any special field. Ethical behavior in auditing or in any other activity is no more than a special application of the general notion of ethical conduct devised by philosophers for*

> *people generally. Ethical conduct in auditing draws its justification and basic nature from the general theory of ethics. Thus, we are well-advised to give some attention to the ideas and reasoning of some of the great philosophers on this subject.*

Accordingly, understanding the importance of ethical behavior is vital for fraud examiners, whose primary function is to aid in the prevention and detection of fraud. In practical terms, ethics involves making the right decision even when one's actions are not under scrutiny. Thus, fraud examiners must be able to make the correct choices in times of pressure, especially when there is no one to answer to but themselves.

Additionally, understanding ethics will help fraud examiners work through ethical dilemmas, provide them with a range of analytical tools with which they can assess ethical issues, and help them communicate ethical arguments to others.

We have attended to the ideas and reasoning of philosophers, and now we turn to the ACFE Code of Professional Ethics and its particular rules.

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS
CODE OF PROFESSIONAL ETHICS

I. An ACFE member shall, at all times, demonstrate a commitment to professionalism and diligence in the performance of his or her duties.

II. An ACFE member shall not engage in any illegal or unethical conduct, or any activity which would constitute a conflict of interest.

III. An ACFE member shall, at all times, exhibit the highest level of integrity in the performance of all professional assignments, and will accept only assignments for which there is reasonable expectation that the assignment will be completed with professional competence.

IV. An ACFE member will comply with lawful orders of the courts, and will testify to matters truthfully and without bias or prejudice.

V. An ACFE member, in conducting examinations, will obtain evidence or other documentation to establish a reasonable basis for any opinion rendered. No opinion shall be expressed regarding the guilt or innocence of any person or party.

VI. An ACFE member shall not reveal any confidential information obtained during a professional engagement without proper authorization.

VII. An ACFE member shall reveal all material matters discovered during the course of an examination, which, if omitted, could cause a distortion of the facts.

VIII. An ACFE member shall continually strive to increase the competence and effectiveness of professional services performed under his or her direction.

The ACFE Code of Professional Ethics was created by the Board of Regents of the Association of Certified Fraud Examiners and was adopted January 1, 1989.

Commitment to Professionalism and Diligence

An ACFE member shall, at all times, demonstrate commitment to professionalism and diligence in the performance of his or her duties.

Professionalism

Professionalism refers to the standing, practice, methods, character, qualities, or typical features of a professional or a professional organization. Professionalism is a quality desired by most people, but it is obtained at a price. Professionalism exists on two basic levels: (1) for the professional group as a whole and (2) for the individual fraud examiner.

Professionalism for the Group as a Whole

People frequently refer to professions, professional men and women, and professional activities without defining the meaning of the concept "professionalism." Some fraud examiners say, "I might not know how to define it, but I know it when I see it."

There are five principal characteristics that help differentiate professional fields from other vocations. The five characteristics are as follows:

- A body of specialized knowledge acquired by formal education
- Admission to the profession governed by standards of professional qualifications
- Recognition and acceptance by society of professional status, and concurrent recognition and acceptance of social responsibility by the professional
- Standards of conduct governing relationships of the professional with clients, colleagues, and the public
- An organization devoted to the advancement of the obligations of the professional group

A BODY OF SPECIALIZED KNOWLEDGE AND FORMAL EDUCATION

Professional fields are characterized by a body of specialized knowledge. A fraud examiner's work involves specialized knowledge derived from several other fields, such as accounting, auditing, criminology, investigation, and law. A profession might not have a body of knowledge truly unique unto itself, but it should have one that requires study,

comprehension, and practice over and above the everyday abilities other people might possess.

In many fields, continuing education has become a hallmark of professionalism, and ongoing efforts to increase competence and effectiveness have become required by numerous professions. The Association of Certified Fraud Examiners requires 20 hours of continuing professional education (CPE) every 12-month period, half of which must be directly related to fraud detection or deterrence. Additionally, two hours of CPE must be directly related to ethics.

PROFESSIONAL ADMISSION STANDARDS

Professional fields are also characterized by an admissions process that is governed by standards of professional qualifications. Some industries govern admission to their ranks by qualifications contained in law, but legal recognition is not required.

Conversely, many professions are not regulated by legal statutes. For instance, the Certified Internal Auditor has the status of a profession without the benefit of licensing laws. The fraud examiner profession is another example.

Additionally, many professions require exams for certification purposes. Certification examinations are offered in many professions, such as law, medicine, real estate, insurance, finance, accounting management, public accounting, and internal auditing. For fraud examiners, the CFE Examination is part of the certification process, and it contributes to the field's professional recognition.

Moreover, many, but not all, professions impose work experience requirements. Experience is required for many, but not all, professional licenses and certifications. For example, experience is required to obtain the Certified Internal Auditor designation. Likewise, designation as a Certified Fraud Examiner requires at least two years of experience in combination with other qualifications.

RECOGNITION AND ACCEPTANCE BY SOCIETY: A RECIPROCAL RELATIONSHIP

No group of practitioners can become a profession merely by declaring itself to be one. Society must acknowledge the group as a professional body. At present, fraud examiners are at the stage of becoming a self-declared profession. Historically, other professions had the same starting point. Modern medicine overcame its roots in magic. Accountants rose from

the level of bookkeepers. Internal auditors advanced social goals by presenting a responsible front to public bodies.

Although social recognition is essential, it is not necessarily permanent. Society will not continue to honor as professional any group that fails to serve a broad-based social and public interest. Thus, professionals such as Certified Fraud Examiners must reciprocate and accept the social responsibility to serve the public interest.

STANDARDS OF CONDUCT

Professional fields are also characterized by the adoption of and adherence to a code of professional ethics and standards of conduct, and such codes and standards can help a profession achieve full social recognition.

Codes of ethics serve as a reference and benchmark for ethical guidance. Like professionals in other fields, ACFE members are required to adhere to an explicit code of ethical conduct—the ACFE Code of Professional Ethics.

Furthermore, codes of conduct provide a set of expectations with regard to professional conduct. They establish a basic framework of expectations for professionals by outlining common principles. From the viewpoint of an organized profession, a code is a public declaration of principled conduct and a means to facilitate the enforcement of standards of conduct.

Fraud examiners and other professionals must observe their codes with an awareness of the society around them. Professionals must not follow such rules in a self-serving manner or in a way that does not benefit the public. Possessing and following a set of behavioral rules is one thing; possessing and following a set of rules in a way that meets public expectations is another.

A PROFESSIONAL ORGANIZATION

Professional fields are typically characterized by a dedicated organization devoted to the advancement of the group's obligations. For example, the Association of Certified Fraud Examiners (ACFE) is an association of professionals comprising Certified Fraud Examiners and Associate Members who have made a commitment to work together for the common goal of detecting and preventing fraud, waste, and abuse.

Professionalism for the Individual Fraud Examiners

Additionally, professionalism exists for the individual fraud examiner. But when the focus of professionalism is turned to the individual fraud examiner, individual members must not forget that their actions reflect on the group as a whole.

By gaining admission into the Association of Certified Fraud Examiners and attaining the Certified Fraud Examiner certification, individual members are presumed to possess a body of knowledge. Also, each member is expected to adhere to the ACFE Code of Professional Ethics and maintain membership in the organization.

Individual fraud examiners exhibit professionalism by continually striving to honor the recognition of the profession granted by the public. In day-to-day life, this is accomplished by exercising diligence in performing fraud examination work.

Diligence

The "diligence in performing his or her duties" phrase in the rule refers to several activities that collectively define high-quality fraud examination work. They include properly planning assignments and supervising assistants and colleagues, avoiding conflicts of interest, performing with competence, obtaining sufficient evidence to establish a basis for opinions, maintaining confidential relations, and avoiding distortion of facts. These activities are the subjects of other rules in the ACFE Code of Professional Ethics, and they will be discussed in more detail later.

Legal and Ethical Conduct and Conflict of Interest

> *An ACFE member shall not engage in any illegal or unethical conduct, or any activity which would constitute a conflict of interest.*

This rule is a composite of three prohibitions: illegal conduct, unethical conduct, and conflict of interest.

Illegal Conduct

This rule states that ACFE members shall not engage in illegal conduct. The prohibition of illegal conduct seems straightforward, but it can sometimes be difficult. While some activities might be obviously illegal, the legality of others might not be so clear. When a fraud

examiner confronts questionable situations, he should consult an attorney because fraud examiners generally are not entitled to claim ignorance of the law. At the same time, however, it might be difficult to know ahead of time whether such a consultation is necessary. Consider the following law-related problems (but remember that this chapter on ethics is not intended to be your primary guide to legal matters).

Libel and Slander

Libel and slander can cause personal injury and subject a fraud examiner to a lawsuit for damages. *Libel* is a written defamation of someone else's character. *Slander* is a spoken defamation. The content of a libelous or slanderous message must:

- Contain words that injure another person's character or reputation or hold him up to ridicule.
- Be communicated orally or in writing to other people.
- Cause an actual damage to the person who is the subject of the communication.

The risks involved in libel and slander are reasons for having the rule in the ACFE Code of Professional Ethics that prohibits expression of opinions on the guilt or innocence of people.

False Imprisonment

False imprisonment can mean more than putting a person behind bars. Courts have found many types of detainment to constitute false imprisonment, including locking an employee in a store, removing a distributor from a car, and detaining a witness by force. Even though drastic action might be essential, a fraud examiner must accomplish his task legally.

Ignorance of the Law

Some rules for professionals insert the word *knowingly* in relation to illegal activities, saying: "One should not knowingly be a party to an illegal activity." The ACFE Code of Professional Ethics does not include this way out. Fraud examiners are generally not entitled to claim ignorance of the law. They are expected to know a considerable amount of law in connection with investigations, and they are expected to know when to consult a lawyer.

Unethical Conduct

Additionally, this rule states that ACFE members shall not engage in unethical conduct. These materials have presented an array of issues in moral philosophy and ethical

thinking—intertwining considerations of principles and values. This latter part is set forth in the ACFE Code of Professional Ethics. Legitimate questions are: What manner of unethical conduct is meant by this rule? Does it refer to general matters of moral philosophy and ethics, or is its applicability limited only to the rules in this code?

In particular, this prohibition is complicated by the question of scope (i.e., the question of what conduct falls within the scope of this prohibition). A narrow focus would center on the rules in the ACFE Code of Professional Ethics, but a broad focus would include a fraud examiner's interaction with the people affected by his choices. The broader focus is more consistent with the concept of professionalism because the code itself is a limited set of rules.

Moreover, a fraud examiner must take personal responsibility for decisions, and must be aware that other professionals are often criticized for adhering too rigidly to their codes. Lawyers face harsh criticisms when they seem to hide knowledge of criminal acts in their privileged communications. Doctors are often criticized for the things they tell their patients about terminal illnesses. Professions are criticized for having specialized rules that seem to permit their members to act contrary to social expectations.

Conflict of Interest and Independence Considerations

The rule also states that ACFE members shall not engage in conflicts of interest. A *conflict of interest* exists when a fraud examiner's ability to objectively evaluate and present an issue for a client is impaired by a current, prior, or potential future relationship with parties to the fraud examination.

The parties whose interests might conflict range widely and can include the fraud examiner, the fraud examiner's clients (e.g., Client A might conflict with Client B or C), the fraud examiner's employer, the public ("innocent bystanders"), and law enforcement agencies. Almost every fraud examination involves most, if not all, of these parties, and the lines that connect them can be muddled.

Deciding if a conflict or a community of interests exists depends on the facts of each particular situation; however, the following are some general rules concerning conflicts of interest:

- A fraud examiner employed full time by a company should not engage in other jobs that create a hardship or loss to the employer.

- A fraud examiner should not be a "double agent" employed by one company, but retained by another company or person to infiltrate the employer and transmit inside information (unless, of course, the employing company agrees to the arrangement in order to apprehend other parties employed by the company).
- A fraud examiner should not accept engagements from both sides to a controversy—just like lawyers are prohibited from representing both parties in a transaction, lawsuit, or trial.

Conflicts of interest and *independence* are related concepts; professional rules prohibiting conflicts of interest often exist specifically to convey to the public a perception of independence.

Independence and conflict avoidance are enhanced by refraining from having financial and managerial interests in clients or in joint cooperation with clients' managers and directors. After all, they might be a suspect in an investigation. When a fraud examiner works as an employee of a company, the prohibitions about employment are not relevant because the employer-employee relationship is known to the employer, who is the client and recipient of any reports. In such cases, independence and conflict should be considered in relation to all the other parties involved.

Independence and Objectivity

ACFE members are responsible for maintaining independence in attitude and appearance and for approaching and conducting fraud examinations in an objective and unbiased manner.

INDEPENDENCE IN ATTITUDE AND APPEARANCE

Independence of attitude requires impartiality and fairness in conducting examinations and in reaching resulting conclusions and judgments. Fraud examiners must also be sensitive to the appearance of independence so that conclusions and judgments will be accepted as impartial by knowledgeable third parties. Fraud examiners who become aware of a situation or relationship that could be perceived to impair independence, whether or not actual impairments exist, should inform management immediately and take steps to eliminate the perceived impairment, including withdrawing from the examination if necessary.

OBJECTIVITY

Objectivity refers to the ability to conduct examinations without being influenced by one's own personal feelings or the feelings and motives of others. To ensure objectivity in performing examinations, fraud examiners must maintain an independent mental attitude, reach judgments on examination matters without undue influence from others, and avoid being placed in positions where they would be unable to work in an objective professional manner. All possible conflicts of interest should be disclosed.

Integrity and Competence

> *An ACFE member shall, at all times, exhibit the highest level of integrity in the performance of all professional assignments, and will accept only assignments for which there is reasonable expectation that the assignment will be completed with professional competence.*

This rule contains two parts. The first deals with integrity and the second with competence. Competence here is related to diligence, as discussed previously in relation to the first rule in the ACFE Code of Professional Ethics.

Integrity

In part, this rule provides that ACFE members must act with integrity at all times. If you were asked to name a desirable personal characteristic, integrity is one that would rank high on the scale, along with honesty, truthfulness, trustworthiness, and loyalty. Thus, outside observers of ACFE members' activity will look for signs of integrity in fraud examiners to determine whether trust is warranted. However, integrity hardly exists apart from other characteristics well known in moral philosophy and recognized in the ACFE Code of Professional Ethics.

Integrity requires honesty, truthfulness, trustworthiness, and confidentiality. It also requires subordination of desires for personal gain to the interests of clients, employers, and the public. It requires independence of mental attitude and avoidance of conflicts of interest. In addition, integrity means that a fraud examiner ought to have a well-developed sense of moral philosophy—an ability to analyze situations where no rules of the ACFE Code of Professional Ethics are specifically applicable and to be able to distinguish right from wrong. It does not mean, however, that an ACFE member must be perfect in all technical

matters, nor does it mean that fraud examiners and others cannot have honest differences of opinion. In the course of a fraud examination, inadvertent errors, mistakes of judgment, and other problems might cause conflict. In such cases, a fraud examiner can preserve integrity either by admitting error or by convincingly justifying a difference of perception or opinion.

Professional Competence

This rule also states that ACFE members must be competent in their respective areas and disciplines, and they shall not accept assignments where competence is lacking. *Professional competence* refers to how well fraud examiners do their job.

Determination of competence always depends on the specific facts and circumstances of the assignment. Competence is best understood in the context of the *prudent practitioner*. The idea of a prudent professional practitioner is present in other social science theories; for example, the "economic man" of economic theory and the "reasonable man" of law. This concept can be summarized for fraud examiners as follows:

> *A prudent practitioner is assumed to have a knowledge of the philosophy and practice of fraud examinations, to have the degree of training, experience, and skill common to the average fraud examiner, to have the ability to recognize indications of frauds, and to keep abreast of developments in the perpetration and detection of fraud. Competence requires the fraud examiner to be acquainted with the company, activity, function, or program under investigation; to review the methods of control in operation; to obtain sufficient evidence pertinent to the suspected fraud or illegal activity; to be responsive to unusual events and unfamiliar circumstances; to persist until any reasonable doubts about the evidence have been eliminated; and to exercise caution in instructing assistants and reviewing their work.*

A related concept is that of *due professional care*, which involves exercising the same level of care and skill that a prudent professional in the same profession and in similar circumstances would exercise. In exercising due professional care, fraud examiners are responsible for ensuring that there is sufficient predication for beginning a fraud examination; that each examination is conducted with diligence and thoroughness; that all applicable laws and regulations are observed; that appropriate methods and techniques are used; and that each examination is conducted in accordance with professional standards.

Thus, fraud examiners must be skilled in obtaining information from records, documents, and people; in analyzing and evaluating information and drawing sound conclusions; in communicating the results of fraud examinations, both orally and in writing; and in serving as an expert witness when appropriate. Fraud examiners must also be knowledgeable in investigative techniques, applicable laws and rules of evidence, fraud auditing, criminology, and ethics.

Fraud examiners cannot be expected to have an expert level of skill and knowledge for every circumstance that might be encountered in a fraud examination. Nevertheless, they must have sufficient skill and knowledge to recognize when additional training or expert guidance is required. It is the responsibility of a fraud examiner to ensure that necessary skills, knowledge, ability, and experience are acquired or available before going forward with a fraud examination.

Sources of Interference with Professional Competence

Professional competence also demands attention to three kinds of interference that can damage the independence and quality of a fraud examiner's work. Fraud examiners who permit these conditions to interfere with the assignment demonstrate less than the desired level of professional competence. The three types of interference are programming, investigation, and reporting.

PROGRAMMING

Fraud examiners must remain free from interference by managers who try to restrict, specify, or modify the procedures they need to perform, including any attempts to assign personnel or otherwise control the examination work. Occasionally, client or employer managers try to limit access to information or to other personnel, or to limit the amount of time available for the assignment.

INVESTIGATION

When appropriate, fraud examiners must have free access to books, records, correspondence, and other evidence. They must have the cooperation of managers or other employees without any attempt to interpret or screen evidence.

REPORTING

Client or employer managers should not be allowed to overrule the fraud examiner's judgments on the appropriate content of a report. Integrity is destroyed and judgment is

subordinated when the fraud examiner is compelled to alter a report or to omit important information or to misstate facts. Fraud examiners must not let any feelings of misguided loyalty to the client, employer, or other sources of conflicts of interest interfere with their obligation to report fully and fairly.

Professional Skepticism

As part of exercising professional integrity and competence, fraud examiners must always perform their work with a mindset of professional skepticism and begin assignments with the belief that something is wrong or someone is committing a fraud (depending on the nature of the assignment and the preliminary information available). Furthermore, fraud examiners should relax their attitude of skepticism only when the evidence shows no signs of fraudulent activity. At no time is a fraud examiner entitled to assume a fraud problem does not exist. Thus, professional skepticism can be dispelled only by evidence. As a result, opinions or attestations about a fraud-free environment are absolutely prohibited for ACFE members.

Court Orders and Testimony

> *An ACFE member will comply with lawful orders of the courts, and will testify to matters truthfully and without bias or prejudice.*

This rule provides that ACFE members must comply with all lawful court orders, and they should testify to matters truthfully and without bias or prejudice. The essence of this rule is truth-telling. The first part of the rule, which concerns complying with lawful court orders, provides that fraud examiners should not flee from a summons or subpoena issued by a court. Even though the rule specifies "courts," it is reasonable to extend it to other agencies that have the legal power to issue such orders (such as government commissions, grand juries, special prosecutors, and quasi-judicial administrative agencies).

If a fraud examiner is involved with legal counsel who devises a strategy to avoid or delay a court order, he can listen to the legal advice but must weigh it against his own knowledge of proper and legal behavior. In some cases, fraud examiners might need to obtain a second legal opinion. A fraud examiner accused of obstruction of justice could be on shaky grounds with a "my lawyer told me to do it" defense.

The second part of this rule provides that fraud examiners should testify to matters truthfully and without bias or prejudice. Fraud examiners commonly provide testimony in legal or equitable proceedings, and they must be truthful when doing so. Any exaggeration or embellishment, if uncovered, will likely reduce the fraud examiner's credibility and persuasiveness. Moreover, the use of false statements, half-truths, and misrepresentations by a fraud examiner could cause the innocent to be punished or the guilty to go free. A fraud examiner's word can hold great weight, and this should not be taken lightly.

Providing truthful testimony can present strategic problems, and fraud examiners—even those who are attorneys—should always be represented by counsel in a courtroom, deposition, or other testimony setting. The lawyers' own saying is: "An attorney who represents himself has a fool for a client." Counsel is necessary to protect witnesses from improper questioning.

When fraud examiners provide testimony in direct examination or cross-examination, they should respond to the questions that are asked—no more and no less. The attorney conducting the examination has the responsibility to ask the right questions, and the fraud examiner's counsel has the responsibility to object to misleading, improper, or irrelevant questions. The fraud examiner's counsel also has the obligation to correct any problems with the cross-examination. A "helpful" fraud examiner who tries to embellish the answers with additional material might offend the court or cause unintentional harm to the case. Of course, a fraud examiner may invoke his own legal rights, upon the advice of counsel.

Additionally, when responding to questions in a testimonial setting, fraud examiners must deliver their answer without bias or prejudice. It is the lawyer's job to be biased and prejudiced—in the context of the adversary judicial system—establishing the case for his own client or for the government. The greatest danger for delivering biased or prejudicial testimony exists when responding to broad, open-ended questions, such as: "Tell the court about your findings in your fraud examination." This type of question is an open-ended invitation to the fraud examiner's thoughts, which might be inadvertently peppered with perceptions and bias. Responding to such questions amounts to delivering reports (which are covered in the next rule in the ACFE Code of Professional Ethics).

Reasonable Evidential Basis for Opinions

> *An ACFE member, in conducting examinations, will obtain evidence or other documentation to establish a reasonable basis for any opinion rendered. No opinion shall be expressed regarding the guilt or innocence of any person or party.*

Evidential Basis for Opinions

In part, this rule states that fraud examiners must obtain evidence to establish a reasonable basis for any opinion rendered. *Evidence* can be defined as all the information that influences a decision maker in reaching decisions. Evidence might be quantitative or qualitative; it may be objective or it may have subjective qualities; it may be absolutely compelling to a decision or it may be mildly persuasive.

Auditors sometimes say they gather evidence to show that financial statements are presented properly or that control procedures are operating effectively. They are following a time-tested method of investigation that consists of three parts:

- Recognize the problem or issue subject to investigation.
- Gather sufficient relevant evidence about it.
- Analyze the evidence and reach a conclusion about the problem or issue.

Most auditors' propositions are expressed positively, such as: "The cash balance is accurately stated." However, an auditor will actually seek evidence to show that the cash balance is *not* properly stated. Imagine a cash balance that is the sum of 110 separate bank accounts. An audit team will probably sample these accounts instead of looking at all of them. The auditors look for evidence that some of these cash balances are misstated. If they fail to find any misstatements in a sufficiently large sample, they have not proved that the total is proper, but they have no reason to believe that it is materially misstated.

A literal report on this kind of work would be called "negative assurance," in which an auditor would say: "Nothing came to my attention to make me believe the cash balance is materially misstated." This statement of negative assurance is an accurate report of the audit process. As long as the "attention" consists of sufficient relevant evidence, the report is useful. Auditors might not know without any doubt that the balance is proper, but they are entitled to act as though it is because they have analyzed sufficient relevant evidence.

Some fraud examinations can take on this same character. Fraud examiners will be assigned to seek the truth about some business records or to try to determine whether some control procedures have failed. The fraud examiner will seek evidence of misstatement or failure, and, if none is found, will report the positive results.

In other cases, a client or employer might already know that fraud, thefts, shortages, control failures, or other such events have occurred. The fraud examiner's assignment is to then determine how the improper activity is being carried out, by whom, and to what extent. This kind of fraud investigation demands sufficient evidence, examples, and suitable documentation to prove the how/whom/extent findings. In these cases, the "negative assurance" type of conclusion is not appropriate. Fraud examiners must obtain the evidence to show the actual how/whom/extent conclusions.

As part of the ACFE Code of Professional Ethics, ACFE members are tasked with collecting and evaluating a sufficient amount of relevant evidence to afford a reasonable and logical basis for any opinions rendered. Thus, fraud examiners must collect evidence, whether exculpatory or incriminating, that supports fraud examination results and will be admissible in subsequent proceedings. To do so, the fraud examiner must obtain and document evidence in a manner that ensures that all necessary evidence is obtained and that the chain of custody is preserved. Additionally, fraud examiners must act prudently to preserve the integrity of relevant evidence and material.

Opinions Regarding Guilt and Innocence

Additionally, this rule prohibits ACFE members from making statements of opinion as to the guilt or innocence of any person or party. Determining whether a person is guilty or innocent of a crime is not a decision for fraud examiners; it is a decision reserved for a judge or jury.

This is a rule of prudence. Clearly, it is prudent for a fraud examiner to refrain from usurping the role of the judge or jury. In a courtroom, no good attorney would ask a fraud examiner for such a conclusion, and no alert judge would allow such testimony.

In most situations, the fraud examiner's job is to present the evidence in his report. Such evidence might constitute a convincing case pointing to the guilt or innocence of a person. But a clear line should be drawn between a report that essentially says, "Here is the evidence

and the reasonable conclusions that can be drawn from it," and one that steps over the line and says, "This person is guilty of the crime of fraud."

Although opinions on guilt or innocence should be avoided, fraud examiners may draw reasonable conclusions based on the evidence; however, they must be very circumspect when doing so. Conclusions are based on observations of the evidence, whereas opinions call for an interpretation of the facts. For example, a fraud examiner might conclude that the suspect employee misappropriated company money, misrepresented a transaction, or concealed funds. There is no prohibition in the Code of Professional Ethics on expressing such conclusions, provided the conclusions have a reasonable basis in fact.

Additionally, opinions regarding technical matters generally are permitted if the fraud examiner is qualified as an expert in the matter. For example, a permissible opinion might address the relative adequacy of an entity's internal controls. Likewise, a permissible opinion might regard whether financial transactions conform to generally accepted accounting principles.

Confidential Information

> *An ACFE member shall not reveal any confidential information obtained during a professional engagement without proper authorization.*

This rule provides that fraud examiners must not disclose confidential information obtained during the course of a professional engagement without appropriate authorization.

Confidential information rules in professional codes of ethics have the potential to create enormous conflicts—conflicts of principles and conflicts of values. Consider this possible exchange between a lawyer and client:

Client:

Because you have taken my case on this fraud charge, I think you should know more about my background.

Lawyer:

Go ahead.

Client:

Three years ago, I participated in an armed robbery and was never caught. My gun went off and killed the storekeeper. One of my buddies was accused and convicted. He's had all his appeals and is scheduled to be executed tomorrow. What can you do?

Lawyer:

Nothing.

The lawyer's single word response of "Nothing" might be oversimplifying the situation, but the point is that lawyers have a keen awareness of the privileged information rights of their clients. Most lawyers will stoutly defend their duty not to endanger their clients, even at the cost of a life. Most laymen are shocked at this particular. One commentator responded to a lawyer defending the position with a sharp retort: "Do you mean you will sacrifice an innocent man to a rule?" The laymen's incredulity is well aimed. It brings into sharp focus two conflicting values: the benefits of a long-standing rule of legal practice and the sanctity of life itself. Not all situations are this dramatic, but fraud examiners can nevertheless get into similar conflicts.

Confidential information, for all practical purposes, is any and all information a fraud examiner might obtain in the course of work, whether it be from the company or client for whom the work is performed or from any other source consulted during the work.

Due to the nature of the anti-fraud profession, fraud examiners often will come into contact with sensitive, privileged, or otherwise confidential information. It is imperative that fraud examiners maintain integrity and trustworthiness and safeguard such information from unauthorized viewing or disclosure.

The rules of confidence are based on the belief that confidentiality facilitates the flow of information between parties. The nature of professional engagements might make it necessary for fraud examiners to have access to sensitive information. Clients and employers would be less likely to reveal such information or to provide access to such information if they could not trust fraud examiners to keep it confidential. Therefore, fraud examiners must be able to exercise prudence and good judgment when dealing with data that should be kept confidential.

Additionally, fraud examiners must not disclose privileged information obtained during the course of a professional engagement without appropriate authority. *Privileged information* is information that cannot be demanded, even by a court; it is information that is protected by law from evidence.

In the solicitor-client privilege, for example, the solicitor is obligated to observe the privilege; it can be waived only by the client (who is considered to be the "holder" of the privilege).

Fraud examiners do not have any such privilege in common law or by statute, and the ACFE Code of Professional Ethics does not assume a privileged status for the fraud examiner-client/employer relationship. (Legal jurisdictions vary on what communications are protected, and not all of these privileges are recognized in all courts.) However, fraud examiners must not disclose privileged information without proper authorization from the fraud examiner's client or employer.

If the client or employer consents to disclosure of information otherwise considered confidential, then the fraud examiner can transmit it to others. Even when such permission is granted, fraud examiners should be careful to let the client/employer know what the consent covers. Consequently, it is best to let the client/employer make the actual disclosure himself.

The obligation to keep information confidential does not terminate when the engagement ends. Thus, the confidentiality rule does not permit disclosure after a case concludes, and fraud examiners are not permitted to disclose confidential information if they are fired, resign, or retire from an employing organization.

Proper Authorization and Other Circumstances for Disclosing Confidential Information

Again, Article VI of the Code of Professional Ethics states that an ACFE member shall not reveal any confidential information obtained during a professional engagement without proper authorization. Consent from a fraud examiner's client or employer is one form of proper authorization, but there are other forms. For example, fraud examiners are not bound by confidentiality when doing so would violate the law. Thus, fraud examiners can reveal client confidences when responding to a legal court order.

Fraud examiners must be careful in situations where keeping silent could be construed as obstructing justice or engaging in a conspiracy. When faced with such circumstances, fraud examiners should seek the advice of an attorney.

Other professions have exceptions that void the confidentiality or privilege rules. For example, lawyers can reveal client confidences if doing so is necessary to prevent a future crime or when initiating complaints to their disciplinary bodies.

Information Supplied by a Suspect

Questions might arise over information a fraud examiner received from someone being investigated. Suppose an employee being questioned tells the fraud examiner something "in confidence" concerning his role in a theft. Fraud examiners must remember that the confidentiality relationship runs first to the client or employer, and that this promise of confidentiality is understood to exist without being spoken.

To illustrate, consider the situation in which a suspect employee tells the fraud examiner something "in confidence" concerning the employee's role in a theft. The fraud examiner does not have an understood or unspoken promise of confidentiality with the employee, and is therefore not bound by the rule of confidentiality. If the fraud examiner makes a promise of confidentiality to the employee-informant, the fraud examiner will likely break the promise by reporting the relevant evidence to the employer. Consequently, a fraud examiner should not promise confidentiality or leniency to an informant to obtain testimony.

Confidential Information and Conflicts of Interest

Additionally, fraud examiners must not use confidential information obtained during the course of a professional engagement in a way that conflicts with the interests of the client/employer.

The Institute of Internal Auditors' Code of Ethics contains language that makes the relation between conflicts of interest and confidential information very clear: "Members and Certified Internal Auditors shall be prudent in the use of information acquired in the course of their duties. They shall not use confidential information for any personal gain nor in any manner which would be contrary to law or detrimental to the welfare of their organization."

When a fraud examiner is privy to confidential information that he can use for personal gain, a conflict of interest exists—the fraud examiner's desire for wealth versus the

client/employer's desire for and trust in confidential services. However, a fraud examiner may only use confidential information in furtherance of his professional responsibilities; any other use without the client/employer's knowledge and consent is prohibited—particularly if such use is for the fraud examiner's personal benefit. For example, a fraud examiner who uses a client's customer database to promote his own services would be in violation of this standard. The same would be true of a fraud examiner who buys or sells stock shares based on confidential financial information that he obtained during a fraud examination or other professional engagement.

Moreover, using information for personal gain or using information to the detriment of the client/employer is akin to lying and stealing.

Public Information

Fraud examiners must be careful about revealing information obtained during the course of a professional engagement even if the information is public (i.e., information that can be accessed by the public).

It is tempting to consider confidential information to be "nonpublic information" instead of "all information" on the grounds that public information is available to everyone anyway, but such an interpretation is inappropriate. Public information might be hard to find and/or expensive to obtain and analyze. When information is public, let others find it for themselves.

Some might argue that no confidence is abused if a fraud examiner discloses public information that is published and widely distributed (e.g., financial statements in annual reports or stories in national newspapers), but the same might not be true if the fraud examiner discloses public information that is not widely available (e.g., real estate deed restrictions, liens on property, and credit records). Accordingly, defending a breach of confidence on the grounds that "it was public anyway" is a weak argument.

Confidentiality and Blowing the Whistle

Difficult problems arise over fraud examiners' obligations to blow the whistle about clients' or employers' shady or illegal practices. The problems exist on two levels. The problem first occurs on the managerial level, where the fraud examiner might be employed or engaged by high-level managers who turn out to be involved in fraudulent practices. To be prepared for such issues, fraud examiners should always have a line of communication to levels of

management above the ones at issue. Thus, for example, evidence of managerial-level misconduct can be reported to the board of directors and its audit committee without trampling on the confidentiality rule.

Second, the problem occurs on the highest level—involvement by the directors, the highest level of management, or the owners. This level presents the biggest problems. When fraud involves the highest level of management, the fraud examiner must communicate the matters to parties outside the organization, such as the police or other governmental or regulatory agencies.

In general, fraud examiners are not obligated to blow the whistle on clients or employers. However, circumstances might exist in which they are morally and legally justified in making disclosures to appropriate outside parties. Examples of such circumstances include those in which a client or employer has intentionally involved a fraud examiner in its illegal or unethical conduct or when a client or employer has distributed misleading reports based on the fraud examiner's work. The confidentiality rule is not a license or excuse for inaction when action is appropriate.

Complete Reporting of Material Matters

> *An ACFE member will reveal all material matters discovered during the course of an examination which, if omitted, could cause a distortion of the facts.*

This rule provides that fraud examiners shall disclose all material matters discovered during the course of a fraud examination. It demands full and fair reporting of the findings made in investigations. Two words—*material* and *distortion*—are key to this requirement.

Material

Information is *material* if having knowledge of such information might reasonably be expected to influence a client's or employer's decisions based on a fraud examiner's report. Accordingly, materiality is a user-oriented concept. Thus, an item of information that, if omitted from a report, would change a user's perceptions and conclusions is material.

When determining what information is material, fraud examiners should not consider what they themselves think is important and material; instead, they should try to decide what users

will consider important and material. Thus, fraud examiners must project a decision-making process onto the users.

It is important for fraud examiners to learn from clients and employers the type of information they consider important. A fraud examiner should obtain as good an understanding as possible of the users' interests, the information desired, the level of detail needed, and other aspects of the users' needs.

Furthermore, information might be considered material in some circumstances and nonmaterial in others.

Distortion

This rule also provides that fraud examiners shall disclose all material matters discovered during the course of a fraud examination that, if omitted, could distort the facts. The "distortion of facts" portion of the rule refers to omissions.

Distortion is related to materiality and users' decisions. The distortion of facts in a report could cause users to undertake inappropriate actions.

In some fraud examinations, it is not possible to obtain sufficient evidence to support a definitive conclusion or recommendation. In such circumstances, the fraud examiner should avoid rushing to judgment. When matters are not clear, the fraud examiner's report should stress the tentative nature of the evidence and withhold judgment. If the fraud examiner jumps to conclusions, he might distort the facts.

Professional Improvement

> *An ACFE member shall continually strive to increase the competence and effectiveness of professional services performed under his or her direction.*

This rule provides advice and a directive for behavior; it instructs ACFE members to progress toward greater expertise so they can better service their clients and employers.

The anti-fraud profession changes continually. Years ago, investigators had to learn how to deal with computers in the world of fraud. Today, fraud examiners are faced with a growing

array of ways to perpetrate fraud. Accordingly, learning is an ongoing and necessary process for fraud examiners to increase their professional competence and effectiveness.

To comply with this requirement, individuals who become Certified Fraud Examiners agree to complete 20 hours of continuing professional education each year. Course content is not specified in detail, but the requirement is that at least ten hours must be spent on technical subjects that contribute directly to fraud examination expertise, and at least two hours must relate directly to ethics.

Certified Fraud Examiners who also are CPAs, CAs, or CIAs, or who hold other professional designations can double-count continuing education hours obtained for the other professional designations toward their CFE-related requirements, as long as the course content meets the ACFE's continuing education criteria. Further details about policies and procedures are available on the ACFE website: www.acfe.com/cpe.aspx.

Professional ethics for fraud examiners is not simply a matter covered by a few rules in a formal Code of Professional Ethics. Concepts of proper professional conduct permeate all areas of practice. Ethics are the foundation of fraud examiners' self-regulatory efforts.

The principled approach to thoughtful decisions is important in fraud examination work in all settings, such as private practice, industrial, government and foreign employment, and other working arrangements. The ethics rules might appear to be restrictive, but they are for the benefit of the public as well as for the discipline, use, and protection of ACFE members.

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS
CFE CODE OF PROFESSIONAL STANDARDS

(Adopted by the Board of Regents, September 10, 2014)

I. Preamble

The Association of Certified Fraud Examiners is an association of professionals committed to performing at the highest level of ethical conduct. Members of the Association pledge themselves to act with integrity and to perform their work in a professional manner.

Members have a professional responsibility to their clients, the public interest, and each other, a responsibility that requires subordinating self-interest to the interests of those served.

These standards express basic principles of ethical behavior to guide members in the fulfilling of their duties and obligations. By following these standards, all Certified Fraud Examiners shall be expected, and all Associate members shall strive, to demonstrate their commitment to excellence in service and professional conduct.

II. Applicability of Code

The CFE Code of Professional Standards shall apply to all certified members of the Association of Certified Fraud Examiners (ACFE). Associate members of the ACFE should strive to adhere to the standards, but are not bound by them. The use of the terms *Certified Fraud Examiner* and *CFE* in this Code shall refer to certified members. For purposes of these standards, the term *fraud examination* means an assignment or engagement, a substantial purpose of which involves the prevention, detection, investigation, or resolution of fraud or fraud-related conduct.

III. Standards of Professional Conduct

A. Integrity and Objectivity

1. Certified Fraud Examiners shall conduct themselves with integrity, knowing that public trust is founded on integrity. CFEs shall not sacrifice integrity to serve their client, their employer, or the public interest.

2. Prior to accepting the fraud examination, Certified Fraud Examiners shall investigate for actual or potential conflicts of interest. CFEs shall disclose any actual or potential conflicts of interest to potentially affected clients or to their employers.

3. Certified Fraud Examiners shall maintain objectivity in discharging their professional responsibilities within the scope of the fraud examination.

4. Certified Fraud Examiners shall not commit acts discreditable to the ACFE or its membership, and shall always conduct themselves in the best interests of the reputation of the profession.

5. Certified Fraud Examiners shall not knowingly make a false statement when testifying under oath in a court of law or other dispute resolution forum. CFEs shall comply with lawful orders of the courts or other dispute resolution bodies. CFEs shall not commit criminal acts or knowingly induce others to do so.

B. Professional Competence

1. Certified Fraud Examiners shall be competent and shall not accept assignments where competence is lacking. In some circumstances, it may be possible to meet the requirement for professional competence by use of consultation or referral.

2. Certified Fraud Examiners shall maintain the minimum program of continuing professional education required by the Association of Certified Fraud Examiners. A commitment to professionalism combining education and experience shall continue throughout the CFE's professional career. CFEs shall continually strive to increase the competence and effectiveness of their professional services.

C. Due Professional Care

1. Certified Fraud Examiners shall exercise due professional care in the performance of their fraud examination services. Due professional care requires diligence, critical analysis, and professional skepticism in discharging professional responsibilities.

2. Conclusions shall be supported with evidence that is relevant, reliable, and sufficient.

3. Fraud examinations shall be adequately planned. Planning controls the performance of a fraud examination from inception through completion and involves developing strategies and objectives for performing the services.

4. Work performed by assistants and other professionals operating under the Certified Fraud Examiner's direction on a fraud examination shall be adequately supervised. The extent of supervision required varies depending on the complexities of the work and the qualifications of the assistants or professionals.

D. Understanding with Client or Employer

1. At the beginning of a fraud examination, Certified Fraud Examiners shall reach an understanding with those retaining them (client or employer) about the scope and limitations of the fraud examination and the responsibilities of all parties involved.

2. Whenever the scope or limitations of a fraud examination or the responsibilities of the parties change significantly, a new understanding shall be reached with the client or employer.

E. Communication with Client or Employer

1. Certified Fraud Examiners shall communicate to those who retained them (client or employer) significant findings made during the normal course of the fraud examination.

F. Confidentiality

1. Certified Fraud Examiners shall not disclose confidential or privileged information obtained during the course of a fraud examination without the express permission of proper authority or the lawful order of a court. This requirement does not preclude professional practice or investigative body reviews as long as the reviewing organization agrees to abide by the confidentiality restrictions.

IV. Standards of Examination

A. Fraud Examinations

1. Fraud examinations shall be conducted in a legal, professional, and thorough manner. The Certified Fraud Examiner's objective shall be to obtain evidence and information that is complete, reliable, and relevant.

2. Certified Fraud Examiners shall establish predication and scope priorities at the outset of a fraud examination and continuously reevaluate them as the examination proceeds. CFEs shall strive for efficiency in their examination.

3. Certified Fraud Examiners shall be alert to the possibility of conjecture, unsubstantiated opinion, and bias of witnesses and others. CFEs shall consider both exculpatory and inculpatory evidence.

B. Evidence

1. Certified Fraud Examiners shall endeavor to establish effective control and management procedures for documents, data, and other evidence obtained during the course of a fraud examination. CFEs shall be cognizant of the chain of custody including origin, possession, and disposition of relevant evidence and material. CFEs shall strive to preserve the integrity of relevant evidence and material.

2. Certified Fraud Examiners' work product may vary with the circumstances of each fraud examination. The extent of documentation shall be subject to the needs and objectives of the client or employer.

V. Standards of Reporting

A. General

1. Fraud examination reports may be oral or written, including fact witness and/or expert witness testimony, and may take many different forms. There is no single structure or format that is prescribed for a CFE's report; however, the report should not be misleading.

B. Report Content

1. Certified Fraud Examiners' reports shall be based on evidence that is sufficient, reliable, and relevant to support the facts, conclusions, opinions, and/or recommendations related to the fraud examination. The report shall be confined to subject matter, principles, and methodologies within the member's area of knowledge, skill, experience, training, or education.

2. No opinion shall be expressed regarding the legal guilt or innocence of any person
or party.

BIBLIOGRAPHY

Akers, Ronald. *Deviant Behavior: A Social Learning Approach*. 2nd ed. Belmont, CA: Wadsworth, 1977.

Akst, Daniel. *Wonderboy Barry Minkow: The Kid Who Swindled Wall Street*. New York, NY: Scribner's, 1990.

Albrecht, W. Steve., Conan C. Albrecht, Chad O. Albrecht, and Mark F. Zimbelman. *Fraud Examination*, 4th Edition. Mason, OH: South-Western, 2011.

Albrecht, W. Steve, Keith R. Howe, and Marshall B. Romney. *Deterring Fraud: The Internal Auditor's Perspective*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1984.

Albrecht, W. Steve, Gerald W. Wernz, and Timothy L. Williams. *Fraud: Bringing Light to the Dark Side of Business*. New York, NY: Irwin Professional Publishing, 1995.

American Accounting Association. *Accounting Education, Vol. 18, Number 2*. Sarasota, FL: American Accounting Association, 2003.

American Accounting Association. *Accounting Horizons, Vol. 7, Number 4*. Sarasota, FL: American Accounting Association, 2003.

American Accounting Association. *Auditing: A Journal of Practice & Theory, Vol. 22, Number 2*. Sarasota, FL: American Accounting Association, 2003.

Androphy, Joel M. *White Collar Crime*. New York, NY: McGraw-Hill, Inc., 1992.

Antle, Rick and Stanley J. Garstka. *Financial Accounting*. Cincinnati, OH: South-Western, 2002.

Arens, Alvin A., Randal J. Elder, and Mark S. Beasley. *Essential Auditing and Assurance Services: An Integrated Approach*. Upper Saddle River, NJ: Prentice Hall, 2003.

Association of Certified Fraud Examiners, The. *2014 Report to the Nations on Occupational Fraud and Abuse*. Austin, TX: ACFE, 2014.

Association of Certified Fraud Examiners, The. *Report to the Nation on Occupational Fraud and Abuse.* Austin, TX: ACFE, 1996.

Banks, David G. "Vendor Fraud: Finding Deals Gone Awry." *The White Paper*, Vol. 16, No. 5. September/October 2002.

Barefoot, J. Kirk, CPP. *Employee Theft Investigation*. Stoneham, MA: Butterworth Publishers, 1979.

Beasley, M.S., J.V. Carcello, and D.R. Hermanson. *Fraudulent Financial Reporting: 1987–1997: An Analysis of U.S. Public Companies*. Committee of Sponsoring Organizations (COSO), 1999.

Beasley, M.S., J.V. Carcello, and D.R. Hermanson. *Fraudulent Financial Reporting: 1998–2007, An Analysis of U.S. Public Companies*. Committee of Sponsoring Organizations (COSO), 2010.

Binstein, Michael and Charles Bowden. *Trust Me: Charles Keating and the Missing Millions*. New York, NY: Random House, 1993.

Biegelman, Martin T. "Designing a Robust Fraud Prevention Program, Part One." *The White Paper*, Vol. 18, No. 1. January/February 2004.

Biegelman, Martin T. "Sarbanes-Oxley Act: Stopping U.S. Corporate Crooks from Cooking the Books." *The White Paper*, Vol. 17, No. 2. March/April 2003.

Bishop, Toby J.F. and Joseph T. Wells, CFE, CPA. "Breaking Tradition in the Auditing Profession." *The White Paper*, Vol. 17, No. 5. September/October 2003.

MENU

BIBLIOGRAPHY

Black's Law Dictionary. Sixth Edition. St. Paul, MN: West Publishing Co., 1990.

Blankenship, Michael B. (Ed.). *Current Issues in Criminal Justice.* Vol. 3*, Understanding Corporate Criminality.* Garland Publishing, Inc., 1993.

Blount, Ernest C. *Occupational Crime: Deterrence, Investigation, and Reporting in Compliance with Federal Guidelines*. Boca Raton, FL: CRC Press, 2003.

BNA/ACCA Compliance Manual: Prevention of Corporate Liability. Washington, D.C.: The Bureau of National Affairs, Inc., 1997.

Bologna, Jack. *Handbook on Corporate Fraud.* Boston, MA: Butterworth-Heinemann, 1993.

Bonner, S.E., Z.V. Palmrose, and S.M. Young. "Fraud Type and Auditor Litigation: An Analysis of SEC Accounting and Auditing Enforcement Releases," *The Accounting Review 73*. October 1998.

Braithwaite, John. "An Exploratory Study of Used Car Fraud," in Paul R. Wilson and John Braithwaite (Eds.), *Two Faces of Deviance*. Brisbane: University of Queensland Press, 1978.

Brenner, Steven and Earl Molander. "Is the Ethics of Business Changing?," *Harvard Business Review*, January/February 1977: 57–71.

Brian, Brad D. and Barry F. McNeil. *Internal Corporate Investigations, Second Edition*. Chicago, IL: ABA Publishing, 2003.

Brown, William D. *Investigation and Prosecution of Insurance Fraud Prepared for the Federal Bureau of Investigation.* Dallas, TX: Arter & Hadden, 1992.

Buckwalter, Art. *Investigative Methods*. Woburn, MA: Butterworth Publishers, 1984.

Caplan, Gerald M. *ABSCAM Ethics: Moral Issues & Deception in Law Enforcement*. Cambridge, MA: Ballinger, 1983.

Carozza, Dick. "Accounting Students Must Have Armor of Fraud Examination." *The White Paper*, Vol. 16, No. 1. January/February 2002.

Carroll, John M. *Confidential Information Sources: Public & Private*. Boston, MA: Butterworth Publishers, 1975.

Cash, Lenhart and Defliese. *Montgomery's Auditing.* Eighth Edition. New York, NY: Ronald Press Company, 1957.

Cissell, James C. *Federal Criminal Trials*. Charlottesville, VA: The Michie Company, 1983.

Cissell, James C. *Proving Federal Crimes*. U.S. Department of Justice, United States Attorney, Southern District of Ohio, May 1980.

Clarke, Michael. *Business Crime: Its Nature and Control*. New York, NY: St. Martin's Press, 1990.

Clinard, Marshall B., and Peter C. Yeager. *Corporate Crime*. New York, NY: Macmillan Publishing Co., Inc., 1980.

Coderre, David. *Computer-Aided Fraud Prevention & Detection: A Step-by-Step Guide*. Hoboken, NJ: John Wiley & Sons, Inc., 2009.

BIBLIOGRAPHY

Coleman, James William. *The Criminal Elite: The Sociology of White Collar Crime.* Second Edition. New York, NY: St. Martin's Press, Inc., 1989.

Comer, Michael J. *Investigating Corporate Fraud.* Aldershot: Gower Publishing Limited, 2003.

Comstock, Anthony. *Frauds Exposed; or, How the People are Deceived and Robbed, and Youth Corrupted*. Montclair, NJ: Patterson Smith, 1969.

Conklin, John E. *Criminology, 11/E.* Englewood Cliffs, NJ: Prentice Hall, 2012.

Cook, Larry E. "Risky Business: Conducting the Internal Fraud Risk Assessment." *Fraud Magazine*, March/April 2005.

Cressey, Donald R. *Other People's Money*. Montclair, NJ: Patterson Smith, 1953.

Davia, Howard R., Patrick C. Coggins, John C. Wideman, and Joseph T. Kastantin. *Accountant's Guide to Fraud Detection and Control, Second Edition*. New York, NY: John Wiley & Sons, 2000.

Davis, Robert C., Arthur J. Lurigio, and Wesley G. Skogan (Ed.). *Victims of Crime, Second Edition*. Thousand Oaks, CA: Sage Publications, 1997.

Dean, Bruce A. "Wrap it Up: Packing Your Case for Prosecution." *The White Paper*, Vol. 16, No. 1. January/February 2002.

Dirks, Raymond L. and Leonard Gross. *The Great Wall Street Scandal*. New York, NY: McGraw-Hill Book Company, 1974.

Domanick, Joe. *Faking It In America: Barry Minkow and the Great ZZZZ BEST Scam*. Chicago, IL: Contemporary Books, 1989.

Drake, John D. *The Effective Interviewer: A Guide for Managers*. New York, NY: AMACOM, 1989.

Drucker, Peter F. *Concept of the Corporation*. New Jersey: Transaction Publishers, 2008.

Durkheim, Emile. *Suicide: A Study in Sociology*. translated by John A. Spaulding and George Simpson. New York: The Free Press, 1951.

Edelhertz, Herbert, Project Director. *The Investigation of White-Collar Crime*. Washington, D.C.: U.S. Department of Justice Law Enforcement Assistance Administration., 1977.

Edelhertz, Herbert. *The Nature, Impact and Prosecution of White Collar Crime*. Washington, D.C.: National Institute of Law Enforcement and Criminal Justice, 1970.

Ekman, Paul. *Telling Lies*. New York: The Berkley Publishing Group, 1986

Enforcement Issues Presented by the Internet. International Organization of Securities Commissions, September, 1997.

Ermann, M. David and Richard J. Lundman. *Corporate Deviance*. New York, NY: Holt, Rhinehart and Winston, 1982.

Flanagan, Timothy J., and Dennis R. Longmire (Eds.). *Americans View Crime and Justice. A National Public Opinion Survey*. Thousand Oaks, CA: Sage Publications, 1996.

Flesher, Dale L., Paul J. Miranti and Gary John Previts. "The First Century of the CPA." *Journal of Accountancy*, October 1996.

BIBLIOGRAPHY

Fridson, Martin S. *Financial Statement Analysis*. New York, NY: John Wiley & Sons, Inc., 1991.

Fusaro, Peter C. and Ross M. Miller. *What Went Wrong at Enron*. Hoboken, NJ: John Wiley & Sons, Inc., 2002.

Gaughan, Patrick A. *Measuring Business Interruption Losses and Other Commercial Damages*. Hoboken, NJ: John Wiley & Sons, 2004.

Geis, Gilbert, Ph.D. and Ezra Stotland (Eds.). *White Collar Crime: Theory and Research*. Beverly Hills, CA: Sage, 1980.

Geis, Gilbert. *On White-Collar Crime*. Lexington, MA: Lexington Books, 1982.

Geis, Gilbert and Robert F. Meier. *White-Collar Crime: Offenses in Business, Politics, and the Professions*. Revised Edition. New York, NY: The Free Press, A Division of Macmillan Publishing Co., Inc., 1977.

Georgiades, George. *Audit Procedures*. New York, NY: Harcourt Brace Professional Publishing, 1995.

Gillette, Clayton P. *Electronic Fund Transfer Fraud Protection: From Identity Theft to Wire Transfer Fraud*. Austin, TX: Sheshunoff, 2005.

Grau, Joseph J., Ph.D. (Ed.), and Ben Jacobson. *Investigative Consultant. Criminal and Civil Investigation Handbook*, New York, NY: McGraw-Hill Book Company, 1981.

Green, Gary, *Occupational Crime*. Belmont, CA: Wadsworth Publishing Company, 1996.

Greene, Craig L. "Audit Those Vendors." *The White Paper*, Vol. 17, No. 3. May/June 2003.

Greene, Craig L. "When Employees Count too Much." *The White Paper*, Vol. 16, No. 6. November/December 2002.

Gross, Edward. "Organizational Structure and Organizational Crime," *White-Collar Crime: Theory and Research*, Gilbert Geis and Ezra Stotland, eds., Beverly Hills: Sage, 1980.

Hafner, Katie, and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York, NY: Simon & Shuster, 1991.

Hall, Jerome. *Theft, Law and Society*. 2nd Edition. 1960.

Hancock, William A. (Ed.). *Corporate Counsel's Guide to Legal Audits and Investigations*. Chesterfield, OH: Business Laws, Inc., 1997.

Hawkins, Keith. *Environment and Enforcement: Regulation and the Social Definition of Pollution*. Oxford: Oxford University Press, 1984.

Hayes, Read. *Retail Security and Loss Prevention*. Stoneham, MA: Butterworth-Heinemann, 1991.

Heilbroner, Robert. *In the Name of Profit*. New York, NY: Doubleday, 1973.

Henderson, M. Allen. *Flim Flam Man: How Con Games Work*. Boulder, CO: Paladin Press, 1985.

Herrnstein, Richard J. and Charles Murray. *The Bell Curve*. New York, NY: Simon and Shuster, 1994

Hetherington, Cynthia and Michael L. Sankey. *The Manual to Online Public Records*. Tempe, AZ: BRB Publications, Inc., 2008.

Hirschi, Travis. *Causes of Delinquency*. Berkeley, CA: University of California Press, 1969.

BIBLIOGRAPHY

Hobbes, Thomas. *Leviathan*. London: Andrew Crooke, 1651.

Hochstedler, Ellen. *Corporations as Criminals*. Beverly Hills, CA: Sage Publications, 1984.

Hollinger, Richard C. and John P. Clark. *Theft by Employees*. Lexington, KY: Lexingtion Books, 1983.

Hough, Harold. *Satellite Surveillance*. Port Townsend, WA: Loompanics Unlimited, 1991.

Hylas, R.E. and R.H. Ashton. "Audit Detection of Financial Statement Errors," *The Accounting Review*. Vol. LVII, No. 4.

Inbau, Fred E., John E. Reid, and Joseph P. Buckley. *Criminal Interrogation and Confessions*. Baltimore, MD: Wilkins, 1986.

Inciardi, James A. *Criminal Justice*. 3rd ed. San Diego, CA: Harcourt Brace Jovanovich, 1990.

Ingram, Donna. "Revenue Inflation and Deflation." *The White Paper*, Vol. 16, No. 6. November/December 2002.

Inkeles, Alex. *National Character: A Psycho-Social Perspective*. New Brunswick: Transaction Publishers, 1997.

Institute of Internal Auditors. *International Professional Practices Framework*. 2009.

Institute of Internal Auditors, the American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners. *Managing the Business Risk of Fraud: A Practical Guide.* 2008

Jaspan, Norman. *Mind Your Own Business*. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1974.

Javelin Strategy & Research. "2011 Identity Fraud Survey Report." Accessed Sept. 2012. http://www.identityguard.com/downloads/javelin-2011-identity-fraud-survey-report.pdf.

Kant, Immanuel. *Foundations of the Metaphysics of Morals* (originally published in 1785), translated by Lewis W. Beck, Indianapolis, IN.: The Bobbs-Merrill Company, Inc., 1959.

Kant, Immanuel. *Lectures on Ethics*. New York, NY: Harper & Row, 1963.

Kellogg, Irving. *How to Find Negligence and Misrepresentations in Financial Statements*. Colorado Springs, CO: Shepard's/McGraw-Hill, 1983.

Ketz, J. Edward. *Hidden Financial Risks: Understanding Off-Balance Sheet Accounting*. Hoboken, NJ: John Wiley & Sons, 2003.

Kimmel, Paul D., Jerry J. Weygandt, Donald E. Kieso. *Financial Accounting: Tools for Business Decision Making, 3rd Edition*. New York, NY: John Wiley & Sons, 2004.

Koletar, Joseph W. *Fraud Exposed: What You Don't Know Could Cost Your Company Millions*. Hoboken, NJ: John Wiley & Sons, 2003.

Kramer, W. Michael. *Investigative Techniques in Complex Financial Crimes*. Washington, D.C.: National Institute on Economic Crime, 1988.

Langsted, Lars B., Peter Garde, and Vagn Greve. *Criminal Law Denmark, 2nd Ed.* Copenhagen: DJOF Publishing, 2004.

Lanza, Richard B. *Proactively Detecting Occupational Fraud Using Computer Audit Reports*. IIA Research Foundation, 2003.

BIBLIOGRAPHY

Leventhal, G. S. "What Should Be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships." In K. Gergen, M. Greenberg, and R. Willis, eds., *Social Exchanges: Advances in Theory and Research*. New York, NY: Plenum, 1980.

Link, Frederick C., and D. Glenn Foster. *The Kinesic Interview Technique.* Interrotec Press, 1980.

Lundelius Jr., Charles R. *Financial Reporting Fraud: A Practical Guide to Detection and Internal Control*. New York, NY: AICPA, Inc. 2003.

Madden, Carl. "Forces Which Influence Ethical Behavior." In Clarence Walton (ed.), *The Ethics of Corporate Conduct*. Englewood Cliffs, NJ: Prentice Hall, 1977

Maggin, Donald L. Bankers. *Builders, Knaves, and Thieves: The $300 Million Scam at ESM*. Chicago, IL: Contemporary Books, 1989.

Mancino, Jane. "The Auditor and Fraud." *Journal of Accountancy*. April 1997.

Mann, Kenneth. *Defending White-Collar Crime: A Portrait of Attorneys at Work*. New Haven, CT: Yale University Press, 1985.

Marcella, Albert J., William J. Sampias and James K. Kincaid. *The Hunt for Fraud: Prevention and Detection Techniques*. Altamonte Springs, FL: Institute of Internal Auditors, 1994.

Margolis, J. "Conflicts of Interest and Conflicting Interests." In T. Beauchamp and N.E. Bowie (eds.), Ethical Theory and Business. Englewood Cliffs, NJ: Prentice Hall, 1979

McCaghy, Charles H. *Deviant Behavior: Crime, Conflict, and Interest Groups*, New York, NY: Macmillan, 1976.

Mill, John Stuart. *Utilitarianism*. Indianapolis, IN: The Bobbs-Merrill Company, Inc., 1957.

Miller, Norman C. *The Great Salad Oil Swindle*. Baltimore, MD: Penguin Books, 1965.

Moffit, Donald (Ed.). *Swindled! Classic Business Frauds of the Seventies.* New York, NY: Dow Jones & Co, 1976.

Moran, William B. *Covert Surveillance & Electronic Penetration.* Port Townsend, WA: Loompanics Unlimited, 1983

Moritz, Scott. "Don't Get Burned by Smiling CEO Candidates." *The White Paper*, Vol. 16, No. 5. September/October 2002.

Mott Graham M. *How to Recognize and Avoid Scams, Swindles, and Rip-Offs*. Littleton, CO: Golden Shadows Press, 1992.

Murphy, T. Gregory. *Asset Forfeiture: Uncovering Assets Laundered Through a Business.* Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance, 1992.

Naftalis, Gary P. (Ed.). *White-Collar Crimes*. Philadelphia, PA: American Law Institute—American Bar Association, 1980.

Nash, Jay Robert. *Hustlers & Con Men: An Anecdotal History of the Confidence Man and His Games*. New York, NY: Lippincott, 1976.

National Commission on Fraudulent Financial Reporting. *Report of the National Commission on Fraudulent Financial Reporting*. New York, NY: American Institute of Certified Public Accountants, 1987.

National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Academy Press, 1991.

BIBLIOGRAPHY

Noonan, John T. Jr. *Bribes*. New York, NY: Macmillan Publishing Company, 1984.

O'Brian, Keith. *Cut Your Losses*! Bellingham: International Self-Press Ltd., 1996.

O'Connell, E. Paul. "Is a Ruse the Best Route?" Security Management. December 1995.

O'Gara, John D. *Corporate Fraud: Case Studies in Detection and Prevention*. Hoboken, NJ: John Wiley & Sons, Inc., 2004.

Olien, Rover M. and Diana Davids Olien. *Easy Money: Oil Promoters and Investors in the Jazz Age*. Chapel Hill, NC: University of NC Press, 1990.

Organization for Economic Cooperation and Development. *G20/OECD Principles of Corporate Governance*. September 2015.

Patterson, James and Peter Kim. *The Day America Told the Truth*. New York, NY: Prentice Hall Publishing, 1991.

Pizzo, Stephen et al. *Inside Job. The Looting of America's Savings and Loans*. New York, NY: McGraw-Hill, 1991.

Powis, Robert E. *The Money Launderers: Lessons From the Drug Wars X How Billions of Illegal Dollars are Washed Through Banks and Businesses*. Chicago, IL: Probus Publishing Company, 1992.

Poynter, Dan. *The Expert Witness Handbook*. Santa Barbara, CA: Para Publishing, 1997.

Rabon, Don. *Investigative Discourse Analysis*. Durham, NC: Carolina Academic Press, 1994.

Rapp, Burt. *Check Fraud Investigation*. Port Townsend, WA: Loompanics Unlimited, 1991.

Rapp, Burt. *Credit Card Fraud*. Port Townsend, WA: Loompanics Unlimited, 1991.

Reiss, Albert J., Jr. and Albert Biderman. *Data Sources on White-Collar Law-Breaking*. Washington, D.C.: National Institute of Justice, U.S. Department of Justice, 1980.

Rezaee, Zabiollah. *Financial Statement Fraud: Prevention and Detection*. New York, NY: John Wiley & Sons, Inc. 2002.

Robertson, Jack C. *Auditing, Seventh Edition*. Boston, MA: BPI Irwin, 1991.

Romney, Marshall B., W. Steve Albrecht, and D. J. Cherrington. "Red-flagging the White-Collar Criminal," *Management Accounting*. March 1980.

Sarnoff, Susan K. *Paying For Crime*. Westport, CT: Praeger, 1996.

Seidler, Lee J., Fredrick Andrews, and Marc J. Epstein. *The Equity Funding Papers: the Anatomy of a Fraud*. New York, NY: John Wiley & Sons, 1997.

Schrager, Laura Shill and James F. Short, Jr. "Toward a Sociology of Organizational Crime." *Social Problems*, June 1978: 407–419.

Schulte, Fred. *Fleeced!* Amherst, MA: Prometheus Books, 1995.

Sharp, Kathleen. *In Good Faith*. New York, NY: St. Martin's Press, 1995.

Shea, Gordon. *Practical Ethics*. New York, NY: American Management Association, 1988.

Siegel, Larry J. *Criminology, 4th Edition*. New York, NY: West Publishing Company, 1992.

BIBLIOGRAPHY

Sifakis, Carl. *Hoaxes and Scams. A Compendium of Deceptions, Ruses and Swindles.* New York, NY: Facts on File, 1993.

Silk, Leonard Solomon and David Vogel. *Ethics and Profits: The Crisis in Confidence in American Business*. New York, NY: Simon & Schuster, 1976

Silverstone, Howard and Michael Sheetz. *Forensic Accounting and Fraud Investigation for Non-Experts*. Hoboken, NJ: John Wiley & Sons, 2004.

Singer, Marcus G. *Generalization in Ethics*. New York, NY: Atheneum, 1971

Skinner, B.F. *Science and Human Behavior*. New York, NY: Macmillan Publishing Co., 1953.

Skinner, B.F. *Walden Two*. Indianapolis, IN: Hacket Publishing Company, 1948.

Snyder, Neil H., O. Whitfield, William J. Kehoe, James T. McIntyre, Jr., and Karen E. Blair. *Reducing Employee Theft: A Guide to Financial and Organizational Controls*. New York, NY: Quorum Books, 1991.

Somers, Leigh Edward. *Economic Crimes: Investigative Principles and Techniques.* New York, NY: Clark Boardman Company, Ltd., 1984.

Steller, Max, and Guenter Koehnken. "Criteria-Based Statement Analysis." In *Psychological Methods in Criminal Investigation and Evidence*, edited by David C. Raskin, 217–245. New York: Springer Publishing Co., 1989.

Stone, Christopher. *Where the Law Ends: The Social Control of Corporate Behavior*. New York, NY: Harper & Row, 1975.

Summerford, Ralph Q. and Robin E. Taylor. "Avoiding Embezzlement Embarrassment (and Worse)." *The White Paper*, Vol. 17, No. 6. November/December 2003.

Sutherland, Edwin H. *Principles of Criminology*. 3rd ed. Chicago, IL: J.B. Lippincott Company, 1939.

Sutherland, Edwin H. *White-Collar Crime.* New York, NY: Dryden Press, 1949.

Suthers, John W. And Gary L. Shupp. *Fraud & Deceit: How to Stop Being Ripped Off*. New York, NY: Arco, 1982.

Thomas, William C. "The Rise and Fall of Enron." *Journal of Accountancy*. April 2002.

Thornhill, William T. *Forensic Accounting: How to Investigate Financial Fraud*. Burr Ridge, IL: Irwin Professional Publishing, 1995.

Titus, Harold T., and Morris Keeton. *Ethics for Today. 4th ed.*, New York, NY: America Book Stratford Press, Inc., 1966.

Tyler, Tom R. *Why People Obey the Law*. New Haven, CT: Yale University Press, 1990.

Van Drunen, Guido. "Traveling the World in Style on the Company's Nickel." *The White Paper*, Vol. 16, No. 1. January/February 2002.

Vaughan, Diane. *Controlling Unlawful Organizational Behavior.* Chicago, IL: The University of Chicago Press, 1983.

Vaughan, Diane. "Transaction Systems and Unlawful Organizational Behavior." *Social Problems*, 29:373-380.

Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, IL: University of Chicago Press, 1996.

BIBLIOGRAPHY

Villa, John K. *Banking Crimes: Fraud, Money Laundering, and Embezzlement*. Deerfield, IL: Clark, Boardman, Callaghan, 1991.

Watson, Douglas M. "Whom Do You trust? Doing Business and Deterring Fraud in a Global e-Marketplace." *The White Paper*, Vol. 16, No. 2. March/April 2002.

Weisburd, David, Stanton Wheeler, Elin Waring, and Nancy Bode. *Crimes of the Middle Classes: White-Collar Offenders in the Federal Courts*. New Haven, CT: Yale University Press, 1991.

Wells, Joseph T. (Ed.) *Computer Fraud Casebook: The Bytes that Bite*. Hoboken, NJ: John Wiley & Sons, 2009.

Wells, Joseph T. *Corporate Fraud Handbook, Fourth Edition.* Hoboken, NJ: John Wiley & Sons, 2013.

Wells, Joseph T. and Laura Hymes. (Ed.) *Corruption Casebook: The View from Under the Table*. Hoboken, NJ: John Wiley & Sons, 2012.

Wells, Joseph T. *The Encyclopedia of Fraud.* Austin, TX: ACFE, 2006.

Wells, Joseph T. (Ed.) *Financial Statement Fraud Casebook: Baking the Ledgers and Cooking the Books*. Hoboken, NJ: John Wiley & Sons, 2011.

Wells, Joseph T. (Ed.) *Fraud Casebook: Lessons from the Bad Side of Business.* Hoboken, NJ: John Wiley & Sons, 2007.

Wells, Joseph T. *Fraud Examination: Investigative and Audit Procedures*. New York, NY: Quorum Books, 1992.

Wells, Joseph T. (Ed.) *Internet Fraud Casebook: The World Wide Web of Deceit*. Hoboken, NJ: John Wiley & Sons, 2010.

Wells, Joseph T. *Occupational Fraud and Abuse*. Austin, TX: Obsidian Publishing Company, Inc, 1997.

Wells, Joseph T., Tedd A. Avey, G. Jack Bologna, and Robert J. Lindquist. *The Accountant's Handbook of Fraud and Commercial Crime*. Toronto: Canadian Institute of Chartered Accountants, 1992.

Weston, Paul B., Kenneth M. Wells. *Criminal Investigation: Basic Perspectives*, 6th Ed. Englewood Cliffs, NJ: Prentice Hall, 1994.

Wheelwright, Phillip. *A Critical Introduction to Ethics*, 3rd ed. Indianapolis, IN.: Odyssey Press, 1959.

Whitlock, Charles R. *Easy Money*. New York, NY: Kensington Books, 1994.

Williamson, Oliver E. *Markets and Hierarchies: Analysis and Antitrust Implications*. New York, NY: Free Press, 1975.

Wilson, James Q and Richard J. Herrnstein. *Crime and Human Nature.* New York, NY: Simon and Shuster, 1985.

Wold, Geoffrey H. and Robert F. Shriver. *Computer Crime: Techniques for Preventing and Detecting Crime in Financial Institutions*. Rolling Meadows, IL: Bankers Publishing Company, 1989.

Yeager, Peter. "Industrial Water Pollution," in Michael Tonry and Albert J. Reiss, Jr., eds., *Beyond the Law: Crime in Complex Organizations*. Chicago, IL: University of Chicago Press, 1993.

Zack, Gerard M. *Fraud and Abuse in Nonprofit Organizations: A Guide to Prevention and Detection*. Hoboken, NJ: John Wiley & Sons, 2003.