SECTION I

INTRODUCTION TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

CHAPTER 1

CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

LEARNING OBJECTIVES

After reading this chapter, you should be able to do the following:

- **1-1** Define fraud and identify a potentially fraudulent situation.
- **1-2** Differentiate between fraud and abuse.
- **1-3** Define financial forensics and identify an appropriate methodology for a given financial forensic fact pattern.
- **1-4** Differentiate the roles of auditing, fraud examination, and financial forensics.
- **1-5** Explain the theory of the fraud triangle.
- **1-6** List the legal elements of fraud.
- **1-7** Identify common fraud schemes.
- **1-8** Give examples of nonfraud forensics and litigation advisory engagements.
- **1-9** Describe the fraud examiner/financial forensic professional's approach to investigations.
- **1-10** Explain fraud examination methodology.

WHAT IS FRAUD?

Imagine that you work in the accounts payable department of your company, and you discover that your boss is padding his business expenses with personal expenses. Consider this: Wal-Mart legend, Thomas M. Coughlin, who was described as a protégé and old hunting buddy of the company's late founder, Sam Walton, was forced to resign on March 25, 2005, from Wal-Mart's Board of Directors. Mr. Coughlin, fifty-five years old at the time, periodically had subordinates create fake invoices to get the company to pay for his personal expenses. The questionable activity appeared to involve dozens of transactions over more than five years, including hunting vacations, custom-made alligator boots, and an expensive dog pen for his family home. Wal-Mart indicated that it found questionable transactions totaling between $100,000 and $500,000. In his last year, Mr. Coughlin's compensation totaled more than $6 million. Interestingly, Mr. Coughlin was an outspoken critic of corporate chicanery. In 2002, he told the *Cleveland Plain Dealer*, "Anyone who is taking money from associates and shareholders ought to be shot."[1]

Answer these questions:

1. What would you do?
2. Should you report it to anyone?
3. Who could you trust?
4. Is this fraud?
5. If you don't report it, are you complicit in fraud?

Fraud, sometimes referred to as the fraudulent act, is an intentional deception, whether by omission or co-mission, that causes its victim to suffer an economic loss and/or the perpetrator to realize a gain. A simple working definition of fraud is theft by deception.

Legal Elements of Fraud

Under common law, fraud includes four essential elements:

1. A material false statement
2. Knowledge that the statement was false when it was spoken

3. Reliance on the false statement by the victim
4. Damages resulting from the victim's reliance on the false statement

In the broadest sense, fraud can encompass any crime for gain that uses deception as its principal technique. This deception is implemented through fraud schemes: specific methodologies used to commit and conceal the fraudulent act. There are three ways to relieve a victim of money illegally: force, trickery, or larceny. Those offenses that employ trickery are frauds.

The legal definition of fraud is the same whether the offense is criminal or civil; the difference is that criminal cases must meet a higher burden of proof. For example, let's assume an employee who worked in the warehouse of a computer manufacturer stole valuable computer chips when no one was looking and resold them to a competitor. This conduct is certainly illegal, but what law has the employee broken? Has he committed fraud? The answer, of course, is that it depends. Let us briefly review the legal ramifications of the theft.

The legal term for stealing is larceny, which is defined as "felonious stealing, taking and carrying, leading, riding, or driving away with another's personal property, with the intent to convert it or to deprive the owner thereof."[2] In order to prove that a person has committed larceny, we would need to prove the following four elements:

1. There was a taking or carrying away
2. of the money or property of another
3. without the consent of the owner and
4. with the intent to deprive the owner of its use or possession.

In our example, the employee definitely carried away his employer's property, and we can safely assume that this was done without the employer's consent. Furthermore, by taking the computer chips from the warehouse and selling them to a third party, the employee clearly demonstrated intent to deprive his employer of the ability to possess and use those chips. Therefore, the employee has committed larceny.

The employee might also be accused of having committed a tort known as conversion.[3] Conversion, in the legal sense, is "an unauthorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition or the exclusion of the owner's rights."[4] A person commits a conversion when he or she takes possession of property that does not belong to him or her and thereby deprives the true owner of the property for any length of time. The employee in our example took possession of the computer chips when he stole them, and, by selling them, he has deprived his employer of that property. Therefore, the employee has also engaged in conversion of the company's property.

Furthermore, the act of stealing the computer chips also makes the employee an embezzler. "To embezzle means wilfully to take, or convert to one's own use, another's money or property of which the wrongdoer acquired possession lawfully, by reason of some office or employment or position of trust." The key words in that definition are "acquired possession lawfully." In order for an embezzlement to occur, the person who stole the property must have been entitled to possession of the property at the time of the theft. Remember, possession is not the same as ownership. In our example, the employee might be entitled to possess the company's computer chips (to assemble them, pack them, store them, etc.), but clearly the chips belong to the employer, not the employee. When the employee steals the chips, he has committed embezzlement.

We might also observe that some employees have a recognized fiduciary relationship with their employers under the law. The term *fiduciary*, according to *Black's Law Dictionary*, is of Roman origin and means "a person holding a character analogous to a trustee, in respect to the trust and confidence involved in it and the scrupulous good faith and candor which it requires. A person is said to act in a 'fiduciary capacity' when the business which he transacts, or the money or property which he handles, is not for his own benefit, but for another person, as to whom he stands in a relation implying and necessitating great confidence and trust on the one part and a high degree of good faith on the other part."[5] In short, a fiduciary is someone who acts for the benefit of another.

Fiduciaries have a duty to act in the best interests of the person whom they represent. When they violate this duty, they can be liable under the tort of breach of fiduciary duty. The elements of this cause of action vary among jurisdictions, but in general they consist of the following:

1. A fiduciary relationship existed between the plaintiff and the defendant.
2. The defendant (fiduciary) breached his or her duty to the plaintiff.
3. The breach resulted in either harm to the plaintiff or benefit to the fiduciary.

A fiduciary duty is a very high standard of conduct that is not lightly imposed. The duty depends upon the existence of a fiduciary relationship between the two parties. In an employment scenario, a fiduciary relationship is usually found to exist only when the employee is "highly trusted" and enjoys a confidential or special relationship with the employer. Practically speaking, the law generally recognizes a fiduciary duty only for officers and directors of a company, not for ordinary employees. (In some cases a quasi-fiduciary duty may exist for employees who are in possession of trade secrets; they have a duty not to disclose that confidential information.) The upshot is that the employee in our example most likely would not owe a fiduciary duty to his employer, and therefore he would not be liable for breach of fiduciary duty. However, if the example were changed so that an officer of the company stole a trade secret, that tort might apply.

But what about fraud? Recall that fraud always involves some form of deceit. If the employee in question simply walked out of the warehouse with a box of computer chips under his or her coat, this would not be fraud, because there is no deceit involved. (Although many would consider this a deceitful act, what we're really talking about when we say deceit, as reflected in the elements of the offense, is some sort of material false statement that the victim relies upon).

Suppose, however, that before he put the box of computer chips under his coat and walked out of the warehouse, the employee tried to cover his trail by falsifying the company's inventory records. Now the character of the crime has changed. Those records are a statement of the company's inventory levels, and the employee has knowingly falsified them. The records are certainly material, because they are used to track the amount of inventory in the warehouse, and the company relies on them to determine how much inventory it has on hand, when it needs to order new inventory, etc. Furthermore, the company has suffered harm as a result of the falsehood, because it now has an inventory shortage of which it is unaware.

Thus, all four attributes of fraud have now been satisfied: the employee has made a material false statement; the employee had knowledge that the statement was false, the company relied upon the statement, and the company has suffered damages. As a matter of law, the employee in question could be charged with a wide range of criminal and civil conduct: fraud, larceny, embezzlement, or conversion. As a practical matter, he or she will probably only be charged with larceny. The point, however, is that occupational fraud always involves deceit, and acts that look like other forms of misconduct, such as larceny, may indeed involve some sort of fraud. Throughout this book, we study not only schemes that have been labeled fraud by courts and legislatures but any acts of deceit by employees that fit our broader definition of occupational fraud and abuse.

Major Categories of Fraud

Asset misappropriations involve the theft or misuse of an organization's assets. (Common examples include skimming revenues, stealing inventory, and payroll fraud.)

Corruption entails the unlawful or wrongful misuse of influence in a business transaction to procure personal benefit, contrary to an individual's duty to his or her employer or the rights of another. (Common examples include accepting kickbacks and engaging in conflicts of interest.)

Financial statement fraud and other fraudulent statements involve the intentional misrepresentation of financial or nonfinancial information to mislead others who are relying on it to make economic decisions. (Common examples include overstating revenues, understating liabilities or expenses, or making false promises regarding the safety and prospects of an investment.)

Enron founder Ken Lay and former chief executive officer (CEO) Jeff Skilling were convicted in May 2006 for their respective roles in the energy company's collapse in 2001. The guilty verdict against Lay included conspiracy to commit securities and wire fraud, but he never served any prison time because he died of a heart attack two months after his conviction. Skilling, however, was sentenced on October 23, 2006, to twenty-four years for conspiracy, fraud, false statements, and insider trading. In addition, Judge Lake ordered Skilling to pay $45 million into a fund for Enron employees. Former Enron chief financial officer (CFO) Andrew Fastow received a relatively light sentence of six years for his role, after cooperating with prosecutors in the conviction of Lay and Skilling.[6] Enron was a $60 billion victim of accounting maneuvers and shady business deals that also led to thousands of lost jobs and more than $2 billion in employee pension plan losses.

If you were working at Enron and had knowledge of this fraud, what would you do?

On January 14, 2002, a seven-page memo, written by Sherron Watkins, was referred to in a *Houston Chronicle* article. This memo had been sent anonymously to Kenneth Lay and begged the question, "Has Enron Become a Risky Place to Work?" For her role as whistleblower, Sherron Watkins was recognized along with WorldCom's Cynthia Cooper and the FBI's Coleen Rowley as *Time* Magazine's Person of the Year in 2002.

The Association of Certified Fraud Examiners defines financial statement fraud as the intentional, deliberate misstatement or omission of material facts or accounting data that is misleading and, when considered with all the information made available, that would cause the reader to change or alter his or her judgment or decision.[7] In other words, the statement constitutes intentional or reckless conduct, whether by act or omission, that results in material misleading financial statements.[8]

Even though the specific schemes vary, the major areas involved in financial statement fraud include the following:

1. Fictitious revenue (and related assets)
2. Improper timing of revenue and expense recognition
3. Concealed liabilities
4. Inadequate and misleading disclosures
5. Improper asset valuation
6. Improper and inappropriate capitalization of expenses

The essential characteristics of financial statement fraud are (1) the misstatement is material and intentional, and (2) users of the financial statements have been misled.

In recent years, the financial press has had an abundance of examples of fraudulent financial reporting. These include Enron, WorldCom, Adelphia, Tyco, and others. The common theme of all these scandals was a management team that was willing to "work the system" for its own benefit and a wide range of stakeholders—including employees, creditors, investors, and entire communities—that are still reeling from the losses. In response, Congress passed the Sarbanes–Oxley Act (SOX) in 2002. SOX legislation was aimed at auditing firms, corporate governance, executive management (CEOs and CFOs), officers, and directors. The assessment of internal controls, preservation of evidence, whistleblower protection, and increased penalties for securities fraud became a part of the new business landscape.

The ACFE 2008 Report to the Nation noted that financial fraud tends to be the least frequent of all frauds, accounting for only 10.3 percent. However, the median loss for financial statement fraud is approximately $2 million, more than thirteen times larger than the typical asset misappropriation and more than five times larger than the typical corruption scheme. In addition, when financial statement fraud has been identified, in 79 of 99 cases, other types of fraud are also being perpetrated.

The 2003 KPMG Fraud Survey also notes that financial statement fraud and health insurance fraud are the most costly schemes. In addition, the rate of occurrence of financial statement fraud more than doubled since the 2001 survey.

According to the 2005 PricewaterhouseCoopers Global Economic Crime Survey, there has been a 140 percent increase in the number of respondents reporting financial misrepresentation. Furthermore, almost 40 percent of the company respondents report significant collateral damage, such as loss of reputation, decreased staff motivation, and declining business relations. The survey also notes that most frauds involve a lack of internal controls (opportunity), the need to maintain expensive lifestyles (incentive), and the perpetrators' lack of awareness that their actions were wrong (rationalization).

Common Fraud Schemes

Table 1-1 depicts the most common fraud schemes.[9]

Suspected frauds can be categorized by a number of different methods, but they are usually referred to as either internal or external frauds. The latter refers to offenses committed by individuals against other individuals (e.g., con schemes), offenses by individuals against organizations (e.g., insurance fraud), or organizations against individuals (e.g., consumer frauds). Internal fraud refers to occupational fraud committed by one or more employees of an organization; this is the most costly and most common fraud. These crimes are more commonly referred to as occupational fraud and abuse.

TABLE 1-1 Common Fraud Schemes

Fraud Acts
Asset Misappropriation
- Cash
  - Larceny (theft)
  - Skimming (removal of cash before it hits books): Sales, A/R, Refunds, and Other
  - Fraudulent Disbursement
    - Billing Schemes - including shell companies, fictitious vendors, personal purchases
    - Payroll Schemes - ghost employees, commission schemes, workers compensation, and false hours and wages
    - Expense Reimbursement Schemes - including overstated expenses, fictitious expenses, and multiple reimbursements
    - Check Tampering
    - Register Disbursements including false voids and refunds
- Inventory and Other Assets
  - Inappropriate Use
  - Larceny (theft)

Corruption
- Conflicts of Interest (unreported or undisclosed)
- Bribery
- Illegal Gratuities
- Economic Extortion

False Statements
- Fraudulent Financial Statements
- False Representations (e.g., employment credentials, contracts, identification)

Specific Fraud Contexts
- Bankruptcy Fraud
- Contract and Procurement Fraud
- Money Laundering
- Tax Fraud
- Investment Scams
- Terrorist Financing
- Consumer Fraud
  - Identity Theft
  - Check and Credit Card Fraud
  - Computer and Internet Fraud
- Divorce Fraud (including hidden assets)
- Intellectual Property
- Business Valuation Fraud

Noteworthy Industry-Specific Fraud
- Financial Institutions
- Insurance Fraud
- Health Care Fraud
- Securities Fraud
- Public Sector Fraud

WHAT IS THE DIFFERENCE BETWEEN FRAUD AND ABUSE?

Obviously, not all misconduct in the workplace amounts to fraud. There is a litany of abusive practices that plague organizations, causing lost dollars or resources, but that do not actually constitute fraud. As any employer knows, it is hardly out of the ordinary for employees to do any of the following:

- Use equipment belonging to the organization
- Surf the Internet while at work
- Attend to personal business during working hours
- Take a long lunch, or a break, without approval

- Come to work late, or leave early
- Use sick leave when not sick
- Do slow or sloppy work
- Use employee discounts to purchase goods for friends and relatives
- Work under the influence of alcohol or drugs

The term *abuse* has taken on a largely amorphous meaning over the years, frequently being used to describe any misconduct that does not fall into a clearly defined category of wrongdoing. Webster's definition of abuse might surprise you. From the Latin word *abusus*, to consume, it means: "1. A deceitful act, deception; 2. A corrupt practice or custom; 3. Improper use or treatment, misuse." To deceive is "to be false; to fail to fulfill; to cheat; to cause to accept as true or valid what is false or invalid."

Given the commonality of the language describing both fraud and abuse, what are the key differences? An example illustrates: suppose that a teller was employed by a bank and stole $100 from her cash drawer. We would define that broadly as fraud. But if she earns $500 a week and falsely calls in sick one day, we might call that abuse—even though each act has the exact same economic impact to the company—in this case, $100.

And, of course, each offense requires a dishonest intent on the part of the employee to victimize the company. Look at the way in which each is typically handled within an organization, however: in the case of the embezzlement, the employee gets fired; there is also a possibility (albeit remote) that she will be prosecuted. But in the case in which the employee misuses her sick time, perhaps she gets reprimanded, or her pay might be docked for the day.

But we can also change the abuse example slightly. Let's say the employee works for a governmental agency instead of in the private sector. Sick leave abuse—in its strictest interpretation—could be a fraud against the government. After all, the employee has made a false statement (about her ability to work) for financial gain (to keep from getting docked). Government agencies can and have prosecuted flagrant instances of sick leave abuse. Misuse of public money in any form can end up being a serious matter, and the prosecutorial thresholds can be surprisingly low.

THE CRAZY EDDIE CASE

Adapted from The White Collar Fraud Web site by Sam E. Antar at http:www.whitecollarfraud.com

Eddie Antar was a retailing revolutionary in his day; he broke the price fixing environment that gripped the consumer electronics industry. To survive in this industry, Eddie circumvented the fair trade laws and discounted the consumer electronics merchandise he was selling. He faced retribution from the manufacturers who stopped shipping merchandise to him. Consequently, he had to purchase his inventory from trans-shippers and grey markets. He built up great customer loyalty in the process and his business volume expanded.

Like numerous other independent small businesses in America, Crazy Eddie paid many of its employees off the books. There was a company culture that believed that nothing should go to the government. Eddie Antar inspired intense loyalty from his employees, most of whom were family. It was us against them—customers, the government, insurance companies, auditors, and anyone else who did not serve the company's interests. The Antar family regularly skimmed profits from the business. If profits couldn't be increased through bait-and-switch tactics, the Antar clan would pocket the sales tax by not reporting cash sales.

The Four Phases of the Crazy Eddie Frauds

- *1969–1979: Skimming to reduce reported taxable income*
- *1979–1983: Gradual reduction of skimming to increase reported income and profit growth in preparation to take the company public*
- *September 13, 1984: Date of Crazy Eddie initial public offering*
- *1985–1986: Increasing Crazy Eddie's reported income to raise stock prices so insiders could sell their stock at inflated values*
- *1987: Crazy Eddie starts losing money. The main purpose of fraud at this stage is to "cover up" prior frauds resulting from the "double down" effect.*

From the Fraudster's Perspective

Sam E. Antar was a CPA and the CFO of the Crazy Eddie electronics chain in the 1980s when that securities fraud scandal hit. The fraud cost investors and creditors hundreds of millions of dollars, and it cost others their careers. In addition to

securities fraud, investigators later learned that the Crazy Eddie business was also involved in various other types of fraud, including skimming, money laundering, fictitious revenue, fraudulent asset valuations, and concealed liabilities and expenses, to name a few. Since then, Sam has shared his views—on white-collar crime, the accounting profession, internal controls, the Sarbanes–Oxley Act, and other related topics—with audiences around the country.

According to Sam, there are two types of white-collar criminal groups: (1) those with common economic interests (e.g., the Enrons and WorldComs) and (2) other cohesive groups (e.g., with family, religious, social, or cultural ties). Fraud is harder to detect in the second category because of behavioral and loyalty issues. Tone at the top is crucial here.

Contrary to the fraud triangle theory—incentive, opportunity, and rationalization—Sam insists that the Crazy Eddie fraud involved no rationalization. "It was pure and simple greed," he says. "The crimes were committed simply because we could. The incentive and opportunity was there, but the morality and excuses were lacking. We never had one conversation about morality during the 18 years that the fraud was going on." He contends that "White-collar criminals consider your humanity as a weakness to be exploited in the execution of their crimes and they measure their effectiveness by the comfort level of their victims." Sam's description of how the Crazy Eddie frauds were successfully concealed from the auditors for so long is a tale of what he refers to as "distraction rather than obstruction." For example, employees of the company wined and dined the auditors to distract them from conducting their planned audit procedures and to eat up the time allotted for the audit. As the end of the time frame approached, the auditors were rushed and didn't have time to complete many of their procedures. Fraudsters use "controlled chaos" to perpetrate their crimes successfully.

The accounting profession doesn't analyze auditor error and therefore learn from it. Sam's advice to the accounting profession, anti-fraud professionals, and Wall Street: "Don't trust, just verify, verify, verify." Audit programs are generic, and auditors have been too process-oriented. Sam recommends that auditors utilize the Internet for searchable items, such as statements to the media and quarterly earnings called *transcriptions*. A pattern of inconsistencies or contradictions found in these sources of information, compared to the financial statements and footnote disclosures, should raise red flags. As an example, Crazy Eddie's auditors never thought to check sales transactions to ensure that the deposits came from actual sales. They never considered that these funds came from previously skimmed money.

Sam believes that white-collar crime can be more brutal than violent crime because white-collar crime imposes a collective harm on society. On using incarceration as a general deterrent, Sam says, "No criminal finds morality and stops committing crime simply because another criminal went to jail."

WHAT IS FORENSIC ACCOUNTING?

A call comes in from a nationally known insurance company. Claims Agent Kathleen begins: "I have a problem and you were recommended to me. One of my insureds near your locale submitted an insurance claim related to an accounts receivable rider. The insurance claim totals more than $1 million, and they are claiming that the alleged perpetrator did not take any money and that their investigation to date indicates that no money is missing from the company. Can you assist with an investigation of this claim?"

She asks for your help to do the following:

1. Verify the facts and circumstances surrounding the claim presented by the insured
2. Determine whether accounting records have been physically destroyed
3. To the best of your ability, determine whether this is a misappropriation or theft of funds
4. If this is a theft of funds, attempt to determine by whom

Financial forensics is the application of financial principles and theories to facts or hypotheses at issue in a legal dispute and consists of two primary functions:

1. Litigation advisory services, which recognizes the role of the financial forensic professional as an expert or consultant
2. Investigative services, which makes use of the financial forensic professional's skills and may or may not lead to courtroom testimony

Financial forensics may involve either an attest or consulting engagement.[10] According to the AICPA, Forensic and Litigation Advisory Services (FLAS) professionals provide educational, technical, functional, and industry-specific services that often apply to occupational fraud, corruption, and abuse and to financial statement fraud cases. FLAS professionals may assist attorneys with assembling the financial information necessary either to bolster (if hired by the plaintiff) or to undercut (if hired by the defendant) a case. They can provide varying levels of support—from technical analysis and data mining, to a broader

approach that may include developing litigation strategies, arguments, and testimony in civil and criminal cases. Engagements may be criminal, civil, or administrative cases that involve economic damage claims, workplace or matrimonial disputes, or asset and business valuations.[11]

Forensic and litigation advisory services require interaction with attorneys throughout the engagement. Excellent communication skills are essential for effective mediation, arbitration, negotiations, depositions, and courtroom testimony. These communication skills encompass the use of a variety of means by which to express the facts of the case—oral, written, pictures, and graphs. Like all fraud and forensic accounting work, there is an adversarial nature to the engagements, and professionals can expect that their work will be carefully scrutinized by the opposing side.

THE FORENSIC ACCOUNTANT'S SKILL SET

Financial forensics *is* the intersection of financial principles and the law and, therefore, applies the (1) technical skills of accounting, auditing, finance, quantitative methods, and certain areas of the law and research; (2) investigative skills for the collection, analysis, and evaluation of evidential matter; and (3) critical thinking to interpret and communicate the results of an investigation.

Critical thinking, sometimes referred to as lateral thinking or thinking "outside the box," is a disciplined approach to problem solving. It is used as a foundation to guide our thought process and related actions.

CRITICAL THINKING EXERCISE

Everything needed to answer the question "How did they die?" is contained in the following passage.

Anthony and Cleopatra are lying dead on the floor in a villa. Nearby on the floor is a broken bowl. There is no mark on either of their bodies, and they were not poisoned. With this information, determine how they died.[12]

Clue: List all of your assumptions from the preceding passage.

This exercise requires the problem solver to guard against jumping to conclusions. Even though the fraud examiner or forensic accountant needs to think critically, the direction of the investigation is often guided by assumptions. The difficult challenge is not the questioning of assumptions that investigators had identified as assumptions; but the questioning of the assumptions that investigators are making without realizing that they have made them. That is why it is important that investigators continually challenge their investigative approach and outcomes to ensure that the investigation is moving toward a resolution—one that stands up to the scrutiny of others.

THE ROLE OF AUDITORS, FRAUD EXAMINERS, AND FORENSIC ACCOUNTANTS

Fraud examination, financial forensics, and traditional auditing are interrelated, yet they have characteristics that are separate and distinct. All require interdisciplinary skills to succeed—professionals in any of these fields must possess a capacity for working with numbers, words, and people.

Financial statement auditing acts to ensure that financial statements are free from material misstatement. Audit procedures, as outlined in PCAOB Auditing Standard No. 5 or AICPA Statement on Auditing Standards (SAS) No. 99, require that the auditor undertake a fraud-risk assessment. However, under generally accepted auditing standards (GAAS) auditors are not currently responsible for planning and performing auditing procedures to detect immaterial misstatements, regardless of whether they are caused by error or fraud. Allegations of financial statement fraud are often resolved through court action, and auditors may be called into court to testify on behalf of a client or to defend their audit work, a point at which auditing, fraud examination, and financial forensics intersect.

However, each discipline also encompasses separate and unique functional aspects. For example, fraud examiners often assist in fraud prevention and deterrence efforts that do not involve the audit of nonpublic companies or the legal system. Financial forensic professionals calculate economic damages, business or asset valuations, and provide litigation advisory services that may not involve allegations of fraud. Finally, most audits are completed without uncovering financial statement fraud or involving

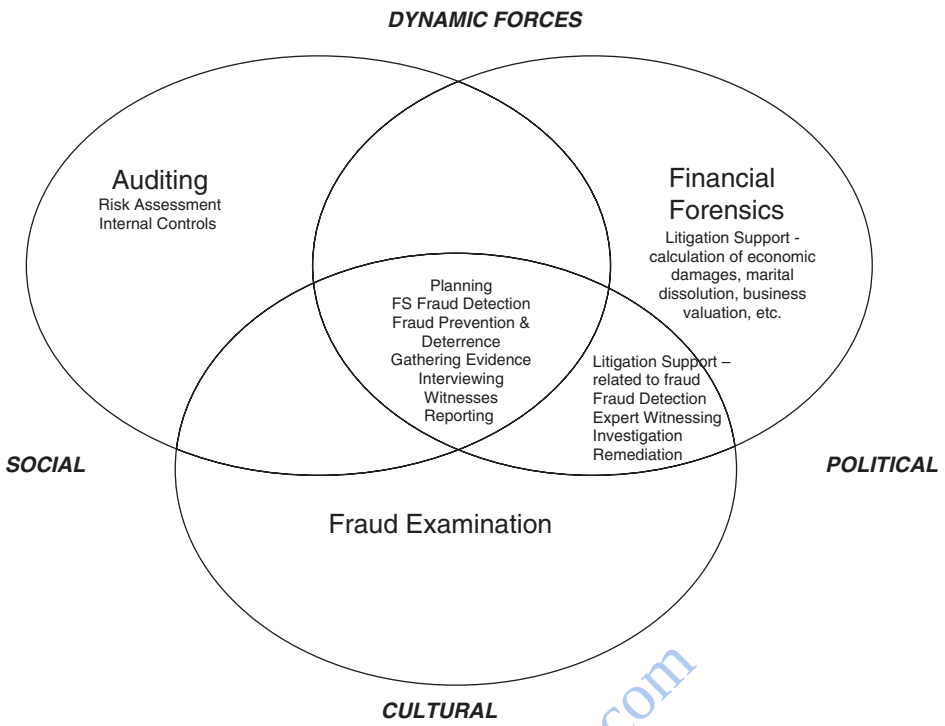


FIGURE 1-1 Auditing, Fraud Examination, and Financial Forensics

the legal system. Thus, as graphically presented in Figure 1-1, auditing, fraud examination, and financial forensics often use the same tools, but they also have responsibilities independent of the other.

The interrelationship among auditing, fraud examination, and financial forensics is dynamic and changes over time because of political, social, and cultural pressure. Because independent auditors operate in an environment impacted by SOX and SAS 99, they are expected to have adequate knowledge and skills in the area of fraud detection and deterrence. In addition, auditing, fraud examination, and financial forensic professionals often have skill sets in multiple areas and are able to leverage their skills and abilities from one area when working in others.[13]

Fraud examination is the discipline of resolving allegations of fraud from tips, complaints, or accounting clues. It involves obtaining documentary evidence, interviewing witnesses and potential suspects, writing investigative reports, testifying to findings, and assisting in the general detection and prevention of fraud. Fraud examination has many similarities to the field of financial forensics. Because the latter uses accounting or financial knowledge, skills, and abilities for courtroom purposes, financial forensics can involve not only the investigation of potential fraud, but a host of other litigation support services.

Similarly, fraud examination and auditing are related. Because most occupational frauds are financial crimes, there is necessarily a certain degree of auditing involved. But a fraud examination encompasses much more than just the review of financial data; it also involves techniques such as interviews, statement analyses, public records searches, and forensic document examination. There are also significant differences between the three disciplines in terms of their scope, objectives, and underlying presumptions. Table 1-2 summarizes the differences between the three disciplines.

Nevertheless, successful auditors, fraud examiners, and financial forensic professionals have several similar attributes; they are all diligent, detail-oriented, and organized critical thinkers, excellent listeners, and communicators.

THE BASICS OF FRAUD

Brian Lee excelled as a top-notch plastic surgeon. Lee practiced out of a large physician-owned clinic of assorted specialties. As its top producer, Lee billed more than $1 million annually and took home $300,000 to $800,000 per year in salary and bonus. During one four-year stretch, Lee also kept his own secret stash of unrecorded revenue—possibly hundreds of thousands of dollars.

TABLE 1-2 Differences between Auditing, Fraud Examination, and Financial Forensics

Issue	Auditing	Fraud Examination	Financial Forensics
Timing	**Recurring** Audits occur on a regular, recurring basis.	**Nonrecurring** Fraud examinations are conducted only with sufficient predication.	**Nonrecurring** Financial forensic engagements are conducted only after allegation of misconduct.
Scope	**General** The examination of financial statements for material misstatements.	**Specific** The purpose of the examination is to resolve specific allegations.	**Specific** The purpose of the examination is to resolve specific allegations.
Objective	**Opinion** An audit is generally conducted for the purpose of expressing an opinion on the financial statements and related information.	**Affix blame** The fraud examination's goal is to determine whether fraud has occurred and who is likely responsible.	**Determine financial impact** The financial forensic professional's goal is to determine whether the allegations are reasonable based on the financial evidence and, if so, the financial impact of the allegations.
Relationship	**Nonadversarial but skeptical** Historically, the audit process was non-adversarial. Since SOX and SAS 99, auditors use professional skepticism as a guide.	**Adversarial** Fraud examinations, because they involve efforts to affix blame, are adversarial in nature.	**Independent** A financial forensic professional calculates financial impact based on formulaic assumptions.
Methodology	**Audit techniques** Audits are conducted primarily by examining financial data using GAAS.	**Fraud examination techniques** Gathering the required financial and nonfinancial evidence to affix culpability.	**Financial forensic techniques** Gathering the required financial and nonfinancial evidence to examine the allegations independently and determine their financial impact.
Presumption	**Professional Skepticism** Auditors are required to approach audits with professional skepticism, as outlined in GAAS.	**Proof** Fraud examiners approach the resolution of a fraud by attempting to gather sufficient evidence to support or refute an allegation of fraud.	**Proof** Financial forensic professionals will attempt to gather sufficient evidence to support or refute the allegation and related damages.

Because plastic surgery is considered by many health insurance plans to be elective surgery, patients were required to pay their portion of the surgery fees in advance. The case that ultimately nailed Brian Lee involved Rita Mae Givens. Givens had elected rhinoplasty, surgery to reshape her nose, and, during her recovery, she reviewed her insurance policy and discovered that this procedure might be covered under her health insurance or, at least, counted toward her yearly deductible. In pursuit of seeking insurance reimbursement for her surgery, Givens decided to file a claim. She called the clinic office to request a copy of her invoice, but the cashier could find no record of her surgical or billing records. Despite the missing records, Givens had her cancelled check, proof that her charges had been paid. An investigator was called in, and Dr. Lee was interviewed several times over the course of the investigation. Eventually, he confessed to stealing payments from the elective surgeries, for which billing records were not required, particularly when payment was made in cash or a check payable to his name. Why would a successful, top-performing surgeon risk it all? Dr. Lee stated that his father and brother were both very successful; wealth was the family's obsession, and one-upmanship was the family's game. This competition drove each of them to see who could amass the most, drive the best cars, live in the nicest homes, and travel to the most exotic vacation spots.

Unfortunately, Lee took the game one step further and was willing to commit grand larceny to win. Luckily for Lee, the other doctors at the clinic decided not to prosecute or terminate their top moneymaker. Lee made full restitution of the money he had stolen, and the clinic instituted new payment procedures. Ironically, Dr. Lee admitted to the investigator that, if given the opportunity, he would probably do it again.[14]

Who Commits Fraud and Why

Fraudsters, by their very nature, are trust violators. They generally have achieved a position of trust within an organization and have chosen to violate that trust. According to the ACFE, owners and executives are involved in only about 23.3 percent of frauds but, when involved, steal approximately $834,000. Managers are the second most frequent perpetrators, committing 37.1 percent of frauds and wreaking $150,000 worth of damage, on average. Finally, line employees are the principle perpetrators in 39.7 percent of schemes, yielding company losses of approximately $70,000. Research suggests that although males are most frequently the perpetrators, in 40.9 percent of fraud cases, a woman is the principle perpetrator. Fraudsters are found in all age categories and educational achievement levels, but victim losses rise with both the age and education of the principle perpetrator. In 63.9 percent of the cases, the perpetrator acted alone; however, when fraudsters collude, the losses to the victim organization increase more than fourfold. The following profile summarizes the characteristics of the typical fraud perpetrator:

Fraud Perpetrator Profile	
Male[15]	Well Educated
Middle-Aged to Retired	Accountant, Upper Management or Executive
With the Company for Five or More Years	Acts Alone
Never Charged or Convicted of a Criminal Offense	

Regardless of whether fraud perpetrators are male or female, they look like average people. Perhaps the most interesting of all the characteristics listed is that fraudsters typically do not have a criminal background.[16] Furthermore, it is not uncommon for a fraud perpetrator to be a well-respected member of the community, attend church services regularly, and have a spouse and children.

Interestingly, in 92.6 percent of the fraud cases examined by the ACFE, the perpetrator had been with the victim organization for more than one year. Dr. W. Steve Albrecht, a pioneer researcher at Brigham Young University, notes: "Just because someone has been honest for 10 years doesn't mean that they will always be honest." Not surprisingly, the longer the tenure is, the larger the average loss is. In only 12.5 percent of the fraud cases examined did the perpetrator have any prior criminal history. In fact, the typical fraudster is not a pathological criminal, but rather a person who has achieved a position of trust. So the critical question remains, what causes good people to go bad?

The Fraud Triangle: Opportunity, Perceived Pressure, and Rationalization

Over the years, a hypothesis developed by Donald R. Cressey (1919–1987), which attempts to explain the conditions that are generally present when fraud occurs, has become better known as the "fraud triangle" (Figure 1-2). One leg of the triangle represents perceived pressure. The second leg is perceived opportunity, and the final leg denotes rationalization.

Perceived Pressure Many people inside any organizational structure have at least some access to cash, checks, or other assets. However, it is a perceived pressure that causes individuals to consider

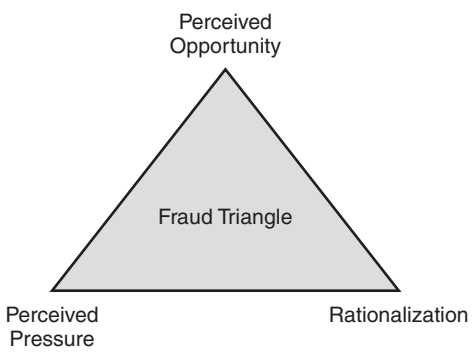


FIGURE 1-2 The Fraud Triangle: Perceived Pressure, Perceived Opportunity, and Rationalization

seriously availing themselves of the opportunity presented by, for example, an internal control weakness. Fraud pressures can arise from financial problems, such as living beyond one's means, greed, high debt, poor credit, family medical bills, investment losses, or children's educational expenses. Pressures may also arise from vices such as gambling, drugs, or an extramarital affair.

Financial statement fraud is often attributed to pressures, such as meeting analysts' expectations, deadlines, and cutoffs, or qualifying for bonuses. Finally, pressure may be the mere challenge of getting away with it or keeping up with family and friends. The word *perceived* is carefully chosen here. Individuals react differently to certain stimuli, and pressures that have no impact on one person's choices may dramatically affect another's. It is important that the fraud examiner or forensic accountant investigating a case recognize this facet of human nature.

Perceived Opportunity Whether the issue is management override, related to a financial statement fraud, or a breakdown in the internal control environment that allows the accounts receivable clerk to abscond with the cash and checks of a business, the perpetrator needs the opportunity to commit a fraud. Furthermore, when it comes to fraud prevention and deterrence, most accountants tend to direct their efforts toward minimizing opportunity through the internal control environment. However, internal controls are just one element of opportunity. Other integral ways to reduce opportunity include providing adequate training and supervision of personnel; effective monitoring of company management by auditors, audit committees, and boards of directors; proactive antifraud programs; a strong ethical culture; anonymous hotlines; and whistleblower protections.

The Perception of Detection Fraud deterrence begins in the employee's mind. Employees who perceive that they will be caught are less likely to engage in fraudulent conduct. The logic is hard to dispute. Exactly how much deterrent effect this concept provides depends on a number of factors, both internal and external. But internal controls can have a deterrent effect only when the employee perceives that such a control exists and is intended for the purpose of uncovering fraud. "Hidden" controls have no deterrent effect. Conversely, controls that are not even in place—but are perceived to be—have the same deterrent value.

Rationalization Finally, according to the fraud triangle hypothesis, the characteristic that puts fraudsters over the top is rationalization. How do perpetrators sleep at night or look at themselves in the mirror? The typical fraud perpetrator has no criminal history and has been with the victim company for some length of time. Because they generally are not habitual criminals and are in a position of trust, they must develop a rationalization for their actions in order to feel justified in what they are doing. Rationalizations may include an employee/manager's feeling of job dissatisfaction, lack of recognition for a job well done, low compensation, an attitude of "they owe me," "I'm only borrowing the money," "nobody is getting hurt," "they would understand if they knew my situation," "it's for a good purpose," or "everyone else is doing it."

The theory of rationalization, however, has its skeptics. Although, it is difficult to know for certain the thought process of a perpetrator, we can consider the following example. Let's say that the speed limit is sixty-five miles per hour, but I put my cruise control on seventy or seventy-five to keep up with the other lawbreakers. Do I consciously think to myself, "I'm breaking the law, so what is my excuse, my rationalization, if I am stopped for speeding by a police officer?" Most people don't think about that until the flashing lights appear in their rear view mirror. Is the thought process of a white-collar criminal really different from that of anyone else?

M.I.C.E

In addition to the fraud triangle, typical motivations of fraud perpetrators may be identified with the acronym M.I.C.E.:

Money
Ideology
Coercion
Ego

Money and ego are the two most commonly observed motivations. Enron, WorldCom, Adelphia, Pharmor, and ZZZ Best provide good examples of cases in which the convicted perpetrators seemed to be motivated by greed (money) and power (ego). Less frequently, individuals may be unwillingly pulled into

a fraud scheme (coercion). These lower-level individuals are often used to provide insight and testimony against the ringleaders and, as such, receive more lenient sentences or no sentence at all. Ideology is probably the least frequent motivation for white-collar crime, but society has seen this occur in the case of terrorism financing. With ideology, the end justifies the means, and perpetrators steal money to achieve some perceived greater good that furthers their cause. Although the M.I.C.E. heuristic oversimplifies fraudulent motivations, and some motivations fit multiple categories, it is easily remembered and provides investigators with a framework to evaluate motive.

Although the fraud triangle was developed to explain fraud, the same motivations can be used to understand financial disputes of all kinds. For example, consider the contract dispute in which company A claims that company B has not fulfilled its contractual obligation. Company B clearly recognizes that company personnel "walked off the job" before meeting the contract specifications. Assuming that companies A and B negotiated a fair, arms-length transaction, something must explain the otherwise unusual action of company B. In contractual disputes, the alleged wrongdoer clearly has the opportunity: that company can simply stop working. Related to pressure and rationalizations, possibly, company B had old equipment, a labor shortage, or a lack of technical expertise to operate under current conditions that have changed over time and is no longer qualified or able to operate profitably. These explanations created pressure on company B to consider not delivering the product to company A. Assume that company A and company B have been working together for many years. How does company B rationalize its behavior? Maybe company B management focuses on contractual ambiguities that were resolved unfavorably from its perspective and then uses that as a basis for the unfulfilled obligation. Consider the divorce situation, where the husband thinks that his former spouse is asking for a more generous settlement than he thinks is appropriate. The fact that his wife is asking for a settlement that is unreasonable (in his mind) may create pressure on him that he is doing the right thing by hiding assets. Furthermore, he may use the size of the settlement request as rationalization for arguing with her over the children. When money is involved, we may see individuals, companies, or organizations behave in ways that are out of character. In those situations, we may often be able to explain their actions in terms of the fraud triangle: pressure, opportunity, and rationalization.

The Cost of Fraud and Other Litigation

The cost of fraud, as estimated by the ACFE, is more than $990 billion annually. Even though this number is staggering in size, it hides the potentially disastrous impact at the organizational level. For example, if a company with a 10 percent net operating margin is a victim of a $500,000 fraud or loses a comparable amount as a result of a lawsuit, that company must generate incremental sales of $5 million to make up the lost dollars. If the selling price of the average product is $1,000 (a computer, for example), the company would need to sell an additional 5,000 units of product.

Organizations incur costs to produce and sell their products or services. These costs run the gamut: labor, taxes, advertising, occupancy, raw materials, research and development—and, yes, fraud and litigation. The cost of fraud and litigation, however, are fundamentally different from the other costs—the true expense of fraud and litigation is hidden, even if a portion of the cost is reflected in the profit and loss figures. Indirect costs of fraud and litigation can have far-reaching impact. For example, employees may lose jobs or be unable to obtain other employment opportunities; the company may have difficulty getting loans, mortgages, and other forms of credit because of the impact of fraud and litigation on the company's finances; the company's reputation in the community may be affected; and the company may become the subject of broader investigations. With regard to either litigation or fraud, prevention and deterrence are the best medicines. By the time a formal investigation is launched and the allegations are addressed within the legal arena, the parties have already incurred substantial cost.

ACFE 2008 Report to the Nation on Occupational Fraud and Abuse

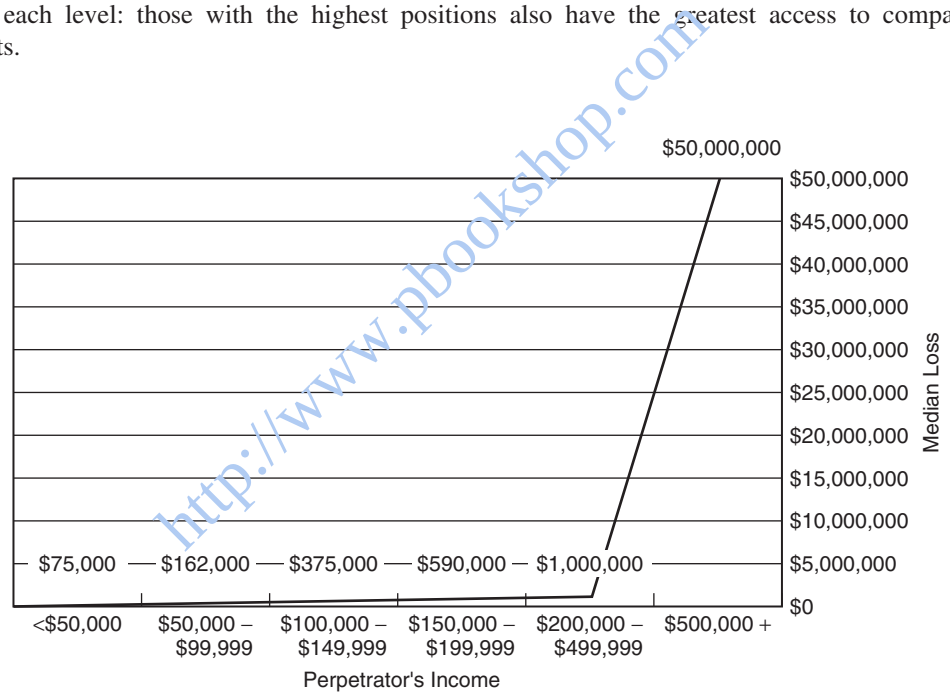
The ACFE began a major study of occupational fraud cases in 1993, with the primary goal of classifying occupational frauds and abuses by the methods used to commit them. There were other objectives, too. One was to get an idea of how antifraud professionals—CFEs—perceive the fraud problems in their own companies.

The ACFE 2008 Report to the Nation on Occupational Fraud and Abuse is a result of what has now become a biannual national fraud survey of those professionals who deal with fraud and abuse on a daily basis.

The Perpetrators of Fraud Another goal of this research was to gather demographics on the perpetrators: How old are they? How well educated? What percentage of offenders are men? Were there any identifiable correlations with respect to the offenders? Participants in the 2008 National Fraud Survey provided the following information on the perpetrators' position, gender, age, education, tenure, and criminal histories.

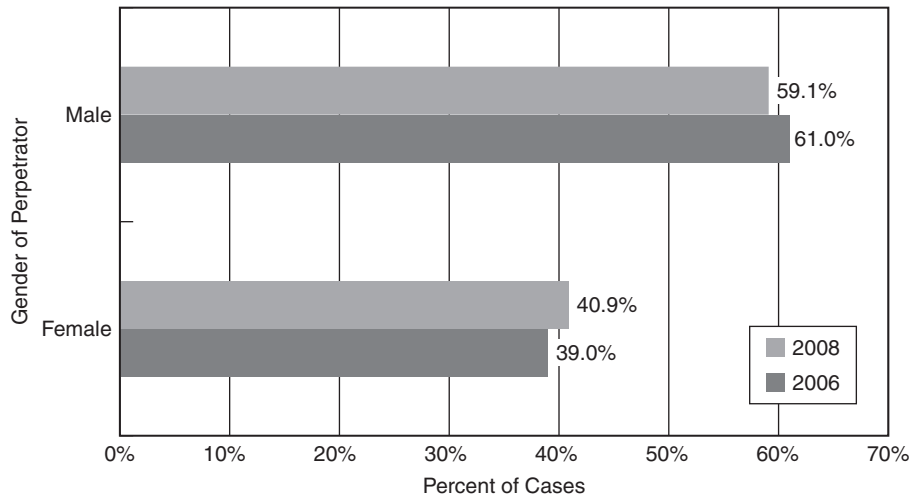
The Effect of Position on Median Loss Fraud losses tended to rise based on the perpetrator's level of authority within an organization. Generally, employees with the highest levels of authority are the highest paid as well. Therefore, it was not a surprise to find a positive correlation between the perpetrators' annual income and the size of fraud losses. As incomes rose, so did fraud losses.

The lowest median loss of $75,000 was found in frauds committed by employees earning less than $50,000 per year. Although the median loss in schemes committed by those earning between $200,000 and $499,999 annually reached $1 million, the median loss skyrocketed to $50 million for executive/owners earning more than $500,000 per year. Approximately 23 percent have the schemes in the executive/owner category also involved financial statement fraud, which might help explain the extraordinarily high median loss. The differences in the loss amounts were likely a result of the degree of financial control exercised at each level: those with the highest positions also have the greatest access to company funds and assets.

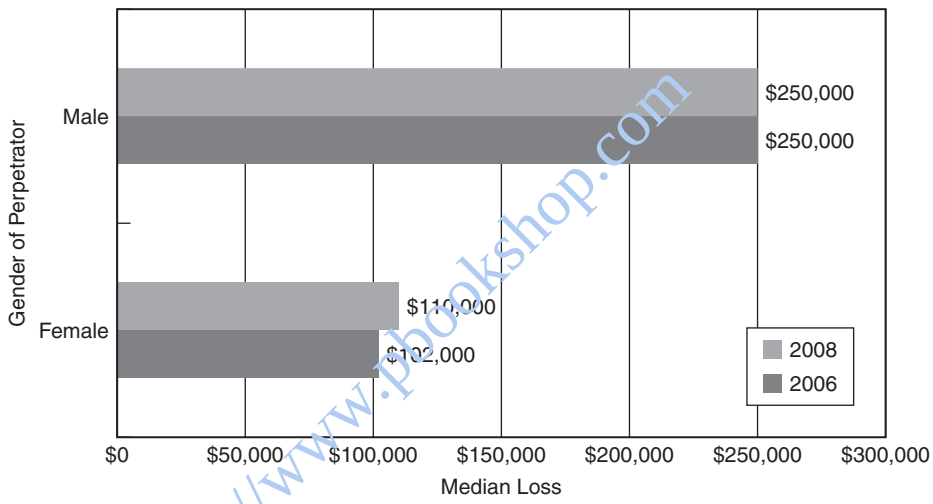


Median Loss vs. Perpetrator's Income

The Effect of Gender on Median Loss The 2008 ACFE Report to the Nation showed that male employees caused median losses that were more than twice as large as those of female employees; the median loss in a scheme caused by a male employee was $250,000, whereas the median loss caused by a female employee was $110,000. The most logical explanation for this disparity seems to be the "glass ceiling" phenomenon. Generally, in the United States, men occupy higher-paying positions than their female counterparts. And as we have seen, there is a direct correlation between median loss and position. Furthermore, in addition to higher median losses in schemes where males were the principal perpetrators, men accounted for 59.1 percent of the cases, as the following chart shows.

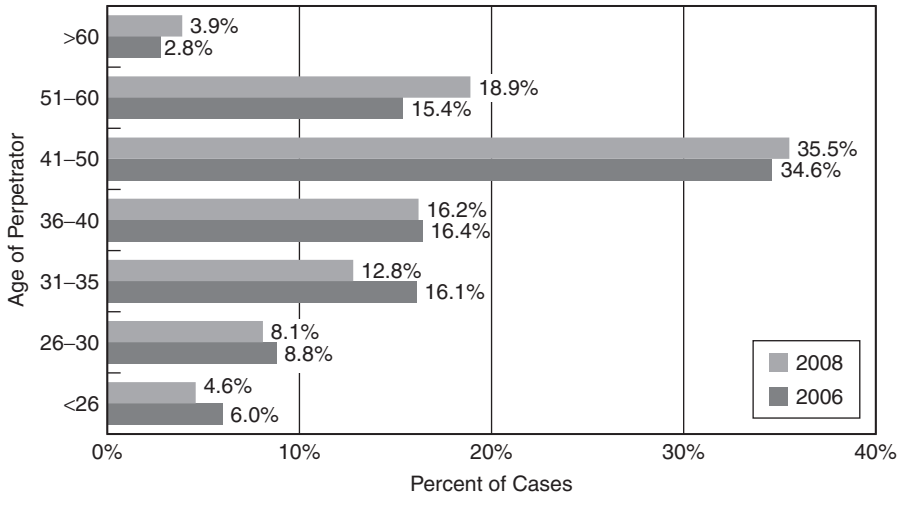


Gender of Perpetrator vs. Percent of Cases



Gender of Perpetrator vs. Median Loss

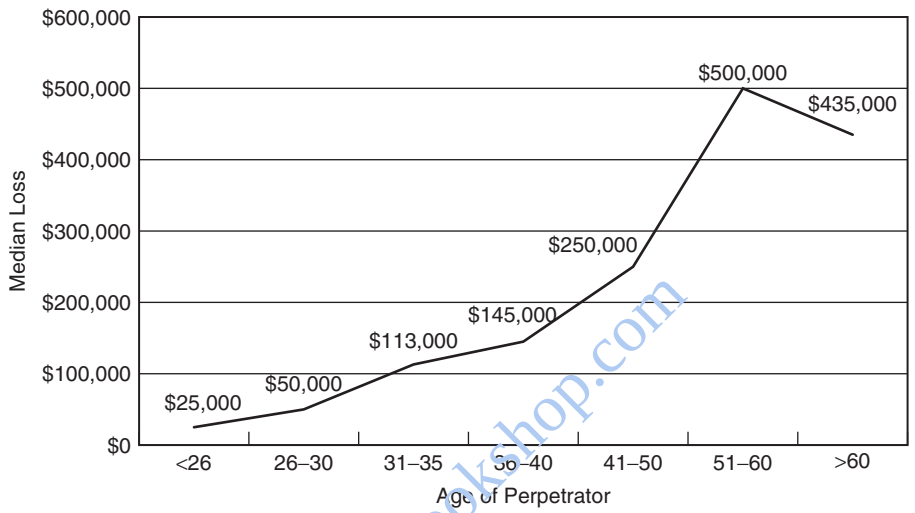
The Effect of Age on Median Loss The frauds in the study were committed by persons ranging in age from eighteen to eighty. There was a strong correlation between the age of the perpetrator and the



Age of Perpetrator vs. Percent of Cases

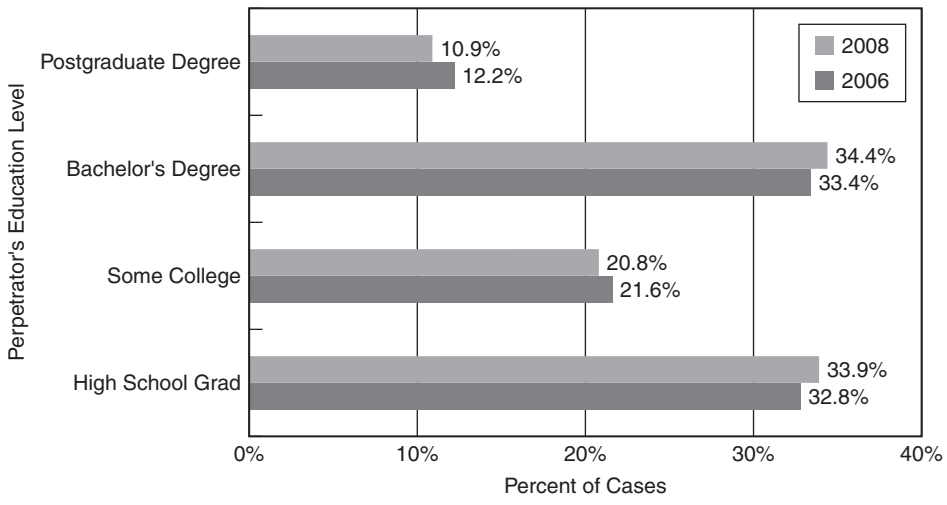
size of the median loss, which was consistent with findings from previous reports. Although there were very few cases committed by employees over the age of sixty (3.9 percent), the median loss in those schemes was $435,000. By comparison, the median loss in frauds committed by those twenty-five or younger was $25,000. As with income and gender, age is likely a secondary factor in predicting the loss associated with an occupational fraud, generally reflecting the perpetrator's position and tenure within an organization.

Although frauds committed by those in the highest age groups were the most costly on average, almost two-thirds of the frauds reported were committed by employees in the thirty-one to fifty age group. The median age among perpetrators was forty-five.

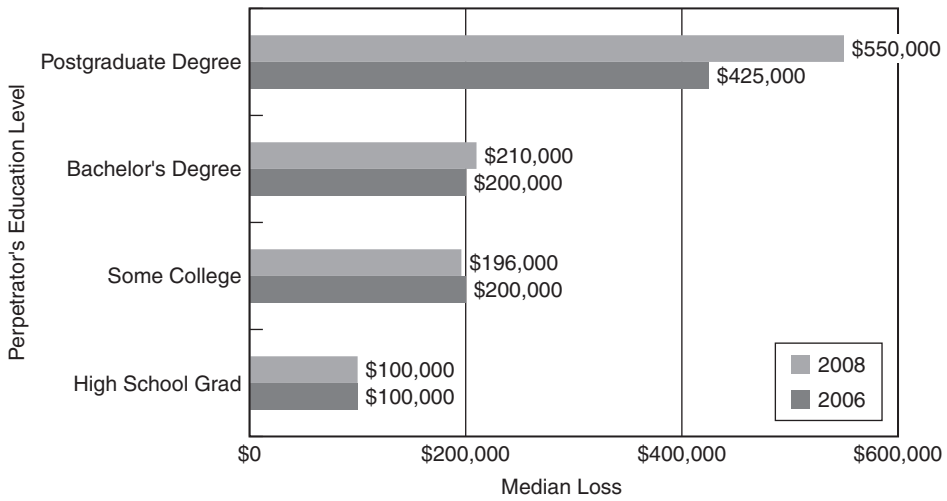


Median Loss vs. Age of Perpetrator

The Effect of Education on Median Loss As employees' education levels rose, so did the losses from their frauds. The median loss in schemes committed by those with only a high school education was $100,000, whereas the median loss caused by employees with a postgraduate education was $550,000. This trend was to be expected, given that those with higher education levels tend to occupy positions with higher levels of authority.

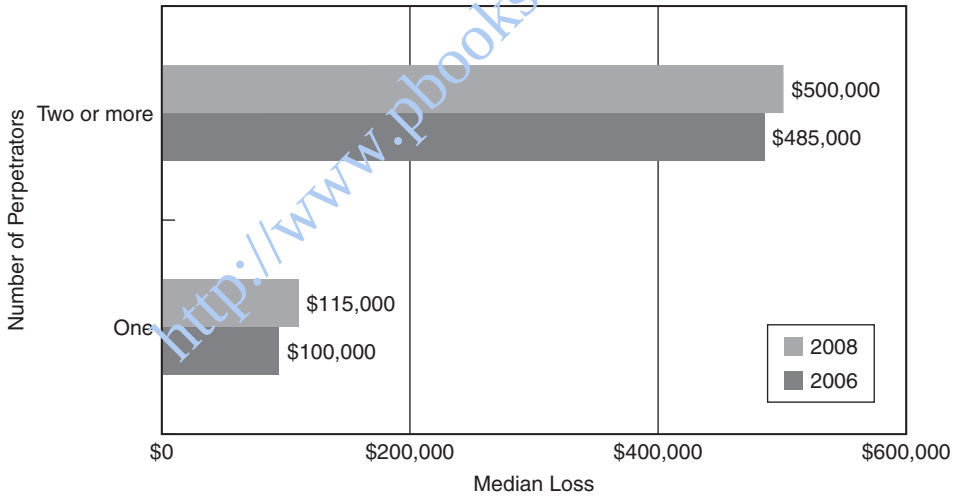


Perpetrator's Education Level vs. Percent of Cases



Perpetrator's Education Level vs. Median Loss

The Effect of Collusion on Median Loss It was not surprising to see that in cases involving more than one perpetrator fraud losses rose substantially. The majority of 2008 survey cases (63.9 percent) only involved a single perpetrator, but, when two or more persons conspired, the median loss was more than four times higher. In the 2006 study, cases involving multiple perpetrators had a median loss that was almost five times higher than single-perpetrator frauds.

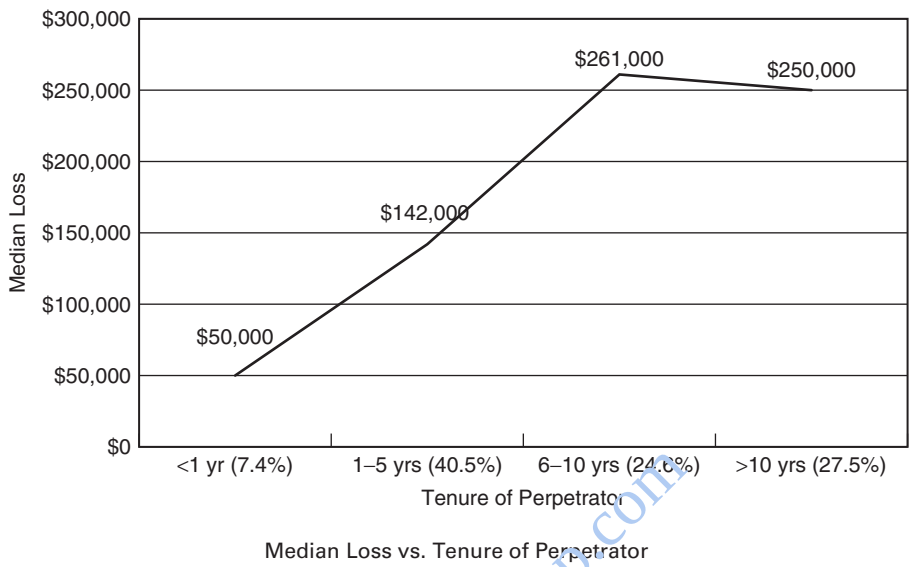


Number of Perpetrators vs. Median Loss

Perpetrators' Tenure with the Victim Organization There was a direct correlation between the length of time an employee had been employed by a victim organization and the size of the loss in the case. Employees who had been with the victim for more than ten years caused median losses of $250,000, whereas employees who had been with their employers for less than one year caused median losses of $50,000. To some extent, these data may also be linked to the position data shown earlier. The longer that an employee works for an organization, the more likely it is that the employee will advance to increasing levels of authority. However, we believe the critical factors most directly influenced by tenure are trust and opportunity.

It is axiomatic that the more trust an organization places in an employee, in the forms of autonomy and authority, the greater that employee's opportunity to commit fraud becomes. Employees with long tenure, by and large, tend to engender more trust from their employers. They also become more familiar with the organization's operations and controls—including gaps in those controls—which can provide a

greater understanding of how to misappropriate funds without getting caught. This is not to imply that all long-term trusted employees commit fraud; however, in general, those employees are better equipped to commit fraud than their counterparts with less experience. When long-term employees decide to commit fraud, they tend to be more successful.



Median Loss vs. Tenure of Perpetrator

Criminal History of the Perpetrators (Figure 1-3) Less than 7 percent of the perpetrators identified in the 2008 study were known to have been convicted of a previous fraud-related offense. Another 5.7 percent of the perpetrators had previously been charged but never convicted. These figures are consistent with other studies showing that most people who commit occupational fraud are first-time offenders. It is also consistent with Cressey's model, in which occupational offenders do not perceive themselves as lawbreakers.

The Victims The victims of occupational fraud are organizations that are defrauded by those they employ. The ACFE's 2008 survey asked respondents to provide information on, among other things, the size of organizations that were victimized, as well as the antifraud measures those organizations had in place at the time of the frauds.

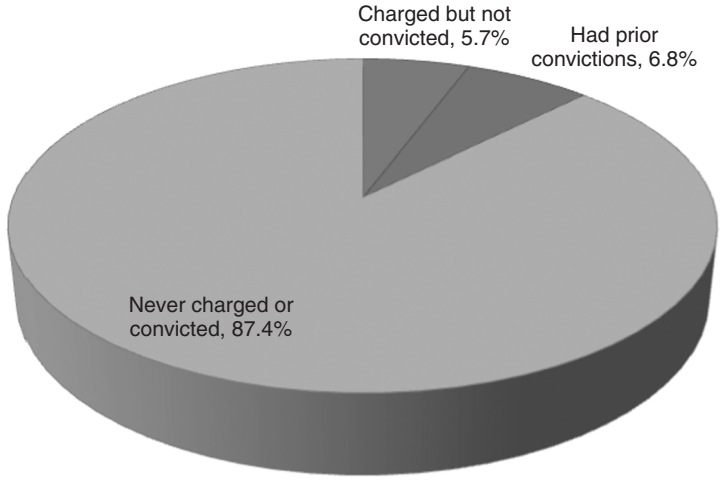
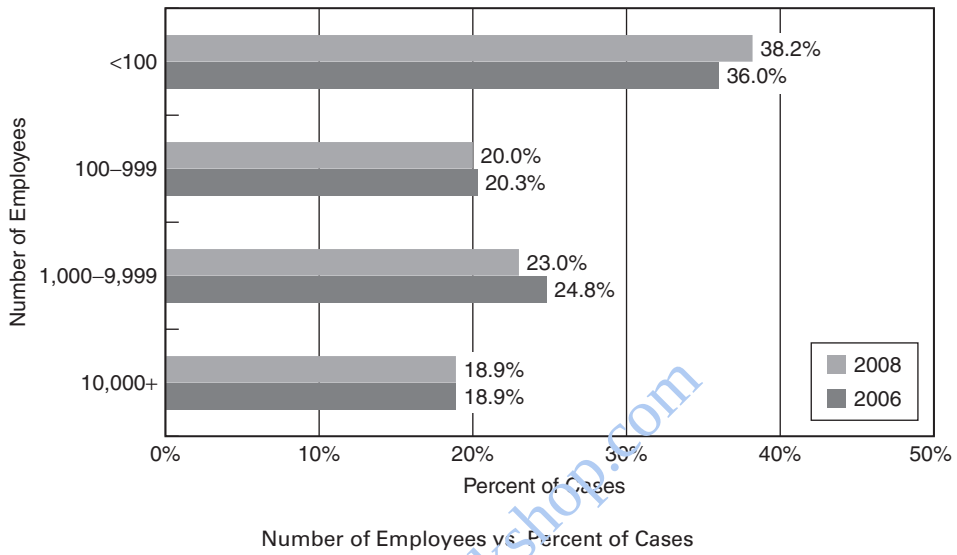
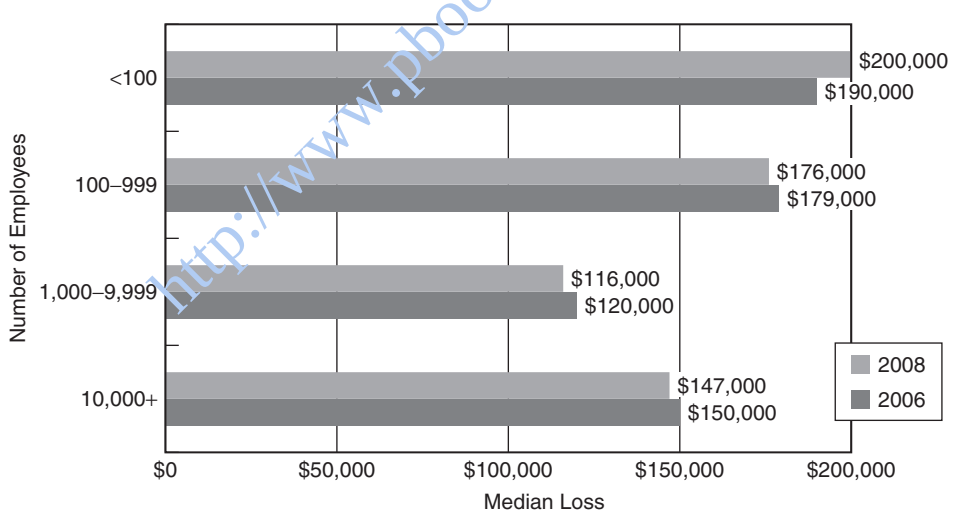


FIGURE 1-3 Perpetrator's Criminal History

Median Loss Based on Size of the Organization Small businesses (those with fewer than 100 employees) can face challenges in deterring and detecting fraud that differ significantly from those of larger organizations. The data show that these small organizations tend to suffer disproportionately large fraud losses, which is similar to the findings in the 2002, 2004, and 2006 reports. The median loss for fraud cases attacking small organizations in our study was $200,000; this exceeded the median loss for cases in any other group. Small organizations were also the most heavily represented group, making up 38.2 percent of all frauds in the study.



Number of Employees vs. Percent of Cases



Number of Employees vs. Median Loss

The data for median loss per number of employees confirm what was always suspected. Accountants logically conclude that small organizations are particularly vulnerable to occupational fraud and abuse. The results from the National Fraud Surveys bear this out: losses in the smallest companies were comparable to or larger than those in the organizations with the most employees. It is suspected that this phenomenon exists for two reasons. First, smaller businesses have fewer divisions of responsibility, meaning that fewer people must perform more functions. One of the most common types of fraud encountered in these studies involved small business operations that had a one-person accounting department—that employee writes checks, reconciles the accounts, and posts the books. An entry-level accounting student could spot the internal control deficiencies in that scenario, but apparently many small business owners cannot or do not.

Which brings up the second reason losses are so high in small organizations: There is a greater degree of trust inherent in a situation where everyone knows each other by name. None of us like to think our

TABLE 1-3 Median Loss Based on Presence of Anti-Fraud Controls

Control	Percent of Cases Implemented	Yes	No	Percent Reduction
Surprise audits	25.5%	$70,000	$207,000	66.2%
Job rotation/mandatory vacation	12.3%	$64,000	$164,000	61.0%
Hotline	43.5%	$100,000	$250,000	60.0%
Employee support programs	52.9%	$110,000	$250,000	56.0%
Fraud training for managers/execs	41.3%	$100,000	$227,000	55.9%
Internal audit/fraud examination dept	55.8%	$118,000	$250,000	52.8%
Fraud training for employees	38.6%	$100,000	$208,000	51.9%
Anti-fraud policy	36.2%	$100,000	$197,000	49.2%
External audit of ICOFR	53.6%	$121,000	$232,000	47.8%
Code of conduct	61.5%	$126,000	$232,000	45.7%
Mgmt review of internal controls	41.4%	$110,000	$200,000	45.0%
External audit of financial statements	69.6%	$150,000	$250,000	40.0%
Independent audit committee	49.9%	$137,000	$200,000	31.5%
Mgmt certification of financial statements	51.6%	$141,000	$200,000	29.5%
Rewards for whistleblowers	5.4%	$107,000	$150,000	28.7%

co-workers would, or do, commit these offenses. Our defenses are naturally relaxed because we generally trust those we know. There again is the dichotomy of fraud: it cannot occur without trust, but neither can commerce. Trust is an essential ingredient at all levels of business—we can and do make handshake deals every day. Transactions in capitalism simply cannot occur without trust. The key is seeking the right balance between too much and too little trust.

The Impact of Anti-Fraud Measures on Median Loss (Table 1-3) CFEs who participated in the ACFE's National Fraud Surveys were asked to identify which, if any, of several common anti-fraud measures were utilized by the victim organizations at the time the reported frauds occurred. The median loss was determined for schemes depending on whether each anti-fraud measure was in place or not (excluding other factors).

The most common anti-fraud measure was the external audit of financial statements, utilized by approximately 70 percent of the victims, followed by a formal code of conduct, which was implemented by 61.5 percent of victim organizations. Organizations that implemented these controls noted median losses that were 40 percent and 45.7 percent lower, respectively, than those of organizations lacking these controls. Interestingly, the two controls associated with the largest reduction in median losses—surprise audits and job rotation/mandatory vacation policies—were among the least commonly implemented anti-fraud controls.

Case Results A common complaint among those who investigate fraud is that organizations and law enforcement do not do enough to punish fraud and other white-collar offenses. This contributes to high fraud levels—or so the argument goes—because potential offenders are not deterred by the weak or often nonexistent sanctions that are imposed on other fraudsters. Leaving aside the debate as to what factors are effective in deterring fraud, the survey sought to measure how organizations responded to the employees who had defrauded them. One of the criteria for cases in the study was that the CFE had to be reasonably certain that the perpetrator in the case had been identified.

Criminal Prosecutions and Their Outcomes (Figure 1-4) In 69 percent of the cases, the victim organization referred the case to law enforcement authorities. The median loss in those cases was $250,000, whereas the median loss was only $100,000 in cases that were not referred.

For cases that were referred to law enforcement authorities, a large number of those cases were still pending at the time of the survey. However, of the 578 responses for which the outcome was known, 15 percent of the perpetrators were convicted at trial, and another 71.3 percent pled guilty or no contest to their crimes. None of the perpetrators in the cases reported in the 2008 Report were acquitted.

No Legal Action Taken One goal of the ACFE study was to try to determine why organizations decline to take legal action against occupational fraudsters. In cases where no legal action was taken, we

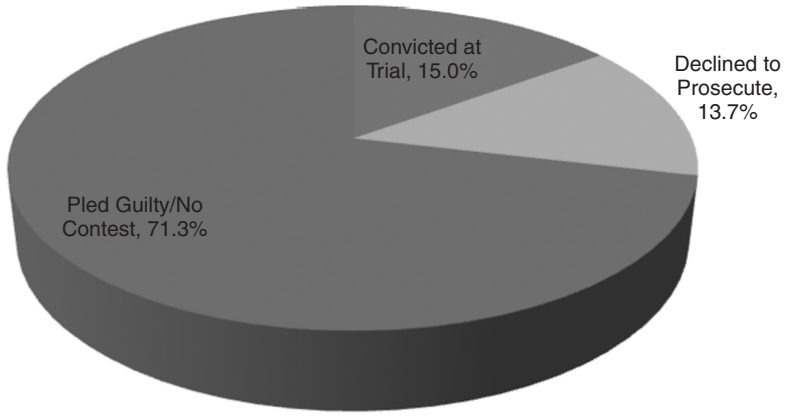
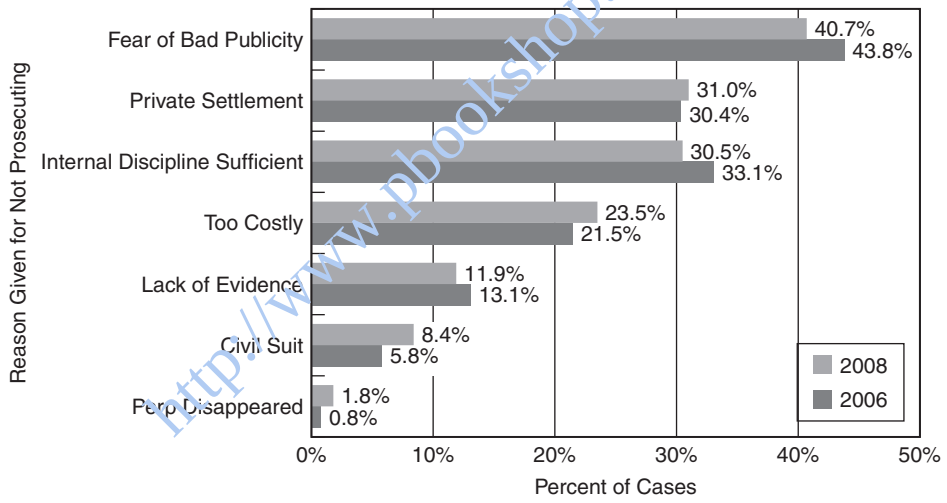


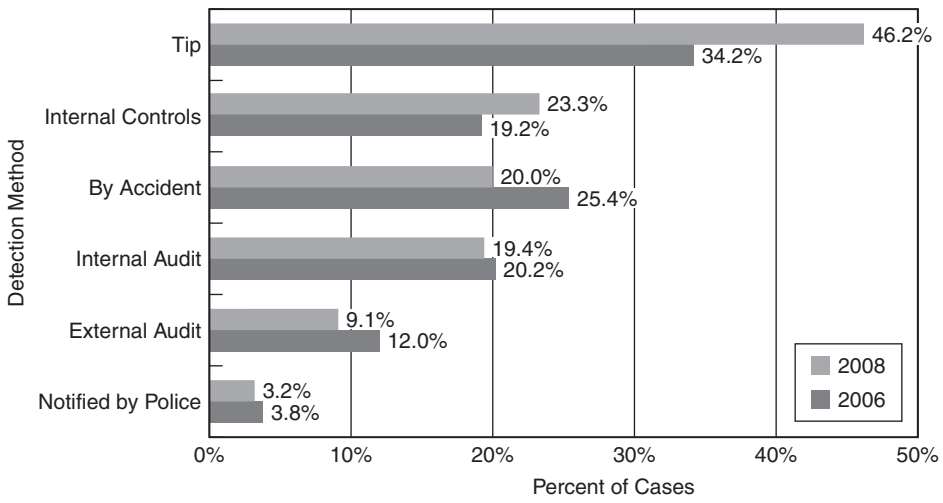
FIGURE 1-4 Criminal Prosecutions and Outcomes

provided respondents with a list of commonly cited explanations and asked them to mark any that applied to their case. The following chart summarizes the results. Fear of bad publicity (40.7 percent) was the most commonly cited explanation, followed by a private settlement being reached (31 percent) and the organization considering its internal discipline to be sufficient (30.5 percent).



Reasons for Not Prosecuting vs. Percent of Cases

Detecting and Preventing Occupational Fraud The obvious question in a study of occupational fraud is this: What can be done about it? Given that the study was based on actual fraud cases that had been investigated, it would be instructional to ask how these frauds were initially detected by the victim organizations. Perhaps by studying how the victim organizations had uncovered fraud, guidance could be provided to other organizations on how to tailor their fraud prevention and detection efforts. Respondents were given a list of common detection methods and were asked how the frauds they investigated were initially detected. As these results show, the frauds were most commonly detected by tips (46.2 percent). It was also interesting—and a bit disappointing—to note that by accident (20 percent) was the third most common detection method, ranking higher than internal or external audits. This certainly seems to support the contention that organizations need to do a better job of proactively designing controls to prevent fraud and audits to detect them. The most glaring reality in all the statistics in this study is that prevention is the most effective measure to reduce losses from fraud.



Detection Method vs. Percent of Cases

NON-FRAUD FORENSIC AND LITIGATION ADVISORY ENGAGEMENTS

The forensic accountant can be expected to participate in any legal action that involves money, following the money, performance measurement, valuation of assets, and any other aspect related to a litigant's finances. In some cases, the finances of the plaintiff are at issue; in some cases, the finances of the defendant are at issue; and in some disputes, the finances of both are under scrutiny, and the forensic accountants may be asked to analyze, compare, and contrast both the plaintiff's and defendant's finances and financial condition.

Some of the typical forensic and litigation advisory services are summarized as follows:

Damage claims made by plaintiffs and in countersuits by defendants
Workplace issues, such as lost wages, disability, and wrongful death
Assets and business valuations
Costs and lost profits associated with construction delays
Costs and lost profits resulting from business interruptions
Insurance claims
Divorce and matrimonial issues
Fraud
Anti-trust actions
Intellectual property infringement and other disputes
Environmental issues
Tax disputes

The issues addressed by a forensic accountant during litigation may or may not be central to the allegations made by the plaintiff's or defense attorneys, but they may serve to provide a greater understanding of the motivations of the parties, other than those motivation claims made publicly, in court filings and in case pleadings.

THE INVESTIGATION

The Mindset: Critical Thinking and Professional Skepticism

As previously noted, we observe that individuals who commit fraud look exactly like us, the average Joe or Jane. If typical fraudsters have no distinguishing outward characteristics to identify them as such, how are we to approach an engagement to detect fraud?

It can be challenging to conduct a fraud investigation unless the investigator is prepared to look beyond his or her value system. In short, you need to think like a fraudster to catch one.

SAS No. 1 states that due professional care requires the auditor to exercise professional skepticism. Because of the characteristics of fraud, the auditor should conduct the engagement "with a mindset that recognizes the possibility that a material misstatement due to fraud could be present." It also requires an "ongoing questioning" of whether information the auditor obtains could suggest a material misstatement as a result of fraud.

Professional skepticism can be broken into three attributes:

1. Recognition that fraud may be present. In the forensic accounting arena, it is recognition that the plaintiff and/or the defendant may be masking the true underlying story that requires a thorough analysis of the evidence.
2. An attitude that includes a questioning mind and a critical assessment of the evidence.
3. A commitment to persuasive evidence. This commitment requires the fraud examiner or forensic accountant to go the extra mile to tie up all loose ends.

At a minimum, professional skepticism is a neutral but disciplined approach to detection and investigation. SAS No. 1 suggests that an auditor neither assumes that management is dishonest nor assumes unquestioned honesty. In practice, professional skepticism, particularly recognition, requires that the fraud examiner or forensic accountant "pull on a thread."

Loose threads: When you pull on a loose thread, a knitted blanket may unravel, a shirt may pucker and be ruined, or a sweater may end up with a hole. Red flags are like loose thread: pull and see what happens; you just might unravel a fraud, ruin a fraudster's *modus operandi*, or blow a hole in a fraud scheme. Red flags are like loose thread: left alone, no one may notice, and a fraudster or untruthful litigant can operate unimpeded. A diligent fraud professional or forensic accountant who pulls on a thread may save a company millions.

Fraud Risk Factors and "Red Flags"

What do these loose threads look like in practice? Fraud professionals and forensic accountants refer to loose thread as anomalies, relatively small indicators, facts, figures, relationships, patterns, breaks in patterns, suggesting that something may not be right or that the arguments being made by litigants may not be the full story. These anomalies are often referred to as red flags.

> *Red flags are defined as a warning signal or something that demands attention or provokes an irritated reaction. Although the origins of the term* red flag *are a matter of dispute, it is believed that, in the 1300s, Norman ships would fly red streamers to indicate that they would "take no quarter" in battle. This meaning continued into the seventeenth century, by which time the flag had been adopted by pirates, who would hoist the "Jolly Roger" to intimidate their foes. If the victims chose to fight rather than submit to boarding, the pirates would raise the red flag to indicate that, once the ship had been captured, no man would be spared. Later it came to symbolize a less bloodthirsty message and merely indicated readiness for battle. From the seventeenth century, the red flag became known as the "flag of defiance." It was raised in cities and castles under siege to indicate that there would be "no surrender."*[17]

Fraud professionals and forensic accountants use the term *red flag* synonymously with *symptoms* and *badges* of fraud. Symptoms of fraud may be divided into at least six categories: unexplained accounting anomalies, exploited internal control weaknesses, identified analytical anomalies where nonfinancial data do not correlate with financial data, observed extravagant lifestyles, observed unusual behaviors, and anomalies communicated via tips and complaints.

Although red flags have been traditionally associated with fraudulent situations, forensic accountants are also on the lookout for evidence that is inconsistent with their client's version of what happened. As independent experts, forensic accountants need to look for evidence that runs counters to their client's claims. Opposing council is always looking for weaknesses in your client's case, so whether the professional is investigating fraud or other litigation issues, it is critical that the forensic accountant maintain a sense of professional skepticism, look for red flags, and pull on loose threads.

Fraud risk factors generally fall into three categories:

Motivational: Is management focused on short-term results or personal gain?

Situational: Is there ample opportunity for fraud?

Behavioral: Is there a company culture for a high tolerance of risk?

Evidence-Based Decision Making

Evidence and other legal issues are explored in depth in a later chapter. For now, we'll use the information in *Black's Law Dictionary*, which defines evidence as anything perceivable by the five senses and any proof—such as testimony of witnesses, records, documents, facts, data, or tangible objects—legally presented at trial to prove a contention and induce a belief in the minds of a jury.[18] Following the issues of critical thinking and professional skepticism is that of a commitment to evidence-based decision making. One of the best ways to ruin an investigation, fail to gain a conviction, or lose a civil case is to base investigative conclusions on logic and conjecture. Many people have tried to convict an alleged perpetrator using the "bad person" theory. The investigator concludes that the defendant is a "bad guy" or that he or she will not come off well during trial and thus must be the perpetrator or have done something wrong. Unfortunately, this approach fails to win the hearts and minds of prosecutors, plaintiff and defense lawyers, and juries, and it can result in significant embarrassment for the fraud professional or forensic accountant.

What do we mean by evidence-based decision making? Critical thinking requires the investigator to "connect the dots," taking disparate pieces of financial and nonfinancial data to tell the complete story of who, what, when, where, how, and why (if "why" can be grounded in evidence). Dots can be business and personal addresses from the Secretary of State's office, phone numbers showing up in multiple places, patterns of data, and breaks in patterns of data. These dots helps prosecutors, defense lawyers, and juries understand the full scheme under investigation. However, in order to be convincing, fraud professionals or forensic accountants must ensure that the dots are grounded in evidence that is consistent with the investigators' interpretation of that evidence. The bottom line is this: successful investigators base their conclusions and the results of their investigations on evidence.

The Problem of Intent: Investigations Centered on the Elements of Fraud

Although the fraud triangle provides an effective explanation for the conditions necessary for fraud to occur and is a source of red flags that require investigation, in order to prove fraud, the investigator has to deal with the problem of intent. Intent, like all aspects of the investigation, must be grounded in the evidence. In a fraud case, the challenge is that—short of a confession by a co-conspirator or the perpetrator—evidence of intent tends to be circumstantial. Although less famous than the fraud triangle, the elements of fraud (Figure 1-5) are critical to the investigative process, whether the engagement includes fraud or litigation issues. The elements of fraud include the act (e.g., fraud act, tort, breach of contract), the concealment (hiding the act or masking it to look like something different), and the conversion (the benefit to the perpetrator).

Provided that the investigator has evidence that the alleged perpetrator committed the act, benefited from that act, and concealed his or her activities, it becomes more difficult for accused or litigants to argue that they did not intend to cause harm or injury. Evidence of concealment, in particular, provides some of the best evidence that the act, fraud or otherwise, was intentional. In civil litigation, especially damage claims based on torts and breaches of contract, the elements of fraud remain important: for example, what evidence suggests that a tort occurred (act), how the tortuous actors benefited (convert) from their action, and how the tortuous actors concealed their tortuous activities.[19]

Evidence of the act may include that gathered by surveillance, invigilation, documentation, posting to bank accounting, missing deposits, and other physical evidence. Proof of concealment can be obtained from audits, through document examination, and from computer searches. Further, conversion can be documented using public records searches, the tracing of cash to a perpetrator's bank account, and indirectly using

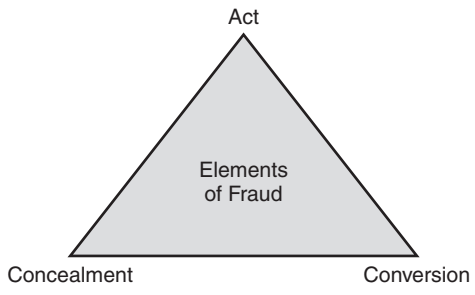


FIGURE 1-5 Elements of Fraud

financial profiling techniques. Finally, interviewing and interrogation are important methods that can be used to supplement other forms of evidence in all three areas: the act, the concealment, and the conversion. There is an ongoing debate in the profession about whether tracing money to a perpetrator's bank account is good enough evidence of conversion or whether the investigator needs to show how the ill-begotten money was used. Although tracing the money into the hands of the perpetrator or his or her bank account is sufficient, showing how the money was used provides a more powerful case and can provide evidence of attributes of the fraud triangle, such as pressure and rationalization, and other motivations included in M.I.C.E. Generally, investigators should take the investigation as far as the evidence leads.

Examples of circumstantial evidence that may indicate the act, concealment, or conversion include the timing of key transactions or activities, altered documents, concealed documents, destroyed evidence, missing documents, false statements, patterns of suspicious activity, and breaks in patterns of expected activity.

The Analysis of Competing Hypotheses (The Hypothesis-Evidence Matrix)

In most occupational fraud cases, it is unlikely that there will be direct evidence of the crime. There are rarely eyewitnesses to a fraud, and, at least at the outset of the investigation, it is unlikely that the perpetrator will come right out and confess. Therefore, a successful fraud examination takes various sources of incomplete circumstantial evidence and assembles them into a solid, coherent structure that either proves or disproves the existence of the fraud. Civil litigation, by its very nature, suggests that there are at least two competing stories, that of the plaintiff and that of the defendant. Thus, in civil litigation, as a starting point, the forensic accountant normally has at least two competing hypotheses. It is inherent in the professional to use the evidence to test each of these hypotheses, as well as others that may arise based on reasonable, objective interpretation of the evidence.

To conclude an investigation without complete evidence is a fact of life for the fraud examiner and forensic accountant. No matter how much evidence is gathered, the fraud and forensic professional would always prefer more. In response, the fraud examiner or forensic accountant must make certain assumptions. This is not unlike the scientist who postulates a theory based on observation and then tests it. When investigating complex frauds, the fraud theory approach is indispensable. Fraud theory begins with an assumption, based on the known facts, of what might have occurred. Then that assumption is tested to determine whether it is provable. The fraud theory approach involves the following steps, in the order of their occurrence:

Analyze available data.

Create hypotheses.

Test the hypotheses.

Refine and amend the hypothesis.

Draw conclusions.

The Hypothesis-Evidence Matrix The analysis of competing hypotheses is captured in a tool called the hypotheses-evidence matrix. This tool provides a means of testing alternative hypotheses in an organized, summary fashion. Consider the following question drawn from the "intelligence community" between the first Gulf War, Desert Storm, and the second Gulf War, Iraqi Freedom: Given Iraq's refusal to meet its United Nations commitments, if the United States bombs Iraqi Intelligence Headquarters, will Iraq retaliate?[20] To answer the question, three hypotheses were developed:

H1 Iraq will not retaliate.

H2 Iraq will sponsor some minor terrorist action.

H3 Iraq will plan and execute a major terrorist attack, perhaps against one or more CIA installations.

The evidence can be summarized as follows:

Saddam's public statements of intent not to retaliate.

Absence of terrorist offensive during the 1991 Gulf War.

Assumption: Iraq does not want to provoke another US war.

Increase in frequency/length of monitoring by Iraqi agents of regional radio and TV broadcasts.

Iraqi embassies instructed to take increased security precautions.

Assumption: Failure to retaliate would be an unacceptable loss of face for Saddam.

Each piece of data needs to be evaluated in terms of each hypothesis as follows:

0 = No diagnostic value for the hypothesis
− = Does not support the hypothesis
+ = Supports the hypothesis

If the United States bombs Iraqi Intelligence Headquarters, will Iraq retaliate?

Hypotheses:

H1 Iraq will not retaliate.
H2 Iraq will sponsor some minor terrorist actions.
H3 Iraq will plan and execute a major terrorist attack, perhaps against one or more CIA installations.

0 No diagnostic value for the hypothesis
− Does not support the hypothesis
+ Supports the hypothesis

	H1	H2	H3
Saddam Hussein's public statements of intent not to retaliate.	0	0	0
Absence of terrorist offensive during the 1991 Gulf War.	+	0	−
Assumption: Iraq does not want to provoke another US war.	+	+	−
Increase in frequency/length of monitoring by Iraqi agents of regional radio and TV broadcasts.	0	+	+
Iraqi embassies instructed to take increased security precautions.	−	+	+
Assumption: Failure to retaliate would be an unacceptable loss of face for Saddam Hussein.	−	+	+

Based on the evidence evaluated, the only hypothesis without any (–) assessments is H2, with the resulting conclusion that if the United States were to bomb Iraqi Intelligence HQ, the most likely response is that Saddam and Iraq would take some minor terrorist action.

Notice also the direction of the "proof." We can never prove any hypothesis; in contrast, we can have two findings: (1) we have no evidence that directly refutes the most likely hypothesis, and (2) we have evidence that seems to eliminate the alternative hypotheses. As an example, one of the key elements of the fraud triangle is opportunity. By charting the flow of activity and interviewing personnel, it is not that we know that person A took the money but that we eliminate most employees because they had no opportunity to take the money and conceal their actions.

Consider the following scenario:

You are an auditor for Bailey Books Corporation of St. Augustine, Florida. Bailey Books, 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. On January 28, you receive a telephone call. The caller advises that he does not wish to disclose his identity. However, he claims to be a "long-term" supplier of paper products to Bailey Books. The caller says that since Linda Reed Collins took over as purchasing manager for Bailey Books several years ago, he has been systematically "squeezed out" of doing business with the company. He hinted that he thought Collins was up to something illegal. Although you query the caller for additional information, he hangs up the telephone. What do you do now?

When you received the telephone call from a person purporting to be a vendor, you had no idea whether the information was legitimate. There could be many reasons why a vendor might feel unfairly treated. Perhaps he just lost Bailey's business because another supplier provided inventory at a lower cost. Under the fraud theory approach, you must analyze the available data before developing a preliminary hypothesis as to what may have occurred.

Analyzing the Evidence If an audit of the entire purchasing function was deemed appropriate, it would be conducted at this time and would specifically focus on the possibility of fraud resulting from the anonymous allegation. A fraud examiner would look, for example, at how contracts are awarded and at the distribution of contracts among Bailey Books' suppliers.

Creating the Hypotheses Based on the caller's accusations, you develop several hypotheses to focus your efforts. The hypotheses range from the null hypothesis that "nothing illegal is occurring" to a "worst-case" scenario—that is, with the limited information you possess, what is the worst possible outcome? In this case, for Bailey Books, it would probably be that its purchasing manager was accepting kickbacks to steer business to a particular vendor. A hypothesis can be created for any specific allegation—i.e., a bribery or kickback scheme, embezzlement, conflict of interest, or financial statement fraud—in which evidence indicates that the hypothesis is a reasonable possibility.

Testing the Hypotheses Once the hypotheses have been developed, each must be tested. This involves developing a "what if" scenario and gathering evidence to support or disprove the proposition. For example, if a purchasing manager such as Linda Reed Collins were being bribed, a fraud examiner likely would find some or all of the following facts:

- A personal relationship between Collins and a vendor
- Ability of Collins to steer business toward a favored vendor
- Higher prices and/or lower quality for the product or service being purchased
- Excessive personal spending by Collins

In the hypothetical case of Linda Reed Collins, you—using Bailey Books' own records—can readily establish whether or not one vendor is receiving a larger proportional share of the business than similar vendors. You could ascertain whether or not Bailey Books was paying too much for a particular product, such as paper, by simply calling other vendors and determining competitive pricing. Purchasing managers don't usually accept offers of kickbacks from total strangers; a personal relationship between a suspected vendor and the buyer could be confirmed by discreet observation or inquiry. Whether or not Collins has the ability to steer business toward a favored vendor could be determined by reviewing the company's internal controls to ascertain who is involved in the decision-making process. The proceeds of illegal income are not normally hoarded; the money is typically spent. Collins's lifestyle and spending habits could be determined through examination of public documents, such as real estate records and automobile liens.

Refining and Amending the Hypotheses In testing the hypotheses, a fraud examiner or forensic accountant might find that all facts do not fit a particular scenario. If such is the case, the hypothesis should be revised and retested. In some cases, hypotheses are discarded entirely. In such cases, the professional should maintain an evidence trail for the discarded hypothesis that demonstrates what evidence was used to suggest that the hypothesis was not supported. Gradually, as the process is repeated and the hypotheses continue to be revised, you work toward what is the most likely and supportable conclusion. The goal is not to "pin" the crime on a particular individual, but rather to determine, through the methodical process of testing and revision, whether a crime has been committed and, if so, how.

Methodologies Used in Fraud and Financial Forensic Engagements

Essentially three tools are available, regardless of the nature of the fraud examination or financial forensic engagement. First, the fraud examiner or financial forensic professional must be skilled in the examination of financial statements, books and records, and supporting documents. In many cases, these provide the indicia of fraud and/or the motivations of the parties under review. Related to such evidence, the fraud examiner must also know the legal ramifications of evidence and how to maintain the chain of custody over documents. For example, if it is determined that Linda Reed Collins was taking payoffs from a supplier, checks and other financial records to prove the case must be lawfully obtained and analyzed, and legally supportable conclusions must be drawn.

The second tool used by fraud examiners or financial forensic professionals is the interview, which is the process of obtaining relevant information about the matter from those with knowledge of it. For example, in developing information about Linda Reed Collins, it might be necessary to interview her co-workers, superiors, and subordinates. In civil litigation, most interview testimony is obtained by counsel during depositions. Despite the fact that financial forensic professionals do not ask the questions, it is common for them to prepare questions for attorneys to ask, attend depositions of key financial personnel and those knowledgeable about the entity's finances, and provide the attorney with feedback and additional questions during the deposition of fact witnesses, who have financial knowledge related to the matters at hand.

FIGURE 1-6 Evidence-Gathering Order in Fraud Examinations

In a fraud examination, evidence is usually gathered in a manner that moves from the general to the specific. That rule applies both to gathering documentary evidence (Figure 1-6) and to taking witness statements (Figure 1-7). Therefore, a fraud examiner most likely starts by interviewing neutral third-party witnesses, persons who may have some knowledge about the fraud but who are not involved in the offense. For example, the fraud examiner may start with a former employee of the company. Next, the fraud examiner interviews corroborative witnesses, those people who are not directly involved in the offense but who may be able to corroborate specific facts related to the offense.

If, after interviewing neutral third-party witnesses and corroborative witnesses, it appears that further investigation is warranted, the fraud examiner proceeds by interviewing suspected co-conspirators in the alleged offense. These people are generally interviewed in order, starting with those thought to be least culpable and proceeding to those thought to be most culpable. Only after suspected co-conspirators have been interviewed is the person suspected of committing the fraud confronted. By arranging interviews in order of probable culpability, the fraud examiner is in a position to have as much information as possible by the time the prime suspect is interviewed. The methodology for conducting interviews is discussed later in the text.

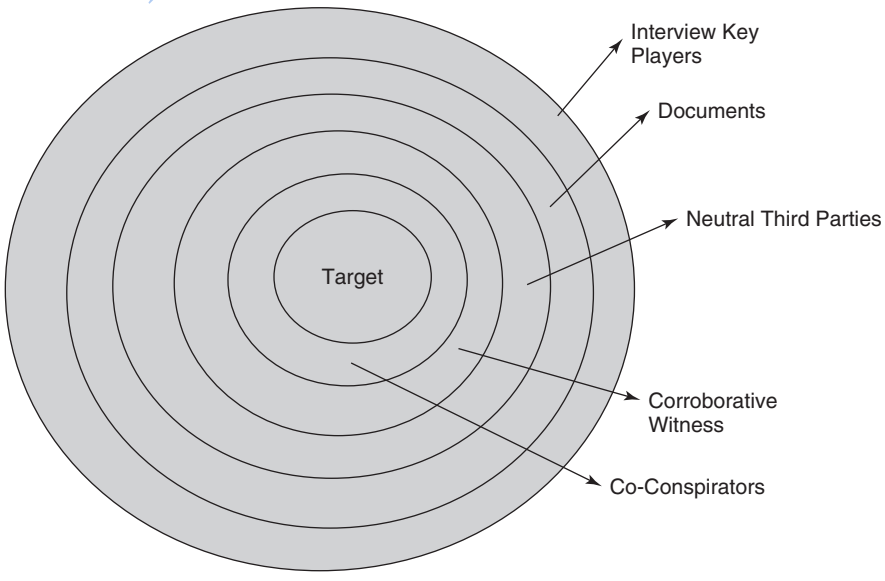


FIGURE 1-7 Fraud Interview Methodologies

Evidence-Gathering Order in Fraudulent Financial Statements and Tax Returns Interestingly, with fraudulent representations, such as materially misstated financial statements and improper tax returns, the investigator starts with the suspected perpetrator. The logic of this is simple: assuming that the person knowingly created false financial statements or tax returns, the act of falsifying is part of the concealment of the act. As such, inherently, the perpetrator has made one of the following assumptions: the auditor or investigator won't find the issue, or, if you identify red flags related to the issue, the auditor or investigator won't be smart enough to unravel the underlying evidence to determine what really happened. Essentially, the alleged perpetrator is betting his or her intellect against that of the auditor or investigator. Thus, by interviewing the suspected perpetrator at the inception of the audit, examination, or investigation, you are documenting his or her claim(s) that the financial statements are not materially misstated or that the tax return properly reflects all items of taxable income. Thus, if auditors find fraudulent financial reporting, they have caught the perpetrators in a lie and have developed further evidence of concealment.

The third tool that must be used in fraud examinations or financial forensic engagements is observation. Fraud examiners or financial forensic professionals are often placed in a position where they must observe behavior, search for displays of wealth, and, in some instances, observe specific offenses. For example, a fraud examiner might recommend a video surveillance if it is discovered that Linda Reed Collins has a meeting scheduled with a person suspected of making payoffs. In forensic litigation, the defendant might argue that the plaintiff had been reassigning his or her employees to another business venture and that action is what caused profits to fall and the business to fail. In that scenario, surveillance of operations and comparison of observation to the payroll records determine whether employees had been inappropriately reassigned. The methodology previously described can be applied to virtually any type of fraud investigation or forensic engagement.

The Importance of Nonfinancial Data

The power of using nonfinancial data to corroborate financial information cannot be overstated. How are nonfinancial data defined? They are data from any source outside of the financial reporting system that can be used to generate an alternative view of the business operation. Consider the following example, in which a husband in a divorce setting argues for a low settlement for his ex-wife:

> A large restaurant sold Southern food and beer, with beer sales being a prominent part of the restaurant. The owner reported only $50,000 of annual income from the business, yet he and his wife drove expensive cars, their children attended private schools, and the husband was buying significant amounts of real estate. Records of the local beer distributors were subpoenaed. Those records detailed exactly how much beer and the types of beer (kegs, bottles, cans, etc.) that were sold to the restaurant during the prior two years. A forensic accountant went to the restaurant and took note of all the beer prices by type. The amount of beer purchased was used to estimate sales by pricing out all of the purchases at retail. Reported sales were found to be approximately $500,000 lower than the calculated amount.[21]

In this case, the nonfinancial data were units of beer purchased and obtained from beer distributors, a source outside the normal accounting reporting function. As examples, similar approaches can be used related to laundromat electricity usage, laundromat wash and dry cycle times, natural gas produced from gas wells, tons of coal mined from underground. Nonfinancial data need not come from sources outside the company; they can be generated from operations and used by management. There has even been a patented data mining technique called NORA (nonobvious relationship analysis) created using nonfinancial data.

Essentially, economists break the world into prices and quantities (p's and q's). Fraud professionals and forensic accountants use this same approach to evaluate expected business relationships. Once critical metrics have been dissected into prices and quantities, each can be evaluated for reasonableness to determine whether the numbers make sense or further investigation is required. Nonfinancial data can then be correlated with numbers represented in the financial accounting system: financial statements and tax returns. Examples of nonfinancial data include employee records and payroll hours, delivery records, shipping records, attorney hours charged, and travel times and destinations. Any data generated outside the normal accounting system can be used to determine the reasonableness of data generated from accounting. Optimally, the nonfinancial data can be reconciled to or at least correlated with the numbers captured in the books and records.

The theory behind the power of nonfinancial data is straightforward. Essentially, managers of operational areas need accurate data to do their jobs. For example, consider managers in a petroleum-refining

business. Petroleum refining is a sophisticated mixture of chemistry and engineering. Without accurate, reliable, and detailed data, managers cannot optimize the refining processes. Although owners and those responsible for the financial data may want to create alternative perceptions of financial performance, they still want the underlying business to maximize profitability. As such, they are not likely to corrupt nonfinancial data. Further, they need to hold operational managers accountable for their performance, and they cannot achieve that goal without accurate nonfinancial data. Finally, even though some executives and financial managers are willing to cook the books, they are not willing to forgo large tax deductions and other benefits from their actions. When nonfinancial data do not reconcile or correlate to financial data, fraud examiners and financial forensic professionals should consider this a red flag. Finally, in most fraud examinations and financial forensic engagements, professionals should seek out nonfinancial data to understand fully the information included in the accounting books and records.

Graphical Tools

As noted in some of the critical thinking analyses, sometimes the only way to figure something out is to use graphical tools—such as who knows who (linkages), who is connected with what business, how the scheme works (flow diagram), who must be involved (links and flows), what the important events are (timelines). During the investigation, these graphical representations, even handwritten ones, can provide important clues and enhance the investigator's understanding of fact and events, interpret evidence, and otherwise draw meaning from seemingly disparate pieces of data. They can also show weaknesses in the case—places where additional evidence is required in order provide a complete evidence trail.

Although completed during the investigation as a work-in-progress tool, the same graphics are often reused during the formal communication process at or near the conclusion of an investigation. Graphical representations can let nonprofessionals and those with less time on the investigation know what happened. Even though catching the bad guy or reconstructing what happened is the primary role of the fraud examiner or financial forensic professional, a successful career requires that the investigators be able to communicate their results in both written and verbal form. The challenge for the typical professional in this field is that they understand and embrace numbers; however, the legal world is one of words. Thus, the successful investigator must move from a world of numbers to the less familiar world of words.

Written format includes meticulously developed work papers and evidence binders, written reports, and written presentation materials. Oral reports include interviewing and interrogation skills, summarizing investigation status and outcomes to attorneys, prosecutors, judges, and juries. Graphical tools, such as link charts, flow charts, commodity and money flow diagrams, timelines, and other graphical representations, are both important investigative tools and excellent communication tools. These tools are examined in more detail in the digital forensic accounting chapter. For now, it is important to note that the investigator needs to ground these graphics in the evidence and needs to maintain backup that indicates where the data came from.

The Importance of the Story Line: Who, What, Where, When, How, and Why

To be successful, the investigator must be able to explain—to prosecutors, attorneys, juries, judges, and other actors in the investigative process—the outcome of the investigation: who, what, when, where, how, and, optimally, why (if the evidence lends itself to explanations of why, such as the perceived pressure, rationalization, and M.I.C.E.). Investigations centered on the elements of fraud (act, concealment, and conversion) that include indications of the fraud triangle, particularly perceived opportunity and M.I.C.E., have the greatest chances of being successful, assuming that these investigative outcomes are grounded in the evidence.

Although fraud examination and financial forensics use evidence-based decision making, critical thinking skills are essential to understanding what the numbers mean. The ability to use nonfinancial information, as well as financial data gathered from the books and records, to tell a compelling story is crucial to success. As fraud examiners or financial forensic professionals move forward in their investigations, they shift from a world grounded in numbers to one where words carry the day. As such, when fraud examiners or forensic accountants reach the point of drawing conclusions, they must be able to tell a complete story that explains who, what, where, when, how, and, possibly, why. Essentially, they need to think like a journalist who is telling a news story.

Teamwork and Leadership

Because thinking like a fraudster is challenging, use of investigative teams can be an effective tool. For example, for larger fraud or financial forensic investigations, one might be part of a team. In those cases, investigators should use other professionals by brainstorming, interpreting the meaning of evidence, helping develop new fraud theories, and working to connect the dots. Even if the fraud examiner or forensic professional is working as the only person "following the money," the broader team might include lawyers, managers, paralegals, and other forensic investigators. All play an integral role as team members and should be consulted regularly.

Being a successful team player requires at least two attributes. First, each team member must be professionally competent at his or her assigned task. In order for your teammates to be able to rely on your work, they must believe that your work will be completed at the highest levels. One of the criteria included in the ACFE code of ethics is that CFEs "at all times, shall 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." Professional competence is one pillar of successful teamwork. The second major attribute of teamwork is character. Your teammates must be able to count on you as a person. The following gives examples of teamwork attributes that are required for successful completion of fraud and forensic investigations.

Competence

- **a.** Contributing high-quality ideas
- **b.** Contributing high-quality written work
- **c.** Demonstrating a professional level of responsibility to the team: "get it done"

Character

- **a.** Attending meetings, prepared and on time with something to contribute
- **b.** Being available to meet with teammates
- **c.** Completing a fair share of the total workload
- **d.** Listening to teammates' ideas and valuing everyone's contributions

At a minimum, being a good team participant means being a trusted team member. That allows each teammate to contribute to the overall success of the team. Interestingly, leadership is also important to successful team operations. Leadership not only refers to the person with the assigned role of leader, but to individual team members. Thus, good teammates also demonstrate leadership when their unique abilities are needed by the team.

FRAUD EXAMINATION METHODOLOGY

Fraud examination is a methodology developed by ACFE for resolving fraud allegations from inception to disposition, including obtaining evidence, interviewing, writing reports, and testifying. Fraud examination methodology requires that all fraud allegations be handled in a uniform legal fashion and that they be resolved in a timely manner. Assuming there is sufficient reason (predication) to conduct a fraud examination, specific steps are employed in a logical progression designed to narrow the focus of the inquiry from the general to the specific, eventually centering on a final conclusion. The fraud examiner begins by developing a hypothesis to explain how the alleged fraud was committed and by whom, and then, at each step of the fraud examination process, as more evidence is obtained, that hypothesis is amended and refined. Fraud examiners, as designated by the ACFE, also assist in fraud prevention, deterrence, detection, investigation, and remediation.[22]

PREDICATION

Predication is the totality of circumstances that lead a reasonable, professionally trained, and prudent individual to believe that a fraud has occurred, is occurring, and/or will occur. All fraud examinations must be based on proper predication; without it, a fraud examination should not be commenced. An anonymous tip or complaint, as in the Linda Reed Collins example cited earlier, is a common method for uncovering fraud and is generally considered sufficient predication. Mere suspicion, without any underlying circumstantial evidence, is not a sufficient basis for conducting a fraud examination.

Fraud Prevention and Deterrence

Given the cost of fraud, prevention and deterrence are typically more cost beneficial than attempting to remediate a fraud that has already occurred. Fraud prevention refers to creating and maintaining environments in which the risk of a particular fraudulent activity is minimal and opportunity is eliminated, given the inherent cost-benefit trade-off. When fraud is prevented, potential victims avoid the costs associated with detection and investigation.[23]

Fraud deterrence refers to creating environments in which people are discouraged from committing fraud, although it is still possible. The 2005 *Federal Sentencing Guideline Manual* defines deterrence as a clear message sent to society that repeated criminal behavior will aggravate the need for punishment with each recurrence. Deterrence is usually accomplished through a variety of efforts associated with internal controls and ethics programs that create a workplace of integrity and encourage employees to report potential wrongdoing. Such actions increase the perceived likelihood that an act of fraud will be detected and reported. Fraud deterrence can also be achieved through the use of continuous monitoring/auditing software tools. Fraud deterrence is enhanced when the perception of detection is present and when potential perpetrators recognize that they will be punished when caught.

Fraud Detection and Investigation

Fraud detection refers to the process of discovering the presence or existence of fraud. Fraud detection can be accomplished through the use of well-designed internal controls, supervision, and monitoring and the active search for evidence of potential fraud. Fraud investigation takes place when indicators of fraud, such as missing cash or other evidence, suggest that a fraudulent act has occurred and requires investigation to determine the extent of the losses and the identity of the perpetrator.[24]

Remediation: Criminal and Civil Litigation and Internal Controls

Remediation is a three-pronged process: (1) the recovery of losses through insurance, the legal system, or other means; (2) support for the legal process as it tries to resolve the matter in the legal environment; and (3) the modification of operational processes, procedures, and internal controls to minimize the chances of a similar fraud recurring.

REVIEW QUESTIONS

1-1 Define fraud and identify a potentially fraudulent situation.

1-2 Differentiate between fraud and abuse.

1-3 Describe the services that a forensic accountant might provide related to a marital dispute.

1-4 Explain the differences between an audit, fraud examination, and forensic accounting engagement.

1-5 Explain the theory of the fraud triangle.

1-6 List the legal elements of fraud.

1-7 Identify common fraud schemes.

1-8 Give examples of nonfraud forensic and litigation advisory engagements.

1-9 Describe the fraud examiner/forensic accountant's approach to investigations.

1-10 Explain fraud examination methodology.

ENDNOTES

1. Bandler, James, and Ann Zimmerman, "A Wal-Mart Legend's Trail of Deceit," *Wall Street Journal*, April 8, 2005.
2. Black, Henry Campbell. *Black's Law Dictionary*, 5th ed St. Paul, MN: West Publishing Co., 1979, p. 792.
3. A tort is a civil injury or wrongdoing. Torts are not crimes; they are causes of action brought by private individuals in civil courts. Instead of seeking to have the perpetrator incarcerated or fined, as would happen in a criminal case, the plaintiff in a tort case generally seeks to have the defendant pay monetary damages to repair the harm that he or she has caused.
4. Black, p. 300.
5. *Black's Law Dictionary*, 6th ed., p. 563.
6. Fowler, Tom, "Skilling Gets 24 Years in Prison for Enron Fraud." Chron.com (October 23, 2006).
7. ACFE, "Cooking the Books: What Every Accountant Should Know," Austin, TX, 1993.

8. National Commission on Fraudulent Financial Reporting, "Report to the National Commission on Fraudulent Financial Reporting," NY, 1987.
9. Except from NIJ Special Report: Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students (December 20, 2005).
10. The AICPA Forensic and Litigation Services Committee developed the definition. See also Crumbley, D. Larry, Lester E. Heitger, and G. Stevenson Smith, *Forensic and Investigative Accounting*, 2005.
11. Adapted from Crumbley, D. Larry, Lester E. Heitger, and G. Stevenson Smith, *Forensic and Investigative Accounting*, 2005. See also: AICPA Business Valuation and Forensic & Litigation Services.
12. Source unknown.
13. Adapted from "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students," a National Institute of Justice project completed at West Virginia University.
14. Adapted from *Occupational Fraud and Abuse*, Joseph T. Wells, Obsidian Publishing Company (1997).
15. According to the ACFE 2008 Report to the Nation, males perpetrate fraud 59.1 percent of the time versus 40.9 percent for females.
16. Some trust violators (fraudsters) are fired with or without paying restitution. Thus, in some cases, the fraud perpetrator is pathological in his or her work, moving from organization to organization. In those cases, some estimates indicate that the fraudster will victimize each new company within twelve to thirty-six months.
17. See http://www.answrs.com/red%20flag.
18. ACFE's Fraud Examiners Manual, Section 2.601.
19. In civil litigation, all the plaintiff has to prove is that the defendant was liable and that the plaintiff suffered damages. Thus, although the elements of fraud are not required, they provide a good framework to investigator allegations in most financial litigation environments.
20. The authors are grateful to West Virginia University Professor Jason Thomas who first shared this example with the forensic accounting and fraud examination students.
21. DiGabriel, James (ed.), *Forensic Accounting in Matrimonial Divorce* (2005), pp. 51–52.
22. Adapted from ACFE *Fraud Examiners Manual*.
23. Albrecht, W. Steve, *Fraud Examination*, 2003.
24. Whether to use the term *fraud investigation* or *fraud examination* is a matter of debate among practitioners. Some, including the ACFE, prefer the term *fraud examination* because it encompasses prevention, deterrence, detection, and remediation elements in addition to investigation. Others prefer *fraud investigation* because the term *examination* has a special meaning for auditors and accountants. The Technical Working Group's position is that either term is acceptable as long as the full term, including the word *fraud* is used: fraud examination or fraud investigation.

CHAPTER 2

CAREERS IN FRAUD EXAMINATION AND FINANCIAL FORENSICS

LEARNING OBJECTIVES

After reading this chapter, you should be able to

2-1 Discuss employment trends in fraud examination and financial forensics and the reasons for these trends.

2-2 Identify employment opportunities for fraud examination and financial forensics specialists and other related professions.

2-3 Define the role of fraud examination and financial forensic skills related to management and those charged with corporate governance responsibilities.

2-4 List professional organizations that support fraud examination and financial forensics professionals and their certifications.

2-5 Discuss international opportunities in fraud examination and financial forensics.

2-6 Describe the role of education in fraud examination and financial forensics.

2-7 Explain the role of research in the fraud examination and financial forensics professions.

CRITICAL THINKING EXERCISE

Why are manhole covers round?[1]

This critical thinking exercise is often supported with visual props such as square and round pieces of plastic containers with lids. Students are encouraged to manipulate the different shaped containers to see if they can determine the answer. This critical thinking activity demonstrates the need to experience your investigative data and evidence using all of your five senses: sight, touch, hearing, taste, and smell. While we don't do much tasting or smelling in forensic accounting, the point is an important one. To be successful, fraud professionals and forensic accountants must immerse themselves in the evidence to answer the essential questions—who, what, where, when, how, and why—of an investigation.

As a result of highly publicized financial scandals and heightened concerns over money laundering associated with terrorism and drug trafficking, the auditor's and accountant's responsibility for detecting fraud within organizations has come to the forefront of the public's awareness. Successful fraud examinations and well-executed forensic investigations may be the difference between whether perpetrators are brought to justice or allowed to remain free. In most cases, success depends upon the knowledge, skills, and abilities of the professionals conducting the work. Consequently, the demand for qualified professionals with education, training, and experience in fraud and financial forensics has increased.

The academic and professional disciplines of fraud examination and financial forensics embraces and creates opportunities in a number of related fields, including accounting, law, psychology, sociology, criminology, intelligence, information systems, computer forensics, and the greater forensic science fields. Each group of these professionals plays an important role in fraud prevention, deterrence, detection, investigation, and remediation.

BACKGROUND

Recent corporate accounting and financial scandals have led to increased legal and regulatory requirements, such as the Sarbanes–Oxley Act of 2002 and the Emergency Economic Stabilization Act of 2008 (EESA). These requirements address internal controls for detecting and deterring fraud, encourage financial statement auditors to be more aggressive in searching for fraud, and have challenged accountants, corporate governance, and other professionals to conduct fraud risk assessments to mitigate its occurrence.

One result has been an increased demand for entry-level and seasoned practitioners. Furthermore, professionals practicing in the traditional areas of tax, audit, management, information systems, government, not-for-profit, external (independent), and internal audit are expected to have a greater understanding of fraud and financial forensics.

The threat of terror activities, public corruption, and organized criminal activities has heightened the need for professionals who are properly trained to investigate and resolve issues and allegations associated with these acts. The emphasis here is on law enforcement and pursuing criminal charges. These engagements are often associated with the Department of Justice, the Department of Homeland Security, the Bureau of Alcohol, Tobacco, Firearms and Explosives, and other federal, state, and local law enforcement agencies. These agencies use legislation, such as the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, to focus on white-collar crime, money laundering, and terrorist financing.

There is also a growing demand for forensic and litigation advisory services related to damages, divorce, valuations, construction delays, antitrust, lost wages, business interruption, intellectual property infringement, insurance claims, environmental issues, tax evasion, wrongful death, reconstruction, and litigation consulting, to name a few.

Another area is the increasing victimization of individuals targeted in fraud schemes (e.g., identity theft). While the most common victims of such fraud are the fraudster's family and friends, international criminal organizations have developed identity theft and similar frauds into "big business." Raising awareness of fraud prevention techniques and assisting in remediation procedures are crucial to effectively addressing this growing problem in our global society.

The demand for students who have specialized qualifications in fraud and financial forensics has grown significantly and is likely to continue to grow. The increasing demand is creating an unprecedented opportunity for those professionals who develop the knowledge, skills, and abilities associated with fraud examination and financial forensics. For example, *The Wall Street Journal* stated that "forensic accounting is a particularly hot field" (*CPA Recruitment Intensifies as Accounting Rules Evolve*, March 22, 2005).[2] Moreover, each of the Big 4 firms is now recruiting accounting students with some exposure to financial forensics. The need for competent staffing at the SEC, at PCAOB, and in private industry is outpacing the supply. According to author Cecily Kellogg, the anticipated growth in the field is expected to be nearly 25 percent over the next ten years. Kellogg goes on to suggest that it is hard to envision a more stable and in-demand career.[3]

PLACES WHERE FRAUD EXAMINERS AND FINANCIAL FORENSIC SPECIALISTS WORK

Figure 2-1 captures several anticipated career paths for fraud examination and financial forensics.[4] Identified career paths include positions at professional service firms, corporations, and government or regulatory agencies and in law enforcement or legal services. Opportunities for fraud and forensic accounting professionals in professional services firms include external auditing, internal audit outsourcing, and forensic and litigation advisory services.

To become a successful professional requires additional specialized training and continuing professional development. Specialized training for entry-level staff helps them achieve the required level of *competency* within a specific organization. Some of the specialized training may be organization-specific, while other training may be task-specific. Further, experienced staff persons are required to maintain *proficiency* in a dynamic environment through continuing professional education courses.

Professional Services Firms

Fraud examiners and financial forensic specialists work in accounting and professional service firms that provide fraud deterrence, detection, investigation, and remediation services to a variety of organizations. In addition, professional service firms, specialized service, and boutique services firms provide litigation advisory services to individuals, as well as to businesses and other entities.

Public and Private Companies

Internal audit, corporate compliance, security, and internal investigation units all operate within companies and utilize the skills of the fraud examiner and the financial forensic professional.

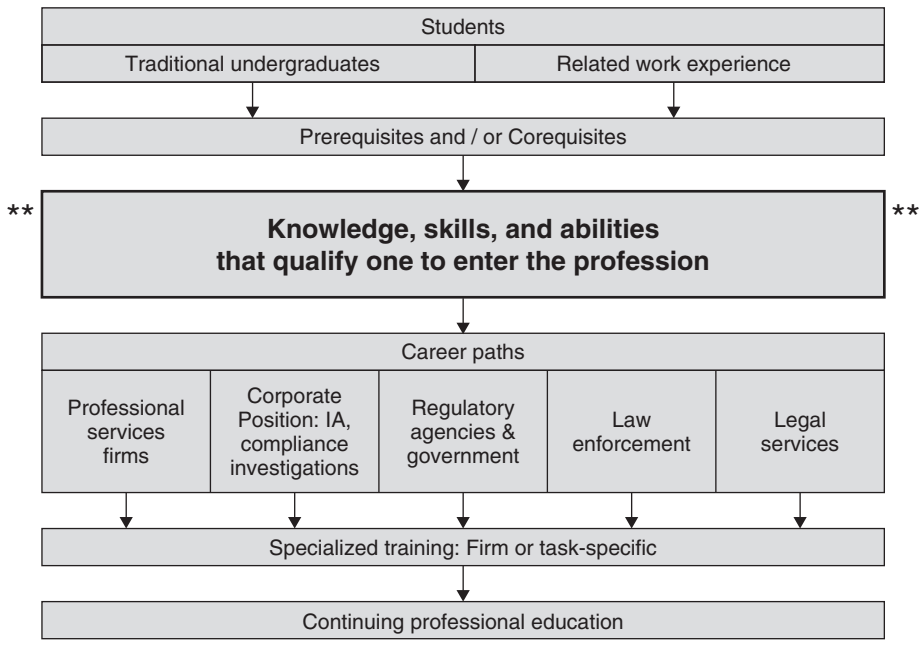


FIGURE 2-1 Career Paths

According to the Association of Certified Fraud Examiners' 2008 "Report to the Nation," internal auditors discover a significantly greater percentage of fraud than external auditors do. Many internal audit departments employ certified fraud examiners (CFE) and financial forensic specialists.

Compliance and risk analysis for SOX, environmental, or health and safety (OSHA) issues are handled by professionals as part of legal and regulatory oversight to prevent misconduct, including fraud. These professionals utilize their skills in terms of compliance and risk assessment as a proactive measure against wrongdoing.

Security, loss prevention, risk management, and investigation professionals with corporations and business entities often have responsibility to protect assets and detect instances of their misuse.

Other business sectors that frequently employ fraud professionals include the insurance, real estate, banking (including investment banking), securities, money management, credit card, health care, construction, and defense contracting industries.

Regulatory Agencies

Regulatory agencies such the Securities and Exchange Commission (SEC), the Public Company Accounting and Oversight Board (PCAOB), and others employ professionals with specialized knowledge, skills, training, education, and experience in fraud examination and financial forensics. Other government organizations, such as the Departments of Defense, Labor, and Homeland Security, may also hire fraud and financial forensic specialists.

Government and Nonprofits

Government accountants and auditors work in the public sector, maintaining and examining the records of government agencies and auditing private businesses and individuals whose activities are subject to government regulations or taxation. Those employed by the federal government may work as Internal Revenue Service agents.

One of the main missions of the Internal Revenue Service (IRS) is to identify unreported or underreported taxable income and the tax-payment deficiencies related to that income. Penalties and interest levied by the IRS on delinquent tax payments have a deterrent effect on the public. Agents are typically at the front line in detecting fraudulent taxpayer activities, whether in regard to payroll taxes, excise taxes, income taxes, or any other taxes. In recent years, the IRS has devoted increasingly greater resources to develop a workforce skilled in fraud detection and remediation. After IRS agents have sufficiently identified deliberate and egregious instances of tax evasion, the cases are further pursued by IRS professionals in the Criminal Investigation Division (CID), who are more like law enforcement personnel than they are auditors.

Professionals with financial forensic and fraud examination skills may also work at federal government agencies, like the Government Accountability Office (GAO), as well as at the state or local level. They administer and formulate budgets, track costs, and analyze programs for compliance with relevant regulations. This work can have a significant impact on the public good, but it may also be very political, as well as subject to bureaucratic obstruction. Government accounting offers advancement in most organizations through a competitive process that considers education and experience. Places that hire heavily at the federal level include the Department of Defense, the GAO, and the IRS. In addition, offices of the state and local comptrollers hire individuals with accounting knowledge or experience.

Nonprofit entities may include public school systems, charities, hospitals, and other healthcare facilities. According to the ACFE 2008 RTTN, fraud schemes at nonprofit and government agencies lasted approximately two years, as compared to the eighteen months they lasted at public companies. The challenges, related to fraud examination and financial forensics, have bled over to the public sector, and many of these organizations are hiring professionals with expertise in these areas.

Law Enforcement Agencies

Law enforcement agencies like the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Postal Inspectors, and others hire forensic accountants and fraud examiners. These professionals investigate money laundering, identity theft–related fraud, arson for profit, and tax evasion.

Although the SEC is not considered to be part of our law enforcement structure because they do not have criminal prosecutorial powers, they develop criminal cases and forward them to the Department of Justice for prosecution.

FROM THE FRAUDSTER'S PERSPECTIVE

Why White-Collar Criminals Do Not Fear Today's FBI

As the heartless, cold-blooded criminal CFO of Crazy Eddie, the Federal Bureau of Investigation was a respected adversary that filled my stomach with butterflies and caused me many sleepless nights as I feared their tenacity to successfully investigate my crimes. Unfortunately, the white-collar criminals of today have much less to fear from the FBI. According to an article in the *New York Times*,

> *The Federal Bureau of Investigation is struggling to find enough agents and resources to investigate criminal wrongdoing tied to the country's economic crisis, according to current and former bureau officials.*
>
> *The bureau slashed its criminal investigative work force to expand its national security role after the Sept. 11 attacks, shifting more than 1,800 agents, or nearly one-third of all agents in criminal programs, to terrorism and intelligence duties. Current and former officials say the cutbacks have left the bureau seriously exposed in investigating areas like white-collar crime, which has taken on urgent importance in recent weeks because of the nation's economic woes.*
>
> *The pressure on the F.B.I. has recently increased with the disclosure of criminal investigations into some of the largest players in the financial collapse, including Fannie Mae and Freddie Mac. The F.B.I. is planning to double the number of agents working financial crimes by reassigning several hundred agents amid a mood of national alarm. But some people inside and out of the Justice Department wonder where the agents will come from and whether they will be enough.*

Even if the FBI doubles the number of agents working financial crimes, it does not solve the main problem of effectively investigating white-collar crime. White-collar crime investigations are often complicated cases that take long periods of time and require enormous resources—and most important, experienced agents.

Top-notch, experienced FBI agents are leaving the bureau for higher-paying private industry jobs as soon as they qualify for retirement, causing a brain drain within the FBI. As white-collar crime becomes increasingly complex, our government must revise employee retention policies to compete with the private sector.

The FBI lacks adequate legal, technological, and personnel resources to meet its responsibilities to investigate white-collar crime. According to the *New York Times* article:

> *From 2001 to 2007, the F.B.I. sought an increase of more than 1,100 agents for criminal investigations*

apart from national security. Instead, it suffered a decrease of 132 agents, according to internal F.B.I. figures obtained by The New York Times. *During these years, the bureau asked for an increase of $800 million, but received only $50 million more. In the 2007 budget cycle, the F.B.I. obtained money for a total of one new agent for criminal investigations.*

Too often, complicated white-collar crime investigations fall apart because the FBI lacks experienced agents with the patience, knowledge, and experience to put together a successful criminal investigation. According to the *New York Times* article:

In some instances, private investigative and accounting firms are now collecting evidence, taking witness statements and even testifying before grand juries, in effect preparing courtroom-ready prosecutions they can take to the F.B.I. or local authorities.

"Anytime you bring to the F.B.I. a case that is thoroughly investigated and reduce the amount of work for investigators, the likelihood is that they will take the case and present it for prosecution," said Alton Sizemore, a former F.B.I. agent who is a fraud examiner for Forensic Strategic Solutions in Birmingham, Ala.

In other words, in order for the FBI to give serious consideration to many cases, such cases must be presented to the FBI neatly gift-wrapped and on a silver platter.

The criminals of today are elated by an underresourced and relatively inexperienced FBI. As a result, the cancer of white-collar crime continues to destroy the integrity of our great capitalist economic system.

Sam E. Antar (former Crazy Eddie CFO
and a convicted felon),
Sunday, October 19, 2008.
Adapted from http://whitecollarfraud.blogspot.com.

Law Firms

Law firms often use forensic accountants to help divorcees uncover a spouse's hidden assets and damages associated with contract disputes and tortuous interference. Most of these forensic professionals are employed as consultants and expert witnesses, but some law firms that do a significant amount of work in this area hire professionals to work on their staff. These forensic professionals can complete initial investigations and develop preliminary findings before a firm's clients incur considerable costs associated with hiring outside consultants. Forensic accountants may uncover instances of companies cooking the books to falsely inflate company profits, minimize losses, or divert large amounts of money to company managers.

RELATED PROFESSIONS

Law

The forensic professional needs to know about the law as it relates to mail and wire fraud, violations of the RICO Act (racketeering influence and corrupt organizations), money laundering, false claims, bankruptcy fraud, tax evasion, conspiracy, and obstruction of justice. Individual rights are protected by laws governing investigative techniques and the admissibility of evidence, including the chain of custody, search and seizure, interviewing, and surveillance. These laws require that "probable cause" is established prior to intrusive searches in order to comply with the statutory rules of evidence. Further, fraud examiners and forensic professionals need to be qualified as "experts" to offer evidence at trial.

Psychology

Forensic psychology is the application of the principles of psychology to the criminal justice system. Because fraud requires intent, in some cases it is necessary for forensic psychologists to delve into the psychological motives of white-collar criminals. These professionals must also address the legal issue of competency and whether a defendant was sane at the time the crime occurred.

The knowledge, skills, and abilities of forensic psychologists are used in various circumstances, such as when treating mentally ill offenders, consulting with attorneys (e.g., picking a jury), analyzing a criminal's mind and intent, and practicing within the civil arena. A forensic psychologist may chose to focus her career on researching—to give only two examples—how to improve interrogation methods or how to evaluate eyewitness testimony. Forensic psychologists have also been used to effectively design correctional facilities. With regard to fraud and financial issues, forensic psychology can help us to understand who commits fraud and why.

Sociology

Forensic sociology uses analysis of sociological data for decision making by the courts and other judicial agencies. The forensic sociologist may also serve as an expert witness in a court of law. Functions for these specialists include the profiling of offenders, unlawful discrimination, spousal abuse, pornography, toxic torts, and premises liability. Emphasis is given to the relationship between the standards of validity and reliability in sociology and the rules of evidence. Related to financial crimes, sociology helps us understand the context of these types of crimes. Data provided in the ACFE's biannual "Report to the Nation" helps us put occupational fraud and related crimes into context by addressing such issues as

- Is the incidence of fraud increasing or decreasing?
- What types of fraud are being committed?
- What is the cost of fraud?
- How is fraud committed?
- How is fraud detected?
- What are the victim profiles?
- What are the perpetrator profiles?

Criminology

Criminology is the study of crime and criminals and includes theories of crime causation, crime information sources, and the behavioral aspects of criminals. Beyond examining and attempting to understand human behavior and theories of crime causation, criminology considers the various types of crimes such as white-collar crime, organizational crime, and occupational crime and concerns itself with fraud prevention and deterrence issues. One of the most important contributions of criminology to the study of fraud is criminologist Donald Cressey's fraud triangle. Finally, criminology considers the "punishments" aspects of the remediation process.

Intelligence

When one thinks of business intelligence, developing corporate competitive intelligence systems and counterintelligence programs to prevent industrial espionage normally comes to mind. However, the prevention, deterrence, detection, and investigation of fraud is closely aligned with the skill set used by the intelligence community. Fraud examiners and forensic accountants take disparate pieces of information and pull them together into a coherent case that tells the story of who, what, when, where, how, and why. In addition, these professionals need to identify potential sources of evidence and then methodically collect that evidence for use in the case. Sources might include documents, interviews, surveillance tapes, public records, and data obtained from the Internet.

Information Systems and Computer Forensics

The impact of information systems in the areas of fraud examination and financial forensics is enormous. Information technology (IT) reaches every aspect of our lives today, and the digital environment plays a crucial role in fraud-related crimes and investigations due to the following factors:

- Increased use of information technology in business
- Large businesses centered on technology, such as Dell, IBM, Google, eBay, and Microsoft
- Increased data use by independent auditors, fraud examiners, and forensic accountants
- Increased exploitation of information technology by fraudsters and cybercriminals

IT professionals, including those with fraud and forensic accounting expertise, need to ensure that the organization's digital environment is adequately protected.

Electronic information feeding the financial reporting process needs to be timely and accurate, and reasonable controls should be in place to support organizational viability in a digital world and its associated threats and opportunities.

Information Systems Governance and Controls Information systems governance and controls are concerned with the prevention, deterrence, and detection of fraud in a digital environment. An organization's information technology group must adhere to best practices consistent with those of the organization as a whole. Information Systems Audit and Control Association (ISACA) is a global organization for information governance, control, security, and audit whose information systems auditing and control standards are followed by practitioners worldwide. ISACA defines IT governance as a set of principles to assist enterprise leaders in their responsibility to ensure that (1) the organization's information technology needs are aligned with the business's goals and deliver value, (2) the organization's performance is measured, (3) the organization's resources are properly allocated, and (4) the organization's risks are mitigated. Best practices associated with IT governance should include preventive countermeasures against fraud and cybercrime, such as continuous auditing and proactive fraud auditing.

Risk assessment is a critical aspect of good corporate governance and the same concept is applicable in an information technology environment. An IT risk assessment should identify risks associated with the digital environment. That assessment requires that IT leadership know and understand how IT prevents and detects internal and external attacks, including those associated with the commission of frauds, computer crimes, and cybercrimes. As part of that risk assessment, IT professionals need to identify and understand the ways in which IT systems are typically exploited during fraud and cybercrime, how IT systems are used to facilitate fraud concealment, and how IT security is commonly breached or circumvented.

Cyberforensics The increased role of information technology in fraud and cybercrime results in a corresponding increase in the need for organizational professionals with digital knowledge, skills, and abilities—in operations systems, but also in fraud, computer crime, and cybercrime. Evidence about who, what, where, when, and how often exists in digital form—in some cases, exclusively. Furthermore, most state-of-the-art digital forensics tools and techniques have come into existence in the last ten to twenty years. The pervasiveness of digital media and information in virtually every aspect of an organization's life illustrates the increased need for cyberforensic specialists. Cyberforensics involves capture, preservation, identification, extraction, analysis, documentation, and case preparation related to digital data and events.

Digital Evidence Capturing electronic information is the first step in the investigation of digital evidence. Because it is possible to hinder a successful legal outcome if the legal requirements associated with digital capture are not followed, a successful cyberforensics investigation requires a professional who has the required technical background in computer technology and systems and who is also familiar with the relevant rules of the legal system and investigations. For example, turning on a confiscated computer can make all the evidence on that computer inadmissible in a courtroom, because this simple act alters the hard drive, thus breaking the chain of custody. Only those persons with specialized training, experience, and appropriate professional certifications should initially capture digital evidence.

The sources of digital evidence are evolving and expanding but include cell phones, personal digital assistants (PDAs), Blackberrys and similar phones, trinkets with digital storage (watches, USB pens, digital cameras, etc.), jump drives, media cards, e-mail, voicemail, CDs, DVDs, printer memory, RAM, slack space, removable drives, iPods/MP3 players, and XM/Sirius radio players. There are also such conventional sources as laptops, office computers, home computers and external drives, servers on the Internet that store e-mail messages, and the entity's own servers. Special software and hardware tools are available to capture digital evidence, such as SF-5000, RoadMASSter, and write blockers.

Electronic Detection and Investigation Notwithstanding the utilization of traditional detection and investigation techniques applied in a digital environment, some additional tools and techniques are also important. Those tools and techniques include data mining software useful for data extraction and analysis and continuous monitoring and auditing software. Most data extraction and analysis tools can retrieve, filter, extract, sort, and analyze data from accounting databases as well as identify gaps, duplicates, missing information, and statistical anomalies.

Cybercrime The Department of Justice defines cybercrime as any violation of criminal law that involves knowledge of computer technology for its perpetration, investigation, or prosecution. Cybercrime knowledge, skills, and abilities include a basic understanding of the types of crimes, as well as of special laws and relevant criminal code. Some typical cybercrimes include unauthorized computer intrusion, hacking, infrastructure attacks, digital credit card theft, online/e-mail extortion, viruses, worms, identity theft, online gambling, theft of computers, online narcotic sales, cyberterrorism, and telecommunications fraud.

Other Forensic Science Fields

Fraud examination and forensic accounting also utilize knowledge, skills, and abilities from other forensic sciences such as crime scene investigation, forensic chemistry, and biology. For example, in crime scene investigation, the investigator has three primary goals: protection of evidence (e.g., crime scene tape), preservation of evidence, and collection of evidence. Although an accounting department and the IT systems cannot be "roped off" with crime scene tape, it is important for the fraud examiner or forensic accountant to be thinking about three concepts: (1) protecting the evidence by using backup tapes of the computer system collected and protected in such a way as to be admissible in court, (2) preserving the evidence by preventing physical and electronic corruption and destruction, and (3) collecting the evidence in sufficient amounts and in a manner that protects the chain of custody. These types of lessons are routinely available from our colleagues in other forensic fields.

Related Career Titles In short, forensic accountants and fraud examiners have opportunities in a number of fields and under a number of titles wherein they combine their forensic and investigative training with other forms of expertise:

Actuary	FBI Agent	Administrator
Internal Auditor	CIA Agent	Business Teacher
Auditor	Financial Analyst	Contract Administrator
Consumer Credit Officer	Methods/Procedures Specialist	Financial Investment Analyst
Bank Examiner	Claims Adjuster	EDP Auditor
Controller	Collection Agent	Insurance Investigator
Benefits/Compensation	Governmental Accountant	Inventory Control Specialist
IRS Investigator	Personal Financial Planner	IRS Investigator
Budgetary Control Analyst	Commercial Banker	Property Accountant
Credit and Collection	Industrial Accountant	Systems Analyst
Loan Administrator	Plant Accountant	Tax Compliance Specialist
Entrepreneur	Professor	Treasurer
Loan/Consumer Credit	Systems Analyst	Treasury Management Specialist
Management Consultant	Systems Accountant	Tax Supervisor/Auditor
Chief Financial Officer	Budget Accountant	Treasury Management
Accountant, Public Practice	Claim Adjuster/Examiner	

BUSINESS ADMINISTRATION, MANAGEMENT, AND CORPORATE GOVERNANCE

FROM THE FRAUDSTER'S PERSPECTIVE

Advice to President-Elect Barack Obama from a Convicted Felon about Combating White-Collar Crime

To President-Elect Barack Obama:
While our capital markets require reform, no amount of regulation or oversight can be effective unless those persons charged with carrying it out have the proper amount of experience, knowledge, competence, and professional skepticism to successfully perform their respective jobs and responsibilities. As the cold-blooded and heartless criminal CFO of Crazy Eddie, I had no fear of oversight from outside or independent board members and our external auditors. I took advantage of their lack of requisite skills, knowledge, and experience to effectively carry out my crimes. If you want to see capitalism succeed as an engine for our future economic prosperity, I respectfully ask you to first consider the issue of competence before looking at the issue of regulation and oversight.

Window Dressing Boards of Directors

We need better standards of qualification for public company board members. Too often, company boards are packed with people with great résumés, but such persons have no specialized experience and training to effectively carry out their functions, or boards are packed with cronies of company management. Instead, we must require that board members have the proper amount of specialized education, background, and experience necessary to perform their duties effectively. We do not need well-meaning, intelligent people serving in

positions they are not well suited for, since in many cases they make ineffective board members. The time for "window dressing" must end.

Today, too many board members are appointed for window dressing purposes only, rather than because of their specific competence to carry out their duties. Michelle Leder's blog, Footnoted.org, once noted:

> *So where do former members of the House and Senate, not to mention Governors and former Cabinet members go when they exit from the political stage? Many of them wind up filling seats on boards of directors.*

For example, your new Chief of Staff Rahm Emanuel was appointed by President Bill Clinton to serve on Freddie Mac's (NYSE: FRE) board of directors after serving in Clinton's administration. I am assuming that Mr. Emanuel took the job and served on Freddie Mac's board from 2000 to 2001 with the best of intentions. However, like many other well-meaning but gullible board members, he found himself in the wrong place at the wrong time, in the hands of an unscrupulous management team.

According to the SEC complaint filed against Freddie Mac:

> *Freddie Mac misreported its net income in 2000, 2001 and 2002 by 30.5 percent, 23.9 percent and 42.9 percent, respectively. Furthermore, Freddie Mac's senior management exerted consistent pressure to have the company report smooth and dependable earnings growth in order to present investors with the image of a company that would continue to generate predictable and growing earnings.*
>
> *"As has been seen in so many cases, Freddie Mac's departure from proper accounting practices was the result of a corporate culture that sought stable earnings growth at any cost," said Linda Chatman Thomsen, the SEC's Director of Enforcement.* "Investors do not benefit when good corporate governance takes a back seat to a single-minded drive to achieve earnings targets."

Rahm Emanuel was not named in the SEC's complaint against Freddie Mac. However, in a statement before the Senate Committee on Banking, Housing, and Urban Affairs, Acting Director of the Office of Federal Housing Enterprise Oversight, James B. Lockhart III noted:

> *For the most part, the same long-tenured shareholder-elected Directors oversaw the same CEO, COO, and General Counsel of Freddie Mac from 1990 to 2003. The non-executive Directors allowed the past performance of those officers to color their oversight.* Directors should have asked more questions, pressed harder for resolution of issues, and not automatically accepted the rationale of management for the length of time needed to address identified weaknesses and problems. *The oversight exercised by the Board might have been more vigorous if there had been a regular turnover of shareholder-elected Directors or if Directors had not expected to continue to serve on the Board until the mandatory retirement age. Conversely, the terms of the presidentially appointed Directors are far too short, averaging just over 14 months, for them to play a meaningful role on the Board. The position is an anachronism that should be repealed so shareholders can elect all Directors.* The Board of Directors was apprised of control weaknesses, the efforts of management to shift income into future periods and other issues that led to the restatement, but did not recognize red flags, failed to make reasonable inquiries of management, or otherwise failed in its duty to follow up on matters brought to its attention.

The problem is that intelligent and well-meaning boards of directors are often duped by unscrupulous company management teams who take advantage of their lack of requisite skills and professional cynicism.

Prospective qualified board members must know how to make effective inquiries and spot red flags. They must know how to ask questions, whom to direct their questions to, and how to handle false and misleading answers by management with effective follow-up questions. Such skills only come from adequately qualified board members who have proper training, education, and experience *before* they join company boards.

Lack of Truly Independent and Properly Qualified Audit Committee Members

So-called independent audit committee members of boards of directors are *less* independent and *less* competent than the external auditors whom they oversee. Too many audit committee members have no formal educational background in accounting and auditing, and no specialized training in fraud detection.

Many "independent" board members own stock and receive stock options in their respective companies, while independent external auditors *cannot* own stock or receive stock-based compensation from their audit clients. Owning company stock and receiving stock-based compensation provides a disincentive to effective independent audit committee oversight of financial reporting and can adversely affect an audit committee member's professional skepticism. Audit committee members cannot be considered truly independent if they own company stock or receive stock-based compensation. I suggest that our securities laws be amended to require truly independent and adequately qualified audit committees.

Lack of Properly Trained Auditors

External auditors receive too little or no training in forensic accounting, fraud detection, or criminology. Most CPAs never take a single college-level course devoted exclusively to issues of white-collar crime or internal controls, and many important subjects covered in the CPA licensing exam are learned *after* graduation, in a cram CPA exam review course.

College-level accounting education needs to be reformed to teach future CPAs the necessary tools to do battle in audits against corporate crooks who take advantage of their lack of skills. We should mandate that a larger proportion of the continuing professional education required by CPAs to maintain their licenses be devoted to issues of white-collar crime and fraud detection.

Not Enough Law Enforcement Resources Devoted to White-Collar Crime

While I never feared Crazy Eddie's board of directors and auditors, I did fear the Securities and Exchange Commission and the Federal Bureau of Investigation. However, I doubt that many criminals have such fear for the SEC and FBI today.

Both the SEC and FBI are underresourced and overwhelmed, and as a result, they are unable to successfully investigate very many complicated white-collar crime cases unless such cases are handed to them on a silver platter by others. The most experienced SEC and FBI personnel are leaving government work for better-paying private sector jobs. Therefore, if you really want criminals to think twice before executing their crimes, I suggest that you beef up our nation's investigative and law enforcement resources.

Our capital markets depend on the integrity of financial information that is supposed to be insured by external auditors, audit committees, and consistently effective law enforcement. Inadequately trained independent external auditors, the first line of defense for ensuring the integrity of financial reporting, are supervised by even less competent and less independent audit committees. On top of that, our regulators and law enforcement agencies lack the required resources to effectively prosecute many crimes enabled by the lack of effective audits and company oversight by boards of directors. Therefore, we face a perfect storm for disaster, as the cancer of white-collar crime destroys our economic fabric and inflicts a collective harm on our great society.

If you want capitalism to succeed as an engine of prosperity for our great nation, I ask you to heed my advice based on my experience as a cold-blooded convicted felon.

Respectfully:

Sam E. Antar (former Crazy Eddie CFO and a convicted felon)

PS: While Rahm Emanuel may not have been an effective board member of Freddie Mac, he can provide valuable insight to you about the perils of lack of effective oversight by boards of directors. After all, the wisest people are those that learn from past mistakes.

In addition, I will continue to provide you with more unsolicited advice from time to time. You can learn a lot from a convicted felon who scammed the system and took advantage of gullible human beings in ways your advisors never dreamed of.

Sunday, November 16, 2008. http://whitecollarfraud.blogspot.com/2008/11/advice-to-president-elect-barack-obama.html

In recent years, corporate governance, including boards of directors, audit committees, executive management, internal audit, external audit, the government, and regulators have been intensely scrutinized by those concerned with the public's interests. Corporate governance simply means the way a corporation is governed through proper accountability for managerial and financial performance. The integrity and quality of the capital market primarily depends on the reliability, vigilance, and objectivity of corporate governance. Particularly, with respect to financial statement fraud, there has been a great deal of concern about the issue of corporate governance and accountability of publicly traded companies. The corporate governance concept has advanced from the debates on its relevance to how best to protect investor interests and effectively discharge oversight responsibility over the financial reporting process. High-profile financial statement frauds allegedly committed by major corporations such as Waste Management, Phar-Mor, ZZZZ Best, Crazy Eddie, Sunbeam, Enron, WorldCom, Adelphia, HealthSouth, Lucent, Xerox, MicroStrategy, Cendant, Rite Aid, and KnowledgeWare have renewed the interest and increasing sense of urgency about more responsible corporate governance and more reliable financial statements.

There has also been a growing awareness that corporate governance can play an important role in preventing and detecting financial statement and other types of fraud and corporate malfeasance. Management's ethical behavior and operating style can have a significant impact on the effectiveness of corporate governance. An operating style that shows excessive risk-taking, for example, is generally a red flag for fraud.

The following outlines the basics of fraud risk management for those charged with corporate governance: the board of directors, the audit committee, management, internal auditors, and external auditors. "Managing the Business Risk of Fraud: A Practical Guide," developed by the IIA, AICPA, and ACFE, suggests that with regard to corporate malfeasance, fraud risk management needs to include five key features:[5]

1. A written policy that outlines the fraud risk management program
2. (Targeted) fraud risk assessment of the exposure of the organization to potential schemes that need mitigation.
3. Prevention techniques
4. Detection techniques:
   - In place in case preventative measures fail
   - In place to address unmitigated risks (where the cost of mitigation exceeds the benefits)
   - In place to address concerns over collusion and management override
5. A reporting process

Boards of Directors

One of the primary roles of the board of directors in corporate America is to create a system of checks and balances in an organization through its authority to hire and monitor management and evaluate their plans and decisions and the outcomes of their actions. The separation of ownership and control in corporations requires the board of directors to (1) safeguard assets and invested capital, (2) review and approve important management decisions, (3) assess managerial performance, and (4) allocate rewards in ways that encourage shareholder value creation.

The board of directors, as an important internal component of corporate governance, receives its authority from shareholders who use their voting rights to elect board members. The board of directors' primary responsibility is one of gatekeeper, an ultimate internal control mechanism to protect the interests of shareholders, creditors, and other stakeholders. Therefore, one goal is to minimize the ability of management to expropriate shareholder value through financial statement and other forms of fraud and financial malfeasance.

Audit Committees

The audit committee is a subcommittee of the board of directors and has the primary responsibility of monitoring the financial reporting and auditing processes. Thus, reviewing the effectiveness of internal controls to ensure the reliability of financial reports is an essential part of the audit committee's role. The audit committee oversees the adequacy and effectiveness of the company's internal control structure to ensure

1. The efficiency and effectiveness of operations
2. The reliability of financial reporting
3. Compliance with applicable laws and regulations

Additionally, the audit committee is charged with addressing the risk of collusion and management override of internal controls. In February 2005, the American Institute of Certified Public Accountants (AICPA) issued a report titled "Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention." It notes that management may override internal controls and engage in financial statement fraud by (1) recording fictitious business transactions and events or altering the timing of recognition of legitimate transactions, (2) recording and reversing biased reserves through unjustifiable estimates and judgments, and (3) changing the records and terms of significant or unusual transactions.

To be proactive, the audit committee should ensure that

- Audit committee members have knowledge, education, awareness, and sophistication concerning the various fraudulent management override and collusive schemes that may be perpetrated by management
- Both the internal and external audit groups have knowledge, education, awareness, and sophistication concerning the various fraudulent management override and collusive schemes that may be perpetrated by management
- The audit committee has reviewed the comprehensive fraud risk assessment provided by management and also considers how collusive fraud and management override schemes are mitigated and detected
- The audit committee periodically participates in continuing education programs that can prepare its members to appraise management's fraud risk assessment
- The audit committee identifies who has the specific responsibility for the collusive and management override fraud risk assessment process: its members, the internal audit group, or the independent audit group?
- The audit committee is interacting with personnel beyond executive management and asking the tough questions of knowledgeable employees, financial managers, internal auditors, and external auditors
- The audit committee has a protocol for acting on allegations of unethical and potentially fraudulent conduct

Senior/Executive Management

Management is primarily responsible for the quality, integrity, and reliability of the financial reporting process, as well as the fair presentation of financial statements in conformity with generally accepted accounting principles (GAAP). Management is also accountable to users of financial statements, particularly investors and creditors, to ensure that published financial statements are not misleading and are free of material errors, irregularities, and fraud.

To effectively discharge its financial reporting responsibility, management should (1) identify and assess the circumstances, conditions, and factors that can lead to fraud, (2) assess and manage the risk of fraud associated with the identified circumstances, conditions, and factors, and (3) design and implement an adequate and effective internal control process for prevention and detection of fraud.

Internal Audit

Internal auditors are an important part of corporate governance and, if assigned, can be tasked and positioned to help ensure a reliable financial reporting process. Internal auditors' day-to-day involvement with both operational and financial reporting systems and the internal control structure provides them with the opportunity to perform a thorough and timely assessment of high-risk aspects of the internal control environment and financial reporting process. However, the effectiveness of internal auditors to prevent and detect fraud depends largely on their organizational status and reporting relationships. Financial statement fraud is normally perpetrated by the top management team. As such, internal audit standards issued by the Institute of Internal Auditors (IIA) require that internal auditors be alert to the possibility of intentional wrongdoing, errors, irregularities, fraud, inefficiency, conflicts of interest, waste, and ineffectiveness in the normal course of conducting an audit. These professionals are also required to inform the appropriate authorities within the organization of any suspected wrongdoing and follow-up to ensure that proper actions are taken to correct the problem.

External (Independent) Audit

Financial statement fraud has been, and continues to be, the focus of the auditing profession. During the early 1900s, external auditors viewed the detection of fraud, particularly financial statement fraud, as the primary purpose of their financial audit. During the twentieth century, the auditing profession moved from acceptance of fraud detection as their primary responsibility to the mere expression of an opinion on the fair presentation of the financial statements. Recently, the accounting profession directly addressed the external auditor's responsibility to detect financial statement fraud in its Statement on Auditing Standards (SAS) No. 99, titled "Consideration of Fraud in a Financial Statement Audit." SAS No. 99 requires independent auditors to obtain information to identify financial statement fraud risks, assess those risks while taking into account the entity's programs and controls, and respond to the results of this assessment by modifying their audit plans and programs.

Auditors in identifying and assessing the risks of material financial statement fraud should (1) make inquiries of the audit committee or other comparable committee of the board of directors, senior executives, legal counsel, chief internal auditors, and others charged with government governance within the client organization to gather sufficient information about the risk of the fraud, (2) communicate with the audit committee, management, and legal counsel about the allegations of fraud and how they are addressed, (3) consider all evidence gathered through analytical procedures that is considered unusual, unexpected, or even suspiciously normal based on the financial condition and results of the business, and (4) consider evidence gathered through the audit of internal control of financial reporting that may suggest the existence of one or more fraud risk factors, and that adequate and effective internal controls did not address and account for the detected risk. Auditors should inquire of the audit committee, management, and others charged with government governance about the entity's antifraud policies and procedures and whether they are in writing, updated on a timely basis, implemented effectively, and enforced consistently.

Regulators and Governing Bodies

Regulatory reforms in the United States are aimed at improving the integrity, safety, and efficiency of the capital markets while maintaining their global competitiveness. Regulations should be perceived as being fair and in balance in order to inspire investor confidence. Regulations, including SOX, are aimed at protecting investors. The provisions of SOX- and SEC-related rules include strengthening the corporate

board and external auditor independence, instituting executive certifications of both financial statements and internal controls, and creating the PCAOB to oversee the accounting profession. These provisions helped to rebuild investor confidence in public financial information.

The various corporate governance participants are being held to greater levels of accountability to create an environment where the risk of fraud is mitigated, at least to levels below the materiality threshold. As such, individuals with knowledge, skills, and abilities in these areas are in demand, which has created employment opportunities for those professionals who have developed this type of expertise.

PROFESSIONAL ORGANIZATIONS AND THEIR RELATED CERTIFICATIONS

Association of Certified Fraud Examiners (ACFE)

The ACFE is the world's premier provider of antifraud training and education. Together with its nearly 50,000 members, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity within the profession. The mission of the Association of Certified Fraud Examiners is to reduce the incidence of fraud and white-collar crime and to assist the membership in fraud detection and deterrence. To accomplish its mission, the ACFE

- Provides bona fide qualifications for certified fraud examiners through administration of the CFE Examination
- Sets high standards for admission, including demonstrated competence through mandatory continuing professional education
- Requires certified fraud examiners to adhere to a strict code of professional conduct and ethics
- Serves as the international representative for certified fraud examiners to business, government, and academic institutions
- Provides leadership to inspire public confidence in the integrity, objectivity, and professionalism of certified fraud examiners

Certified Fraud Examiner (CFE) The ACFE established and administers the Certified Fraud Examiner (CFE) credential. The CFE credential denotes expertise in fraud prevention, detection, and deterrence. There are currently more than 20,000 CFEs worldwide. As experts in the major areas of fraud, CFEs are trained to identify the warning signs and red flags that indicate evidence of fraud and fraud risk. To become a CFE, one must pass a rigorous examination administered by the ACFE, meet specific education and professional requirements, exemplify the highest moral and ethical standards, and agree to abide by the CFE Code of Professional Ethics. A certified fraud examiner also must maintain annual CPE requirements and remain an ACFE member in good standing. The FBI officially recognizes the CFE credential as a critical skill set for its diversified hiring program, and the U.S. Department of Defense officially recognizes the CFE credential as career advancement criteria. the Forensic Audits and Special Investigations Unit (FSI) of the Government Accountability Office announced that all professionals in the FSI unit must obtain CFE credentials.

American Institute of Certified Public Accountants (AICPA)

The AICPA is the national professional organization for all certified public accountants. Its mission is to provide members with the resources, information, and leadership to enable them to provide valuable services in the highest professional manner to benefit the public as well as employers and clients. In fulfilling its mission, the AICPA works with state Certified Public Accountant (CPA) organizations and gives priority to those areas where public reliance on CPA skills is most significant. The CPA is still one of the most recognized and valued professional certifications of any profession and is the standard bearer for accountants working in the United States.

Furthermore, the Forensic and Valuation Services (FVS) Center of the AICPA is designed to provide CPAs with a vast array of resources, tools, and information about forensic and valuation services. The center has information and resources for the following issues:

- Analytical guidance
- Family law

- Antifraud/forensic accounting
- Laws, rules, standards, and other guidance
- Bankruptcy
- Litigation services
- Business valuation
- Practice aids and special reports
- Document retention and electronic discovery
- Practice management
- Economic damages
- Fair value for financial reporting

Accredited in Business Valuation (ABV) The mission of the ABV credential program is to provide a community of business valuation experts with specialized access to information, education, tools, and support that enhance their ability to make a genuine difference for their clients and employers. The ABV credential program allows credentialholders to brand or position themselves as CPAs who are premier business valuation service providers. ABV credentialholders differentiate themselves by going beyond the core service of reaching a conclusion of value to also create value for clients through the strategic application of this analysis. The ABV credential program is designed to

- Increase public awareness of the CPA as the preferred business valuation professional
- Increase exposure for CPAs who have obtained the ABV credential
- Enhance the quality of the business valuation services that members provide
- Ensure the continued competitiveness of CPAs versus other valuation services providers through continuous access to a comprehensive community of resources and support
- Increase the confidence in the quality and accuracy of business valuation services received from CPA/ABV providers

Certified Information Technology Professional (CITP) A Certified Information Technology Professional (CITP) is a certified public accountant recognized for technology expertise and a unique ability to bridge the gap between business and technology. The CITP credential recognizes technical expertise across a wide range of business and technology practice areas. The CITP credential is predicated on the facts that in today's complex business environment, technology plays an ever-growing role in how organizations meet their business obligations, and that no single professional has a more comprehensive understanding of those obligations than a certified public accountant. An increasingly competitive global marketplace has organizations clamoring for new technologies and the capacities, efficiencies, and advantages they afford. While IT professionals have the technical expertise necessary to ensure that technology solutions are properly deployed, they lack the CPA's perspective and ability to understand the complicated business implications associated with technology. The CITP credential encourages and recognizes excellence in the delivery of technology-related services by CPA professionals and provides tools, training, and support to help CPAs expand their IT-related services and provide greater benefit to the business and academic communities they serve.

Certified in Financial Forensics (CFF) In May 2008, the AICPA's governing council authorized the creation of a new CPA specialty credential in forensic accounting. The Certified in Financial Forensics (CFF) credential combines specialized forensic accounting expertise with the core knowledge and skills that make CPAs among the most trusted business advisers. The CFF encompasses fundamental and specialized forensic accounting skills that CPA practitioners apply in a variety of service areas, including bankruptcy and insolvency, computer forensics, economic damages, family law, fraud investigations, litigation support, stakeholder disputes, and valuations. To qualify, a CPA must be an AICPA member in good standing, have at least five years' experience practicing accounting, and meet minimum requirements in relevant business experience and continuing professional education. The objectives of the CFF credential program are to

- Achieve public recognition of the CFF as the preferred forensic accounting professional
- Enhance the quality of forensic services that CFFs provide
- Increase practice development and career opportunities for CFFs
- Promote members' services through the Forensic and Valuation Services (FVS) Web site

Forensic CPA Society (FCPAS)

The Forensic CPA Society was founded July 15, 2005. The purpose of the society is to promote excellence in the forensic accounting profession. One of the ways the society has chosen to use to accomplish this is the Forensic Certified Public Accountant (FCPA) certification. The use of this designation tells the public and the business community that the holder has met certain testing and experience guidelines and has been certified not only as a CPA, but also as a forensic accountant.

Forensic Certified Public Accountant (FCPA). An individual must be a licensed CPA, CA (Chartered Accountant) or another country's CPA equivalent to be eligible to take the five-part certification test and receive the FCPA designation. If an individual is a licensed CPA and a CFE, Cr.FA, or CFF, he or she is exempt from taking the certification exam and can automatically receive the FCPA. Once an individual has earned his or her FCPA, he or she must take twenty forensic accounting– or fraud-related hours of continuing professional education (CPE) each year to keep his or her membership current.

Information Systems Audit and Control Association (ISACA)

Since its inception, ISACA has become a pace-setting global organization for information governance, control, security, and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide. Its research pinpoints professional issues challenging its constituents, and its Certified Information Systems Auditor (CISA) certification is recognized globally and has been earned by more than 60,000 professionals since inception. The Certified Information Security Manager (CISM) certification uniquely targets the information security management audience and has been earned by more than 9,000 professionals. The Certified in the Governance of Enterprise IT (CGEIT) designation promotes the advancement of professionals who wish to be recognized for their IT governance–related experience and knowledge and has been earned by more than 200 professionals. It publishes a leading technical journal in the information control field (the *Information Systems Control Journal*) and hosts a series of international conferences focusing on both technical and managerial topics pertinent to the IS assurance, control, security, and IT governance professions. Together, ISACA and its affiliated IT Governance Institute lead the information technology control community and serve its practitioners by providing the elements needed by IT professionals in an ever-changing worldwide environment.

Certified Information Systems Analyst (CISA) The technical skills and practices that CISA promotes and evaluates are the building blocks of success in the field. Possessing the CISA designation demonstrates proficiency and is the basis for measurement in the profession. With a growing demand for professionals possessing IS audit, control, and security skills, CISA has become a preferred certification program by individuals and organizations around the world. CISA certification signifies commitment to serving an organization and the IS audit, control, and security industry with distinction.

Certified Information Security Manager (CISM). The Certified Information Security Manager (CISM) certification program is developed specifically for experienced information security managers and those who have information security management responsibilities. CISM is unique in the information security credential marketplace because it is designed specifically and exclusively for individuals who have experience managing an information security program. The CISM certification measures an individual's management experience in information security situations, not general practitioner skills. A growing number of organizations are requiring or recommending that employees become certified. For example, the U.S. Department of Defense (DoD) mandates that information assurance personnel be certified with a commercial accreditation approved by the DoD. CISM is an approved accreditation, signifying the DoD's confidence in the credential. To help ensure success in the global marketplace, it is vital to select a certification program based on universally accepted information security management practices. CISM delivers such a program.

Institute of Internal Auditors (IIA)

Established in 1941, the Institute of Internal Auditors (IIA) is an international professional association of more than 150,000 members with global headquarters in Altamonte Springs, Florida. Worldwide, the IIA is recognized as the internal audit profession's leader in certification, education, research, and technical guidance. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator. Members work in internal auditing, risk management, governance,

internal control, information technology audit, education, and security. The mission of the IIA is to provide dynamic leadership for the global profession of internal auditing. Although the institute does not have a designation directly associated with fraud examination and forensic accounting, its dedication to this area is demonstrated in its training programs, its work with the Institute for Fraud Prevention, and its leadership in developing (along with the ACFE and AICPA) "Managing the Risk of Fraud: A Practical Guide."

Certified Internal Auditor. The Certified Internal Auditor (CIA) designation is the only globally accepted certification for internal auditors and remains the standard by which individuals demonstrate their competency and professionalism in the internal auditing field. Candidates leave the program with educational experience, information, and business tools that can be applied immediately in any organization or business environment.

National Association of Certified Valuation Analysts (NACVA)

NACVA's Financial Forensics Institute (FFI) was established in partnership with some of the nation's top authorities in forensic accounting, law, economics, valuation theory, expert witnessing, and support fundamentals to offer practitioners comprehensive training in all facets of forensic financial consulting. The Certified Forensic Financial Analyst (CFFA) designation offers five different pathways to acquire the specialized training.

Financial Litigation Path. The Financial Litigation specialty program requires the five-day Litigation Bootcamp for Financial Experts training, designed to provide participants with a foundation in the role of a financial expert. Among other requirements, applicants must have been involved in eight different litigation matters, for three of which the applicant gave deposition or expert testimony. (This experience requirement can be met by attending the three-day Financial Forensics Institute-sponsored course Expert Witness Bootcamp.)

Forensic Accounting Path. The Forensic Accounting specialty program requires attendance at the five-day Forensic Accounting Academy, plus the three-day litigation workshop Forensics Workshop for Financial Professionals. Among other requirements, applicants must have also been involved in ten engagements or have 1,000 hours of experience in the applicable field.

Business and Intellectual Property Damages Path. The Business and Intellectual Property Damages specialty program requires attendance at the five-day Business and Intellectual Property Damages Workshop (BIPD), plus the three-day Forensics Workshop for Financial Professionals. Among other requirements, applicants must have also been involved in ten engagements or have 1,000 hours of experience in the applicable field.

Business Fraud—Deterrence, Detection, and Investigation Path. The Business Fraud Deterrence, Detection, and Investigation specialty program requires attendance at the five-day Business Fraud—Deterrence, Detection, and Investigation Training Center (FDDI), plus the three-day Forensics Workshop for Financial Professionals.

Matrimonial Litigation Support Path. The Matrimonial Litigation Support specialty program requires attendance at the five-day Matrimonial Litigation Support Workshop, plus the three-day Forensics Workshop for Financial Professionals. Among other requirements, applicants must have also been involved in ten engagements in the applicable field or have 1,000 hours of experience providing valuation services, 200 hours of which were in the applicable field.

NACVA also has four certifications: Accredited Valuation Analyst (AVA), Certified Forensic Financial Analyst (CFFA), Certified in Fraud Deterrence (CFD), and Certified Valuation Analyst (CVA).

Society of Financial Examiners (SOFE)

The Society of Financial Examiners is a professional society for examiners of insurance companies, banks, savings and loans, and credit unions. The organization has a membership of over 1,600 representing the fifty states, the District of Columbia, Canada, Aruba, and the Netherlands Antilles. SOFE is the one organization in which financial examiners of insurance companies, banks, savings and loans, and credit unions come together for training and to share and exchange information on a formal and informal level. The society was established in 1973 to establish a strict code of professional standards for members engaged in the examination of financial institutions, to promote uniform ethical standards to engender employer and public confidence to the degree that those interested can identify professionally qualified practitioners, and to promote and enforce minimum requirements of conduct, training, and expertise for members engaged in financial examination. SOFE offers three professional designations, which may be earned by completing

extensive requirements including the successful completion of a series of examinations administered by the society. The designations are Accredited Financial Examiner, Certified Financial Examiner, and Automated Examiner Specialist.

INTERNATIONAL FRAUD EXAMINATION AND FINANCIAL FORENSICS

Chartered Accountant (CA), one equivalent of the CPA around the globe, is the title used by members of certain professional accountancy associations in the British Commonwealth nations and Ireland. The term "chartered" comes from the Royal Charter granted to the world's first professional body of accountants upon their establishment in 1854.

The Association of Certified Fraud Examiners, which administers the certified fraud examiner (CFE) credential, has international activities in more than 120 countries around the world. Other international certifications related to the fraud examination and forensic accounting specializations include the following:

- AAFM: The American Academy of Financial Management offers sixteen separate financial certifications recognized worldwide
- MFP: Master Financial Professional
- CWM: Chartered Wealth Manager
- CTEP: Chartered Trust and Estate Planner
- CAM: Chartered Asset Manager
- RFS: Registered Financial Specialist in Financial Planning
- CPM: Chartered Portfolio Manager
- RBA: Registered Business Analyst
- MFM: Master Financial Manager
- CMA: Chartered Market Analyst
- FAD: Financial Analyst Designate
- CRA: Certified Risk Analyst
- CRM: Certified in Risk Management
- CVM: Certified Valuation Manager
- CCC: Certified Cost Controller (offered in the Middle East, Europe, Asia, and Africa)
- CCA: Certified Credit Analyst (offered in Asia, the Middle East, and Africa)
- CCA: Chartered Compliance Analyst
- CITA: Certified International Tax Analyst (for lawyers or LLM holders)
- CAMC: Certified Anti-Money Laundering Consultant (for lawyers or LLM holders)
- Ch.E. Chartered Economist (for PhDs and double master's degree holders)
- CAPA: Certified Asset Protection Analyst

EDUCATION: BUILDING KNOWLEDGE, SKILLS, AND ABILITIES IN FRAUD EXAMINATION AND FINANCIAL FORENSICS

The progression of knowledge, skills, and abilities for fraud and forensic accounting for entry-level professionals is presented in Figure 2-2. This section and Figure 2-2 were developed with the extensive use of the DOJ's National Institute of Justice model curriculum project "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students" (available at www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf). This project was also highlighted in the November 2008 volume of *Issues in Accounting Education*.

As noted above, fraud examination and financial forensics embraces many more disciplines than accounting. Those disciplines and professionals include the law, psychology, sociology, criminology, intelligence, information systems, computer forensics, and the greater forensic science fields. One of the

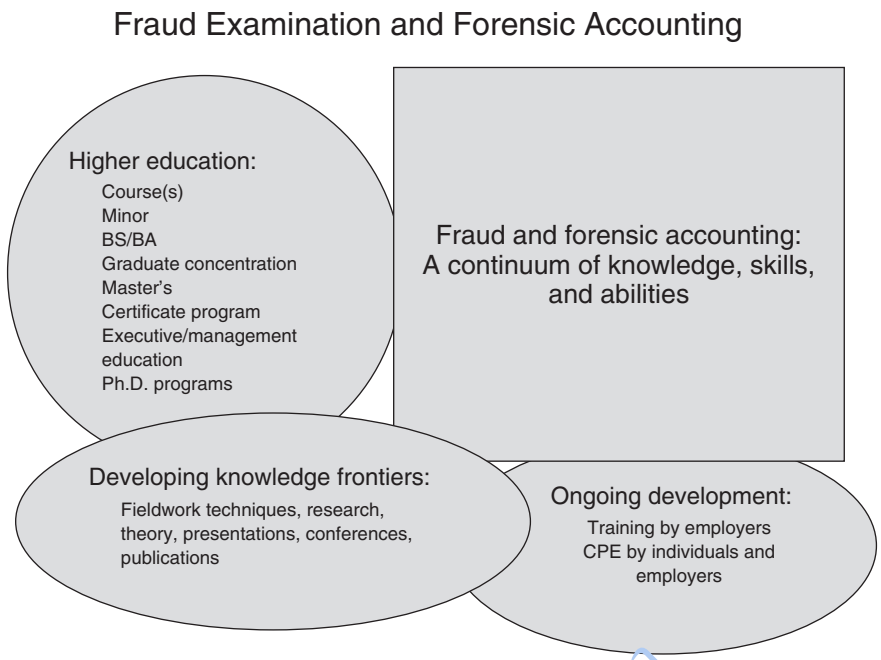


FIGURE 2-2 Fraud Examination and Forensic Accounting: A Continuum of Knowledge, Skills, and Abilities

challenges for individuals with these backgrounds is that most fraud and financial forensics engagements require at least some knowledge of accounting, finance, and economics because of the nature of the work. Thus, the first two columns in Figure 2-2 address prerequisite accounting, auditing, and business law knowledge that is considered necessary for the fraud and financial forensics curriculum. Students with an accounting degree will have met these prerequisites as part of their degree requirements. Students who do not have an accounting degree will need to obtain the prerequisite knowledge and skills before embarking on the fraud examination and financial forensics curriculum. That prerequisite knowledge, skills, and abilities can be developed through experience, and many educational programs recognize past professional accomplishments.

Figure 2-2 depicts the continuum of knowledge development, transfer (education), and use in practice.

Prerequisite Knowledge and Skills

The knowledge and skills students should obtain when they study fraud and financial forensics include the following:[6]

Basic Accounting Concepts

- Key concepts of accounting such as the definitions of assets, liabilities, stockholders' equity, revenue and expenses, revenue recognition, expense measurement, reliability, objectivity, verifiability, materiality, accruals, deferrals, etc.
- Basic financial statement presentation and appropriate disclosure
- The effects of debits and credits on account balances. This understanding is essential in identifying fraud schemes and financial statement manipulation. Students need to be able to analyze accounts (i.e., recognize a normal balance for each type of account and ascertain how a given transaction would affect each account balance) and determine whether each component has been examined directly or indirectly for under- and overstatement
- Account balance analysis for both over- and understatement
- Basic ratio analysis—students need to be able to calculate ratios and interpret the results, such as identifying trends across time and unusual variances in comparison to key industry ratios and other benchmarks (skills normally covered in entry-level accounting courses)

Basic Auditing Concepts

- The basic elements of auditing, including professional skepticism in evaluating statements or representations made

- Different types and quality of audit evidentiary matter and how to evaluate types of evidence (definitive, circumstantial, direct, corroborative, and conflicting)
- Relevant current accounting and auditing standards and the roles and responsibilities of standard-setting, professional, and regulatory bodies
- Organization and development of working papers

Transaction Processing Cycles and Control Environment

- Internal control concepts and an ability to recognize potential weaknesses in a company's internal control structure
- Corporate governance and culture (e.g., tone at the top), including ethics and entity-level controls
- Operational processes and transaction flows within an organization, and tracing transactions (cash and noncash) from source documents to initial entry in the accounting system through the various subledgers and ledgers to reported financial statements. The documentation of processes and transaction flows includes both manual activities and those that incorporate automated information systems

Basic Finance and Economics

- The time value of money
- Net present value concept
- Basic working of markets
- An understanding of opportunity costs
- Valuation techniques

Business Law Concepts

- The fundamental legal principles associated with contracts, civil and criminal matters, social goals associated with the legal system, and the role of the justice system
- Securities and other laws that demonstrate how fraud and fraudulent financial reporting violate the law and how the regulatory, professional, civil, and law enforcement systems operate to prevent, detect, and deter violations
- Ethical duties and legal responsibilities associated with confidentiality

General Business Communications Skills and Business Ethics

- Communications: The second column in Figure 2-2 identifies two courses that are often included as business core or business electives: general communications and business ethics. These courses are not listed as prerequisites, but are highly recommended. Fraud and forensics professionals must have strong written and oral presentation skills. Therefore, a general communications course is extremely beneficial. Students without formal training in oral and written communication may wish to complete such a course before entering a fraud and forensics program
- Ethics: Many states specify a business ethics course as a requirement to sit for the CPA exam. Business majors are likely to have completed a business ethics course as part of their degree requirements. Because ethics is such an important part of the fraud and financial forensics curriculum, students who have the opportunity to take a business ethics course are advised to do so

Basic Computer Skills

- Familiarity with computers, computer operations, and general business software packages such as Word, WordPerfect, Excel, Quattro, and PowerPoint. Enhanced computer skills associated with Visio, IDEA, ACL, and Analysts Notebook's I-2 are also beneficial

Exposure Material/Course

Column 3 of Figure 2-2 shows the exposure to fraud and forensic accounting topics that may be covered in an undergraduate or graduate accounting curriculum. Colleges, universities, and other curriculum providers may use this outline of topical areas as a guide to provide exposure to students by incorporating coverage in current offerings or may add a single course/training module. Some of these topics are covered briefly—for

example, as one chapter in the auditing text or one chapter in the accounting systems text. Because the coverage of these topics in traditional texts is relatively minimal, they should be reinforced and explored in greater depth as part of the fraud and forensic accounting curriculum.

In-Depth Course Material

Columns 4 and 5 of Figure 2-2 provide an overview of the model curriculum areas required for in-depth study. Entry-level fraud and forensic accounting professionals should possess knowledge, skills, and abilities in the following areas:

1. Criminology
2. The legal, regulatory, and professional environment
3. Ethics
4. Fraud and financial forensics:
   - Asset misappropriation, corruption, false representations, and other frauds
   - Financial statement fraud
   - Fraud and forensic accounting in a digital environment
5. Forensic and litigation advisory services

THE ROLE OF RESEARCH IN A PROFESSION

The long-term success of any professional endeavor is derived from three sources: research, practice, and education. Research drives professional innovation. Practitioners in the field implement the products of research (concepts, ideas, theories, and evidence) by applying, testing, and refining theory and research findings in the "real world." Finally, educators create learning frameworks through which students benefit from the combined efforts of practice and research. For fraud examination and forensic accounting to be a viable specialization over the long term, research opportunities and recognition are required to take the profession to the highest levels possible. To date, auditing and behavioral research focusing on fraud and forensic accounting issues has been published in many journals. In other related business disciplines such as economics and finance, forensically grounded research has also been completed and published.

Descriptive research, such as the ACFE's biannual "Report to the Nation," has been funded and completed by such organizations as the ACFE, the AICPA, the large accounting firms, the U.S Department of Treasury, the IRS, the NFF, the Secret Service, the U.S. Postal Service, and others. Topics have typically answered questions such as

- Is the incidence of fraud increasing, or decreasing?
- What types of fraud are being committed?
- What is the cost of fraud?
- How is fraud committed?
- How is fraud detected?
- What are the victim profiles?
- What are the perpetrator profiles?

The Institute for Fraud Prevention (IFP)

The Institute for Fraud Prevention (IFP) is a voluntary association of organizations and researchers dedicated to fraud prevention and orientated toward research and education as a basis for developing antifraud best practices.

As documented by the ACFE's 2008 "Report to the Nation," despite the tremendous impact fraud and corruption have on our economy, there is relatively little research available on the costs of fraud and how and why fraud occurs. Similarly, there exists no repository for gathering, storing, and disseminating fraud-related research findings and descriptive statistics. The primary goal of the IFP is to develop our

understanding of the causes and effects of fraud by serving as a catalyst for the exchange of ideas among top antifraud practitioners, government officials, and academics.

The IFP fulfills its mission in two ways. First, member organizations support research by selecting projects and providing funding, guidance, and data that will help us better understand fraud with a long-term goal of reducing its incidence and effects. Second, the IFP's mission is to provide independent, nonpartisan expertise on antifraud policies, procedures, and best practices. The IFP was founded by the ACFE and the AICPA. A select group of intellectual partners, including the FBI, the GAO, the U.S. Postal Inspectors, the National White-Collar Crime Center (NW3C), and the Council of Better Business Bureaus, have provided guidance to the IFP.

The IFP identifies potentially fruitful research projects in the disciplines of accounting, law, psychology, sociology, criminology, intelligence, information systems, computer forensics, and the greater forensic science fields related to issues specific and unique to white-collar crime, fraud examination, and forensic accounting with a focus on antifraud efforts and best practices.

Where Are the Knowledge Frontiers?

In summer 2008, the IFP solicited white papers in several key areas in an attempt to identify the current body of knowledge:

- Financial Statement Fraud: Joseph Carcello (University of Tennessee) and Dana Hermanson (Kennesaw State University)
- The Legal Environment and White Collar Crime/Forensic Accounting: John Gill (Director of Research at the ACFE)
- White Collar Crime and Psychology, Sociology and Criminology: Sri Ramamoorti (Grant Thornton), Daven Morrison (board of the Chicago-based Information Integrity Coalition (IIC)), and Joseph Koltar (noted author)
- Fraud and Forensic Accounting in a Digital Environment: Conan Albrecht (Brigham Young University)
- Asset Misappropriation: Ethical and International Perspectives: Chad Albrecht (Utah State University), Mary-Jo Kranacher (Editor-in-Chief, CPA Journal and York College), and Steve Albrecht (Brigham Young University)

Each white paper includes a brief overview of past research (descriptive and investigative) at the beginning of the article and answers the following questions:

- What do we currently know about the topical area?
- What research has been done?
- What are the lessons that we have learned?
- What don't we know, and what are we missing?
- What additional resources are needed to do research on the topical area (additional theory, data, subjects, research methodology, etc.)?

Each white paper also has underpinnings with practice and bridges the gap between the research findings and its implications to practitioners. These papers will help members, intellectual partners, and academics understand the knowledge frontiers as they exist. The IFP Web site, www.theifp.org, includes recent IFP studies and research, best practices, and antifraud resources for practicing professionals.

REVIEW QUESTIONS

2-1 According to this chapter, what employment trends are expected for professionals in the fields of fraud examination and financial forensics? Why?

2-2 What employment opportunities currently exist for fraud examiners and financial forensics specialists?

2-3 What role do fraud examination and financial forensic skills have in the corporate governance area?

2-4 Which professional organizations support fraud examination and financial forensics professionals? What certifications do they offer?

2-5 What international opportunities exist in fraud examination and financial forensics?

2-6 Other than accounting, which disciplines do fraud examination and financial forensics encompass?

2-7 What is the role of research in the fraud examination and financial forensics professions?

ENDNOTES

1. Source unknown.
2. See also Mark Anderson, "Accountants Rock," *Sacramento Business Journal* (July 29, 2005), www.sacramento.bizjournals.com/sacramento/stories/2005/08/01/focus1.html.
   Kate Berry, "Business Booming for Forensic Accountants," *Los Angeles Business Journal* (June 6, 2005), http://www.thefreelibrary.com/Business+booming+for+forensic+accountants.-a0133465662.
   Neil A. Martin, "Super Sleuths," *Barron's Online* (February 28, 2005).
3. Cecily Kellogg, "Accounting CSI: The World of Forensic Accounting," http://ezinearticles.com/?Accounting-CSI—The-World-of-Forensic-Accounting&id=817884.
4. Figure 2-1 was developed as part of the DOJ's National Institute of Justice model curriculum project "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students," www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf.
5. "Managing the Business Risk of Fraud: A Practical Guide," The Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), and Association of Certified Fraud Examiners (ACFE), 2008, http://www.acfe.com/documents/managingbusinessrisk.pdf.
6. University students who develop an early interest in fraud and forensic accounting may also want to take criminology and risk management courses to the extent that such courses are available and fit into their course of study.

SECTION II

CRIMINOLOGY, ETHICS, AND THE LEGAL REGULATORY AND PROFESSIONAL ENVIRONMENTS

CHAPTER 3

WHO COMMITS FRAUD AND WHY: CRIMINOLOGY AND ETHICS

LEARNING OBJECTIVES

After reading this chapter, you should be able to:

- **3-1** Describe occupational fraud and abuse.
- **3-2** Compare and contrast theories of crime causation.
- **3-3** Identify the six situational categories that cause nonshareable problems from Cressey's research.
- **3-4** Discuss the essence of organizational crime.
- **3-5** Give examples of behavioral or other environmental indications of fraud.
- **3-6** Explain the relationship between an employee's position and the level of theft (according to Hollinger and Clark's research).
- **3-7** Analyze the role of corporate governance mechanisms in fraud prevention.
- **3-8** Describe corporate governance breakdowns in the facilitation of historical fraudulent acts.
- **3-9** Identify ethical issues, conflicts of interest, and noncompliance with corporate policies and procedures in the context of a specific case.
- **3-10** Discuss alternative courses of action in a given scenario within the framework of appropriate ethical conduct.

CRITICAL THINKING EXERCISE

The Killer Apartment[1]

Colin McFee had a Manhattan apartment to die for, an enormously spacious duplex that looked down on Park Avenue from the 18th and 19th floors. He also had a fortune worth killing for. So *it wasn't too surprising when the old man was found to be a victim of foul play. The day of the murder began innocently enough. McFee's two nephews and his niece were all visiting him from Duluth, and the old millionaire had been so captivated by the charming trio that he impulsively decided to change his will.*

The generous millionaire spent the morning signing the new document, which left his entire estate divided equally among the three vacationing relatives. McFee's faithful maid witnessed the document, ushered the lawyer out, and, with an uneasy glance at the shiny-eyed heirs, retreated to her room.

Nothing happened until shortly after noon. The maid was in her upper floor bedroom watching TV when she heard McFee's unmistakable voice screaming out in pain. For a few seconds, she was in shock, wondering what her employer's voice was doing on an old Columbo episode. And then she realized it wasn't the TV.

The maid went out into the hall and found Nick, the older nephew, standing at the top of a rarely used back staircase. "It came from downstairs," Nick stammered.

Pushing past Nick, the maid led the way down the narrow stairs. "Mr. McFee!" she shouted, and a moment later caught a spider web across the face. The back staircase went directly down to the east library. The dim, wood-paneled room was empty, except for the corpse on the floor by the bookshelves. Colin McFee, it seemed, had been hacked to death, although there was no weapon in sight.

The three McFee heirs sat with the maid in the center of the lower level, by the main staircase, awaiting the police and rehearsing their stories. "I was in my second floor bedroom," Nick said, "watching an old murder mystery show. When Uncle Colin screamed, I didn't do anything for a minute. Then I went out into the hall. That's where I met up with you." Nick smiled at the maid, his alibi.

"I was upstairs in the west dining room," Nora volunteered, "examining the old dumbwaiter. Even though the scream came from downstairs and on the far side of the apartment, I still heard it. I thought it must be robbers, so, I barricaded the dining room door and didn't come out until I heard you all calling my name."

Astor McFee, the younger nephew, claimed to have been asleep. "I was reading a magazine right here in this chair and I nodded off. The scream woke me. It took a few seconds to realize that something was wrong. When I heard people talking in the library, I went off in that direction. That's when I ran into you," he said, nodding toward Nick and the maid.

When the police arrived, they took everyone's statement, and then went to the main floor kitchen in search of the murder weapon. They found it in a utensil drawer, a huge butcher knife that had been wiped clean of blood, the same blood type as the victim's."This tells us everything we need to know," the homicide chief said with a grin.

Who killed Colin McFee?

This critical thinking exercise emphasizes the importance of drawing a picture. Without visually representing the crime scene, very different conclusions are reached about who committed this crime. Upon drawing out the crime scene, however, and placing the suspects in their various locales, it becomes clear who killed Colin McFee, or at least who was involved.

CRIMINOLOGY

Bethany holds the position of office manager at a small commercial real estate company. Jackson Stetson, the owner, conducts numerous entertainment events each month to interact with and locate new clientele. In addition, Mr. Stetson prides himself on his support of charitable organizations. In his capacity as a leader, organizer, and board member of several high-profile charities, Jackson has additional charity events each month. In her position, Bethany is a trusted assistant to Mr. Stetson, runs many aspects of the company, and organizes and hosts many of the social events for Mr. Stetson. Bethany has been with the company for many years, and has a company credit card to pay for social events and incidentals associated with the events. The company pays the monthly credit card balance, although Bethany is supposed to save receipts and match those receipts to her company credit cards before seeking Mr. Stetson's approval for company payment.

Initially, Bethany lost a few receipts, and Mr. Stetson waived the requirement that she provide all receipts. As the business grew, Bethany's schedule became even crazier, and she had less time for administrative bureaucracy. Mr. Stetson was so happy with her work on his beloved social events that he was willing to overlook her lack of attention to administrative details. The problem was that, over time, Bethany started charging personal expenses on the company-paid credit card. Not only was the company paying Bethany a salary, they paid her grocery bills and household expenses to retailers where she would shop for social event incidentals. Over a twenty-four month-period, Bethany was able to double her $40,000 take-home pay, and the additional income was tax-free!

Criminology is the sociological study of crime and criminals. Understanding the nature, dynamics, and scope of fraud and financial crimes is an important aspect of an entry-level professional's knowledge base. As noted in Chapter 1, fraudsters often look exactly like us, and most are first-time offenders. As such, to understand the causes of white-collar crime our research needs to focus on perpetrators of fraud, not street crime.[2]

Before talking about crime, it is prudent to consider why the vast majority of people do not commit crime. A number of theories have been put forth but essentially, people obey laws for the following reasons:

1. fear of punishment
2. desire for rewards
3. to act in a just and moral manner according to society's standards.

Most civilized societies are dependent upon people doing the right thing. Despite rewards, punishment, and deterrence, the resources required to fully enforce all the laws would be astronomical. Even deterrence is costly to implement and does not guarantee an adequate level of compliance. The bottom line is that a person's normative values of right and wrong dictate their behavior and determine compliance or noncompliance with the law.[3]

Occupational Fraud and Abuse

Occupational fraud and abuse 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."[4] By the breadth of this definition, occupational fraud and abuse involves a wide variety of conduct by executives, employees, managers, and principals of organizations, ranging from sophisticated investment swindles to petty theft. Common violations include asset misappropriation, fraudulent statements, corruption, pilferage, petty theft, false overtime, using company property for personal benefit, fictitious payroll, and sick time abuses.

Four common elements to these schemes were first identified by the Association of Certified Fraud Examiners in its 1996 *Report to the Nation on Occupational Fraud and Abuse* (Section 3, p. 3), which stated: "The key is that the activity (1) is clandestine, (2) violates the employee's fiduciary duties to the organization, (3) is committed for the purpose of direct or indirect financial benefit to the employee, and (4) costs the employing organization assets, revenues, or reserves."

Employee in the context of this definition is any person who receives regular and periodic compensation from an organization for his or her labor. The employee moniker is not restricted to the rank and file, but specifically includes corporate executives, company presidents, top and middle managers, and other workers.

White-Collar Crime

The term *white-collar crime* was a designation coined by Edwin H. Sutherland in 1939, when he provided the following definition: crime in the upper, white-collar class, which is composed of respectable, or at least respected, business and professional men. White-collar crime is often used interchangeably with occupational fraud and economic crime. While white-collar crime is consistent with the notion of trust violator and is typically associated with an abuse of power, one difficulty with relying on white-collar crime as a moniker for financial and economic crimes is that many criminal acts such as murder, drug trafficking, burglary, and theft are motivated by money. Furthermore, the definition, though broad, leaves out the possibility of the perpetrator being an organization where the victim is often the government and society (e.g., tax evasion and fixed contract bidding). Nevertheless, the term *white-collar crime* captures the essence of the type of perpetrator that one finds at the heart of occupational fraud and abuse.

Organizational Crime

Organizational crimes occur when entities, companies, corporations, not-for-profits, nonprofits, and government bodies, otherwise legitimate and law-abiding organizations, are involved in a criminal offense. In addition, individual organizations can be trust violators when the illegal activities of the organization are reviewed and approved by persons with high standing in an organization such as board members, executives, and managers. Federal law allows organizations to be prosecuted in a manner similar to individuals.[5] For example, although the Arthur Andersen conviction was later overturned by the U.S. Supreme Court, the organization was convicted of obstruction of justice, a felony offense that prevented them from auditing public companies. Corporate violations may include administrative breaches, such as noncompliance with agency, regulatory, and court requirements; environmental infringements; fraud and financial crimes, such as bribery and illegal kickbacks; labor abuses; manufacturing infractions related to public safety and health; and unfair trade practices.

Organizational crime is more of a problem internationally and often consists of unfair pricing, unfair business practices, and tax evasion. Organizations are governed by a complex set of interactions among boards of directors, audit committees, executives, and managers. In addition, the actions of external stakeholders such as auditors and regulators also impact the governance of organizations. As such, it is often difficult to distinguish between those individuals with responsibility for compliance with particular laws and regulations, and those infractions committed by the organization. In addition, when considerable financial harm has been inflicted on society as a result of corporate wrongdoing, the organization is often an attractive target because of its deep pockets with which to pay fines and restitution.

It is more common for corporations to become embroiled in legal battles that wind up in civil court. Such litigation runs the gamut of forensic litigation advisory services, including damage claims made by plaintiffs and defendants; workplace issues such as lost wages, disability, and wrongful death; assets and business valuations; costs and lost profits associated with construction delays or business interruptions; insurance claims; fraud; anti-trust actions, intellectual property infringement; environmental issues; tax claims; or other disputes. If you open any 10-K or annual report, you will likely find mention of a pending lawsuit in the notes to the financial statements. Furthermore, these filings include only those lawsuits deemed to be "material" as defined by accounting standards. Most corporations are involved in numerous lawsuits considered to be below the auditor's materiality threshold.

Organized Crime

These crimes are often complex, involving many individuals, organizations, and shell companies, and often cross jurisdictional borders. In this context, fraud examiners and financial forensic professionals often think of terrorist financing, the mob, and drug trafficking. Some of the crimes typically associated with organized crime include money laundering, mail and wire fraud, conspiracy, and racketeering. Money laundering addresses the means by which organized criminals take money from illegal sources and process it so that it looks like it came from legitimate business sources. Conspiracy is a means of prosecuting the individuals involved in the illegal organized activity. RICO (Racketeering Influence and Corrupt Organizations Act) addresses organizations involved in criminal activity. For example, portions of the RICO Act:

- outlaw investing illegal funds in another business
- outlaw acquisition of a business through illegal acts
- outlaw the conduct of business affairs with funds derived from illegal acts.

Torts, Breach of Duty, and Civil Litigation

Black's Law Dictionary defines "tort" as "a private or civil wrong or injury, other than breach of contract, for which the law will provide a remedy in the form of an action for damages." When a tort is committed, the party who was injured is entitled to collect compensation for damages from the wrongdoer for that private wrong.[6] The tort of contract interference or tortuous interference with contracts occurs when parties are not allowed the freedom to contract without interference from third parties. While the elements of tortuous interference are complex, a basic definition is that the law affords a remedy when someone intentionally persuades another to break a contract already in existence with a third party.[7]

Another tort—negligence—applies when the conduct of one party did not live up to minimal standards of care. Each person has a duty to act in a reasonable and prudent manner. When individuals or entities fail to live up to this standard, they are considered "negligent." The legal standard for negligence has five elements:[8]

a. Duty—a duty to act exists between the parties

b. Breach—a determination that the defendant failed to use ordinary or reasonable care in the exercise of that duty

c. Cause In Fact—an actual connection between the defendant's breach of duty and the plaintiff's harm can be established

d. Proximate Cause—the defendant must have been the proximate cause or contributed to the injury to the plaintiff

e. Damages—the plaintiff must establish that damages resulted from the defendant's breach of duty.

In order to win an award for damages, the injured party must generally prove two points:

1. liability—that the other party was liable for all or part of the damages claimed, and

2. damages—that the injured party suffered damages as the results of the actions or lack of actions of the offending party.

Furthermore, the amount of damages must be proven with a reasonable degree of certainty as to the amount claimed, and that the defendant could reasonably foresee the likelihood of damages if they failed to meet their obligations. Thus, generally speaking, the threshold for suing another person in civil court for a tort, breach of contract, or negligence is fairly low. While judges have the ability to issue summary

judgments and dismiss frivolous lawsuits, most judges are more apt to let the parties negotiate a settlement or let the jury decide the case based on the merits of the arguments put forth by the plaintiff and defense.

RESEARCH IN OCCUPATIONAL FRAUD AND ABUSE

Edwin H. Sutherland

Considering its enormous impact, 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 (1883–1950), a criminologist at Indiana University. Sutherland was particularly interested in fraud committed by the elite upper-world business executive, either against shareholders or the public. As Gilbert Geis noted, 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."[9]

For the uninitiated, Sutherland is to the world of white-collar criminality what Freud is to psychology. Indeed, it was Sutherland who coined the term *white-collar crime* in 1939. He intended the definition to mean criminal acts of corporations and individuals acting in their corporate capacity. Since that time, however, the term has come to mean almost any financial or economic crime, from the mailroom to the boardroom.

Many criminologists believe that Sutherland's most important contribution to criminal literature was elsewhere. Later in his career, he developed the theory of differential association, which is now the most widely accepted theory of criminal behavior in the 20th century. Until Sutherland's landmark work in the 1930s, most criminologists and sociologists held the view that crime was genetically based, that criminals beget criminal offspring.

While this argument may seem naive today, it was based largely on the observation of non–white-collar offenders—the murderers, rapists, sadists, and hooligans who plagued society. Numerous subsequent studies have indeed established a genetic base for "street" crime, which must be tempered by environmental considerations. (For a thorough explanation of the genetic base for criminality, see *Crime and Punishment* by Wilson and Herrnstein.) Sutherland was able to explain crime's environmental considerations through the theory of differential association. The theory's basic tenet is that crime is learned, much like we learn math, English, or guitar playing.[10]

Sutherland believed this learning of criminal behavior occurred 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 involved two specific areas: the techniques to commit the crime; and the attitudes, drives, rationalizations, and motives of the criminal mind. You 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

One of Sutherland's brightest students at Indiana University during the 1940s was Donald R. Cressey (1919–1987). Although 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 concentrate on embezzlers. To serve as a basis for his research, Cressey interviewed about 200 incarcerated inmates at prisons in the Midwest.

Cressey's Hypothesis Embezzlers, whom he called "trust violators," intrigued Cressey. 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 as the classic model for the occupational offender. His research was published in *Other People's Money: A Study in the Social Psychology of Embezzlement*.

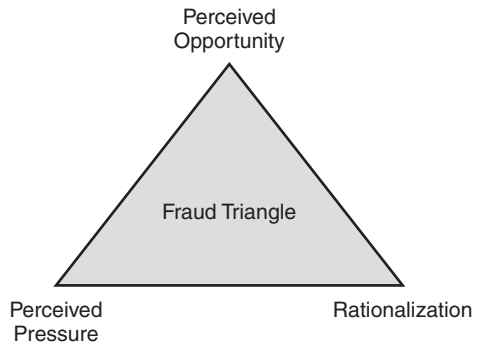


FIGURE 3-1 Fraud Triangle

Cressey's final hypothesis read as follows:

> *Trusted persons become trust violators when they conceive of themselves as having a financial problem that is nonshareable, 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.*[11]

Over the years, the hypothesis became known as the *fraud triangle* (Figure 3-1). One leg of the triangle represents a *perceived pressure (or nonshareable financial need)*. The second leg represents *perceived opportunity*, and the final leg denotes *rationalization*.

Nonshareable Financial Pressures The role of perceived nonshareable financial pressures is important. Cressey said, 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."[12] "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."[13]

What is considered nonshareable is, of course, wholly in the eyes of the potential occupational offender, as Cressey noted:

> *Thus a man could lose considerable money at the racetrack daily, but the loss, even if it construed a problem for the individual, might not constitute a nonshareable problem for him. Another man might define the problem as one that must be kept secret and private. 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 nonshareable.*[14]

In addition to being nonshareable, the problem that drives the fraudster is described as "financial" because these are the types of 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 noted, 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 her employer for perceived "unfair" treatment uses financial means to solve what is essentially a nonfinancial problem.[15]

Through his research, Cressey also found that the nonshareable 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
- employer-employee relations

All of these situations dealt in some way with status-seeking or status-maintaining activities by the subjects.[16] In other words, the nonshareable 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.

Violations of Ascribed Obligations Violation of ascribed obligations has historically proved to be a strong motivator of financial crimes. Cressy explains in this way:

> *Financial problems incurred through nonfinancial violations of positions of trust often are considered as nonshareable by trusted persons since they represent a threat to the status which holding the position entails. Most individuals in positions of financial trust, and most employers of such individuals, consider that incumbency in such a position necessarily implies that, in addition to being honest, they should behave in certain ways and should refrain from participation in some other kinds of behavior.*[17]

In other words, the mere fact that a person has a trusted position carries with it the implied duty to act in a manner becoming his status. Persons in trusted positions may feel they are expected to avoid conduct such as gambling, drinking, drug use, or other activities that are considered seamy and undignified.

When these persons then fall into debt or incur large financial obligations as a result of conduct that is "beneath" them, they feel unable to share the problem with their peers because this would require admitting that they have engaged in the dishonorable conduct that lies at the heart of their financial difficulties. Basically, by admitting that they had lost money through some disreputable act, they would be admitting—at least in their own minds—that they are unworthy to hold their trusted positions.

Problems Resulting from Personal Failure Problems resulting from personal failures, Cressey writes, are those that the trusted person feels he caused through bad judgment and therefore feels personally responsible for. Cressey cites one case in which an attorney lost his life's savings in a secret business venture. The business had been set up to compete with some of the attorney's clients, and though he thought his clients probably would have offered him help if they had known what dire straits he was in, he could not bring himself to tell them that he had secretly tried to compete with them. He also was unable to tell his wife that he'd squandered their savings. Instead, he sought to alleviate the problem by embezzling funds to cover his losses.[18]

> *While some pressing financial problems may be considered as having resulted from "economic conditions," "fate," or some other impersonal force, others are considered to have been created by the misguided or poorly planned activities of the individual trusted person. Because he fears a loss of status, the individual is afraid to admit to anyone who could alleviate the situation the fact that he has a problem which is a consequence of his "own bad judgment" or "own fault" or "own stupidity."*[19] *In short*, pride goeth before the fall.[20] *If the potential offender has a choice between covering his poor investment choices through a violation of trust and admitting that he is an unsophisticated investor, it is easy to see how some prideful people's judgment could be clouded*.

Business Reversals Business reversals were the third type of situation Cressey identified as leading to the perception of nonshareable financial problems. This category differs from the class of "personal failures" described above because here the trust violators tend to see their problems as arising from conditions beyond their control: inflation, high interest rates, economic downturns, etc. In other words, these problems are not caused by the subject's own failings, but instead by outside forces.

Cressey quoted the remarks of one businessman who borrowed money from a bank using fictitious collateral:

> ***Case 36***. *There are very few people who are able to walk away from a failing business. When the bridge is falling, almost everyone will run for a piece of timber. In business there is this eternal optimism that things will get better tomorrow. We get to working on the business, keeping it going, and we get almost mesmerized by it . . . Most of us don't know when to quit, when to say, 'This one has me licked. Here's one for the opposition.'*[21]

It is interesting to note that even in situations where the problem is perceived to be out of the trusted person's control, the issue of status still plays a big role in that person's decision to keep the problem a secret. The subject of Case 36 continued, "If I'd have walked away and let them all say, 'Well, he wasn't a success as a manager, he was a failure,' and took a job as a bookkeeper, or gone on the farm, I would have been all right. But I didn't want to do that."[22] The desire to maintain the appearance of success was a common theme in the cases involving business reversals.

Physical Isolation The fourth category Cressey identified consisted of problems resulting from physical isolation. In these situations, the trusted person simply has no one to turn to. It's not that he is afraid to share his problem; it's that he has no one to share the problem with. He is in a situation where he does not have access to trusted friends or associates who would otherwise be able to help him. Cressey cited the subject of Case 106 in his study, a man who found himself in financial trouble after his wife had died. In her absence, he had no one to go to for help and he wound up trying to solve his problem through an embezzlement scheme.[23]

Status Gaining The fifth category involves problems relating to status gaining, which is a sort of extreme example of "keeping up with the Joneses" syndrome. In the categories that have been discussed previously, the offenders were generally concerned with maintaining their status (i.e., not admitting to failure, keeping up appearance of trustworthiness), but here the offenders are motivated by a desire to *improve* their status. The motive for this type of conduct is often referred to as "living beyond one's means" or "lavish spending," but Cressey felt that these explanations did not get to the heart of the matter. The question was, what made the desire to improve one's status nonshareable? He noted,

> *The structuring of status ambitions as being nonshareable is not uncommon in our culture, and it again must be emphasized that the structuring of a situation as nonshareable is not alone the cause of trust violation. More specifically, in this type of case a problem appears when the individual realizes that he does not have the financial means necessary for continued association with persons on a desired status level, and this problem becomes nonshareable when he feels that he can neither renounce his aspirations for membership in the desired group nor obtain prestige symbols necessary to such membership.*[24]

In other words, it is not the desire for a better lifestyle that creates the nonshareable problem (we all want a better lifestyle), rather it is the inability to obtain the finer things through legitimate means, and at the same time, an unwillingness to settle for a lower status that creates the motivation for trust violation.

Employer-Employee Relations Finally, Cressey described problems resulting from employer-employee relationships. The most common, he stated, was an employed person who resents his status within the organization in which he is trusted and at the same time feels he has no choice but to continue working for the organization. The resentment can come from perceived economic inequities, such as pay, or from the feeling of being overworked or underappreciated. Cressey said this problem becomes nonshareable when the individual believes that making suggestions to alleviate his perceived maltreatment will possibly threaten his status in the organization.[25] There is also a strong motivator for the perceived employee to want to "get even" when he feels ill-treated.

The Importance of Solving the Problem in Secret Given that Cressey's study was done in the early 1950s, the workforce was obviously different from today. But the employee faced with an immediate, nonshareable financial need hasn't changed much over the years. That employee is still placed in the position of having to find a way to relieve the pressure that bears down upon him. Simply stealing money, however, is not enough; Cressey found it was crucial that the employee be able to resolve the financial problem in *secret*. As we have seen, the nonshareable 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 the financial problems they encountered. 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 the problems existed in the first place.

The interesting thing to note is that it is not the embezzlement itself that creates the need for secrecy in the perpetrator's mind; it is the circumstances that led to the embezzlement (e.g., a violation of ascribed obligation, a business reversal, etc.). Cressey pointed out,

> *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 nonshareable 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*[26] (emphasis added).

Perceived Opportunity According to the fraud triangle model, the presence of a nonshareable 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 nonshareable 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.

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 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.[27] 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."[28]

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 nonshareable 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 nonshareable problem"[29]

Rationalizations The third and final factor in the fraud triangle is the *rationalization*. Cressey pointed out that the rationalization is not an *ex post facto* means of justifying a theft that has already occurred. Significantly, the 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 him and maintain his concept of himself as a trusted person.[30]

After the criminal act has taken place, the rationalization will often be abandoned. This reflects 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, she will usually continue to steal past the point where there is any realistic possibility of repaying the stolen funds.

Cressey found that the embezzlers he studied generally rationalized their crimes by viewing them: (1) as essentially noncriminal, (2) as justified, or (3) as part of a general irresponsibility for which they were not completely accountable.[31] 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 persons who were in business for themselves and who converted deposits that had been entrusted to them.[32] 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 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.[33] Also, the independent businessmen almost universally felt their illegal actions were predicated by an "unusual situation," which Cressey perceived to be in reality a nonshareable 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.[34] Similar to independent businessmen, the long-term violators also generally preferred the "borrowing" rationalization. Other rationalizations of long-term violators were noted, 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; or (3) their employers were dishonest towards 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 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 position by the exposure of their nonshareable *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 criminals until he comes to look upon himself as a criminal."[35]

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.[36]

Without the rationalization that they are 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 attitudes of the (law-abiding) social group that they identified with before the thefts began; or (2) they can adopt the attitudes of the new category of persons (criminals) with whom they now identify.[37] 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."[38] 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."[39]

Absconders The third group of offenders Cressey discussed was *absconders*—people who take the money and run. Cressey found that the nonshareable 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."[40] Cressey also found that the absconders tended to have lower occupational and socioeconomic 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 nonshareable 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.[41] 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 themselves, and a belief that they could not help themselves because they were predisposed to criminal behavior. The latter two rationalizations, which were adopted by absconders in Cressey's study, allowed them to remove almost all personal accountability from their conduct.[42]

In the 1950s, when Cressey gathered this data, 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.[43]

Conjuncture of Events One of the most fundamental observations of the Cressey study was that it took all three elements—perceived nonshareable financial problem, perceived opportunity, and the ability to rationalize—for the trust violation to occur. If any of the three elements were missing, trust violation did not occur.

[a] trust violation takes place when the position of trust is viewed by the trusted person according to culturally provided knowledge about and rationalizations for using the entrusted funds for solving a nonshareable problem, and that the absence of any of these events will preclude violation. The three events make up the conditions under which trust violation occurs and the term "cause" may be applied to their conjecture 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.[44]

Cressey's Conclusion 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 antifraud professionals believe there is a new breed of occupational offender—those who simply lack a conscience sufficient to overcome temptation. Even Cressey saw the trend later in his life.

After doing this landmark study in embezzlement, Cressey went on to a distinguished academic career, eventually authoring thirteen books and nearly 300 articles on criminology. He rose to the position of Professor Emeritus in Criminology at the University of California, Santa Barbara.

Joe Wells Remembers Donald Cressey

It was my honor to know Cressey personally. Indeed, he and I collaborated extensively before he died in 1987, and his influence on my own antifraud theories has been significant. Our families are acquainted; we stayed in each other's homes; we traveled together; he was my friend. In a way, we made the odd couple—he, the academic, and me, the businessman; he, the theoretical, and me, the practical.

I met him as the result of an assignment in about 1983. A Fortune 500 company hired me on an investigative and consulting matter. They had a rather messy case of a high-level vice president who was put in charge of a large construction project for a new company plant. The $75 million budget for which he was responsible proved to be too much of a temptation. Construction companies wined and dined the vice president, eventually providing him with tempting and illegal bait: drugs and women. He bit.

From there, the vice president succumbed to full kickbacks. By the time the dust settled, he had secretly pocketed about $3.5 million. After completing the internal investigation for the company, assembling the documentation and interviews, I worked with prosecutors at the company's request to put the perpetrator in prison. Then the company came to me with a very simple question:"Why did he do it?" As a former FBI Agent with hundreds of fraud cases under my belt, I must admit I had not thought much about the motives of occupational offenders. To me, they committed these crimes because they were crooks. But the company—certainly progressive on the antifraud front at the time—wanted me to invest the resources to find out why and how employees go bad, so they could possibly do something to prevent it. This quest took me to the vast libraries of The University of Texas at Austin, which led me to Cressey's early research. After reading his book, I realized that Cressey had described the embezzlers I had encountered to a "T." I wanted to meet him.

Finding Cressey was easy enough. I made two phone calls and found that he was still alive, well, and teaching in Santa Barbara. He was in the telephone book, and I called him. Immediately, he agreed to meet me the next time I came to California. That began what became a very close relationship between us that lasted until his untimely death in 1987. It was he who recognized the real value of combining the theorist with the practitioner. Cressey used to proclaim that he learned as much from me as I from him. But then, in addition to his brilliance, he was one of the most gracious people I have ever met. Although we were only together professionally for four years, we covered a lot of ground. Cressey was convinced there was a need for an organization devoted exclusively to fraud detection and deterrence. The Association of Certified Fraud Examiners, started about a year after his death, is in existence in large measure because of Cressey's vision. Moreover, although Cressey didn't know it at the time, he created the concept of what eventually became the certified fraud examiner. Cressey theorized that it was time for

a new type of corporate cop—one trained in detecting and deterring the crime of fraud. Cressey pointed out that the traditional policeman was ill equipped to deal with sophisticated financial crimes, as were traditional accountants. A hybrid professional was needed; someone trained not only in accounting, but also in investigation methods, someone as comfortable interviewing a suspect as reading a balance sheet. Thus, the certified fraud examiner was born.

Dr. Steve Albrecht

Another pioneer researcher in occupational fraud and abuse—and another person instrumental in the creation of the certified fraud examiner program—was Dr. Steve Albrecht of Brigham Young University. Unlike Cressey, Albrecht was educated as an accountant. Albrecht agreed with Cressey's vision—traditional accountants, he said, were poorly equipped to deal with complex financial crimes.

Albrecht's research contributions in fraud have been enormous. He and two of his colleagues, Keith Howe and Marshall 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*.[45] 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 and his colleagues believed that, taken as a group, occupational fraud perpetrators are hard to profile and that fraud is difficult to predict. His research included an examination of comprehensive data sources to assemble a complete list of pressure, opportunity, and integrity variables, resulting in a list of fifty 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 the potential employee's background.[46] Table 3-1 shows the complete list of occupational fraud red flags that Albrecht identified.[47]

The researchers gave participants both sets of twenty-five 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:[48]

1. Living beyond their means
2. An overwhelming desire for personal gain
3. High personal debt
4. A close association with customers
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

As you can see from the list, these motivators are very similar to the nonshareable financial problems Cressey identified.

The ten most highly ranked factors from the list dealing with organizational environment were:[49]

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

TABLE 3-1 Occupational Fraud Red Flags

Personal Characteristics	Organizational Environment
1. Unusually high personal debts.	**26.** A department that lacks competent personnel.
2. Severe personal financial losses.	**27.** A department that does not enforce clear lines of authority and responsibility.
3. Living beyond one's means.	**28.** A department that does not enforce proper procedures for authorization of transactions.
4. Extensive involvement in speculative investments.	**29.** A department that lacks adequate documents and records.
5. Excessive gambling habits.	**30.** A department that is not frequently reviewed by internal auditors.
6. Alcohol problems.	**31.** Lack of independent checks (other than internal auditor).
7. Drug problems.	**32.** No separation of custody of assets from the accounting for those assets.
8. Undue family or peer pressure to succeed.	**33.** No separation of authorization of transactions from the custody of related assets.
9. Feeling of being underpaid.	**34.** No separation of duties between accounting functions.
10. Dissatisfaction or frustration with job.	**35.** Inadequate physical security in the employee's department such as locks, safes, fences, gates, guards, etc.
11. Feeling of insufficient recognition for job performance.	**36.** No explicit and uniform personnel policies.
12. Continuous threats to quit.	**37.** Failure to maintain accurate personnel records of disciplinary actions.
13. Overwhelming desire for personal gain.	**38.** Inadequate disclosures of personal investments and incomes.
14. Belief that job is in jeopardy.	**39.** Operating on a crisis basis.
15. Close associations with suppliers.	**40.** Inadequate attention to details.
16. Close associations with customers.	**41.** Not operating under a budget.
17. Poor credit rating.	**42.** Lack of budget review or justification.
18. Consistent rationalization of poor performance.	**43.** Placing too much trust in key employees.
19. Wheeler-dealer attitude.	**44.** Unrealistic productivity expectations.
20. Lack of personal stability such as frequent job changes, changes in residence, etc.	**45.** Pay levels not commensurate with the level of responsibility assigned.
21. Intellectual challenge to ''beat the system.''	**46.** Inadequate staffing.
22. Unreliable communications and reports.	**47.** Failure to discipline violators of company policy.
23. Criminal record.	**48.** Not adequately informing employees about rules of discipline or codes of conduct within the firm.
24. Defendant in a civil suit (other than divorce).	**49.** Not requiring employees to complete conflict-of-interest questionnaires.
25. Not taking vacations of more than two or three days.	**50.** Not adequately checking background before employment.

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

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 (nonshareable 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.*[50]

The Fraud Scale (Figure 3-2) To illustrate the concept, Albrecht developed the "Fraud Scale," which included the components of: *situational pressures, perceived opportunities*, and *personal integrity*.[51] 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.[52]

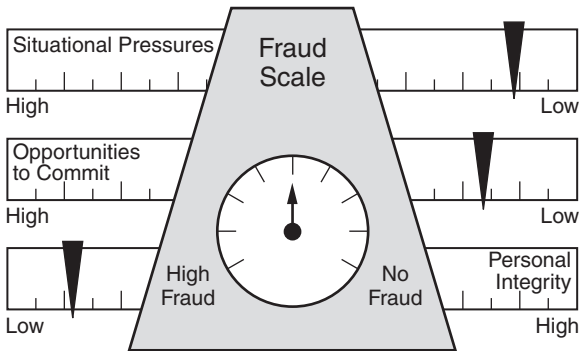


FIGURE 3-2 The Fraud Scale

Albrecht described situational pressures as "the immediate problems individuals experience within their environments, the most overwhelming of which are probably high personal debts or financial losses."[53] 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."[54]

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, recreation property, and expensive vacations, support extramarital relationships, and make speculative investments. Those committing small frauds did not.[55]

There were other observations: 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 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 take 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.[56]

Richard C. Hollinger and John P. Clark

In 1983, Richard C. Hollinger of Purdue University and John P. Clark of the University of Minnesota published federally funded research involving surveys of nearly 10,000 American workers. In their book, *Theft by Employees*, the two researchers reached a different conclusion than Cressey. They found that employees steal primarily as a result of workplace conditions. They also concluded that the true costs of employee theft are vastly understated: "In sum, when we take into consideration the incalculable social costs . . . the grand total paid for theft in the workplace is no doubt grossly underestimated by the available financial estimates."[57]

Hypotheses of Employee Theft In reviewing the literature on employee theft, Hollinger and Clark noted that experts had developed five separate but interrelated sets of hypotheses to explain employee theft. The first was that external economic pressures, such as the "nonshareable financial problem" that Cressey described, motivated theft. The second hypothesis was that contemporary employees, specifically young ones, are not as hardworking and honest as those in past generations. The third theory, advocated primarily by those with years of experience in the security and investigative industry, was that every employee could be tempted to steal from his employer. The theory basically assumes that people are greedy and dishonest by nature. The fourth theory was that job dissatisfaction is the primary cause of employee theft, and the fifth was that theft occurs because of the broadly shared formal and informal structure of organizations. That is, over time, the group norms—good or bad—become the standard of conduct. The sum of their research led Hollinger and Clark to conclude that the fourth hypothesis was correct, that employee deviance is primarily caused by job dissatisfaction.

Employee Deviance Employee theft is at one extreme of employee deviance, which can be defined as conduct detrimental to the organization and to the employee. At the other extreme is counterproductive employee behavior such as goldbricking and abuse of sick leave. Hollinger and Clark defined two basic categories of employee deviant behavior: (1) acts by employees against property, and (2) violations of the norms regulating acceptable levels of production. The former includes misuse and theft of company property such as cash or inventory. The latter involves acts of employee deviance that affect productivity.

Hollinger and Clark developed a written questionnaire that was sent to employees in three different sectors: retail, hospital, and manufacturing. The employees were presented with lists of category 1 and category 2 offenses and were asked which offenses they had been involved in, and with what frequency. The researchers eventually received 9,175 valid employee questionnaires, representing about 54 percent of those sampled. Below are the results of the questionnaires. The first table represents category 1 offenses—acts against property.[58] Hollinger and Clark found that approximately one-third of employees in each sector admitted to committing some form of property deviance.

Combined Phase I and Phase II Property-Devlance Items and Percentage of Reported Involvement, by Sector

	Involvement				
Items	Almost daily	About once a week	Four to twelve times a year	One to three times a year	Total
Retail Sector (N = 3, 567)					
Misuse the discount privilege	0.6	2.4	11	14.9	28.9
Take store merchandise	0.2	0.5	1.3	4.6	6.6
Get paid for more hours than were worked	0.2	0.4	1.2	4	5.8
Purposely underring a purchase	0.1	0.3	1.1	1.7	3.2
Borrow or take money from employer without approval	0.1	0.1	0.5	2	2.7
Be reimbursed for more money than spent on business expenses	0.1	0.2	0.5	1.3	2.1
Damage merchandise to buy it on discount	0	0.1	0.2	1	1.3
Total involved in property deviance					35.1
Hospital Sector (N = 4, 111)					
Take hospital supplies (e.g., linens, bandages)	0.2	0.8	8.4	17.9	27.3
Take or use medication intended for patients	0.1	0.3	1.9	5.5	7.8
Get paid for more hours than were worked	0.2	0.5	1.6	3.8	6.1
Take hospital equipment or tools	0.1	0.1	0.4	4.1	4.7
Be reimbursed for more money than spent on business expenses	0.1	0	0.2	0.8	1.1
Total involved in property deviance					33.3
Manufacturing Sector (N = 1, 497)					
Take raw materials used in production	0.1	0.3	3.5	10.4	14.3
Get paid for more hours than were worked	0.2	0.5	2.9	5.6	9.2
Take company tools or equipment	0	0.1	1.1	7.5	8.7
Be reimbursed for more money than spent on business expenses	0.1	0.6	1.4	5.6	7.7
Take finished products	0	0	0.4	2.7	3.1
Take precious metals (e.g., platinum, gold)	0.1	0.1	0.5	1.1	1.8
Total involved in property deviance					28.4

Adapted from Richard C. Hollinger, John P. Clark, *Theft by Employees*. Lexington: Lexington Books, 1983, p. 42.

Following is a summary of the Hollinger and Clark research with respect to production deviance. Not surprisingly, they found that this form of employee misconduct was two to three times more common than property violations.[59]

Combined Phase I and Phase II Production-Deviance Items and Percentage of Reported Involvement, by Sector

	Involvement				
Items	Almost daily	About once a week	Four to twelve times a a year	One to three times a year	Total
Retail Sector (N = 3, 567)					
Take a long lunch or break without approval	6.9	13.3	15.5	20.3	56
Come to work late or leave early	0.9	3.4	10.8	17.2	32.3
Use sick leave when not sick	0.1	0.1	3.5	13.4	17.1
Do slow or sloppy work	0.3	1.5	4.1	9.8	15.7
Work under the influence of alcohol or drugs	0.5	0.8	1.6	4.6	7.5
Total involved in production deviance					65.4
Hospital Sector (N = 4, 111)					
Take a long lunch or break without approval	8.5	13.5	17.4	17.8	57.2
Come to work late or leave early	1	3.5	9.6	14.9	29
Use sick leave when not sick	0	0.2	5.7	26.9	32.8
Do slow or sloppy work	0.2	0.8	4.1	5.9	11
Work under the influence of alcohol or drugs	0.1	0.3	0.6	2.2	3.2
Total involved in production deviance					69.2
Manufacturing Sector (N = 1, 497)					
Take a long lunch or break without approval	18	23.5	22	8.5	72
Come to work late or leave early	1.9	9	19.4	13.8	44.1
Use sick leave when not sick	0	0.2	9.6	28.6	38.4
Do slow or sloppy work	0.5	1.3	5.7	5	12.5
Work under the influence of alcohol or drugs	1.1	1.3	3.1	7.3	12.8
Total involved in production deviance					82.2

Adapted from Richard C. Hollinger, John P. Clark, *Theft by Employees.* Lexington: Lexington Books, 1983, p. 45.

Income and Theft In order to empirically test whether economics had an effect on the level of theft, the researchers sorted their data by household income under the theory that lower levels of income might produce higher levels of theft. However, they were unable to confirm such a statistical relationship. This would tend to indicate—at least in this study—that absolute income is not a predictor of employee theft.

Despite this finding, Hollinger and Clark were able to identify a statistical relationship between employees' *concern* over their financial situation and the level of theft. They presented the employees with a list of eight major concerns, ranging from personal health to education issues to financial problems. They noted the following:

> *Being concerned about finances and being under financial pressure are not necessarily the same. However, if a respondent considered his or her finances as one of the most important issues, that concern could be partially due to "nonshareable (sic) economic problems," or it could also be that current realities are not matching one's financial aspirations regardless of the income presently being realized.*[60]

The researchers concluded "in each industry, the results are significant, with higher theft individuals more likely to be concerned about their finances, particularly those who ranked finances as the first or second most important issue."[61]

Age and Theft Hollinger and Clark found in their research a direct correlation between age and the level of theft. "Few other variables . . . have exhibited such a strong relationship to theft as the age of the employee."[62] The reason, they concluded, was that the younger employee generally has less tenure with his organization and therefore has a lower level of commitment to it than the typical older employee. In addition, there is a long history of connection between youth and many forms of crime. Sociologists have suggested that the central process of control is determined by a person's "commitment to conformity." Under this model—assuming employees are all subject to the same deviant motives and opportunities—the probability of deviant involvement depends on the stakes that one has in conformity. Since younger

employees tend to be less committed to the idea of conforming to established social rules and structures, it follows that they would be more likely to engage in illegal conduct that runs contrary to organizational and societal expectations.

The researchers suggested that the policy implications from the commitment to conformity theory are that rather than subjecting employees to draconian security measures,

> *companies should afford younger workers many of the same rights, fringes, and privileges of the tenured, older employees. In fact, by signaling to the younger employee that he or she is temporary or expendable, the organization inadvertently may be encouraging its own victimization by the very group of employees that is already least committed to the expressed goals and objectives of the owners and managers.*[63]

Although this may indeed affect the level of employee dissatisfaction, its policy implications may not be practical for non–fraud-related reasons.

Position and Theft Hollinger and Clark were able to confirm a direct relationship between an employee's position and the level of the theft, with thefts being highest in jobs with greater access to the things of value in the organization. Although they found obvious connections between opportunity and theft (for example, retail cashiers with daily access to cash had the highest incidence), the researchers believed opportunity to be "... only a secondary factor that constrains the manner in which the deviance is manifested."[64] Their research indicated that job satisfaction was the primary motivator of employee theft; the employee's position only affects the method and amount of the theft *after* the decision to steal has already been made.

Job Satisfaction and Deviance The research of Hollinger and Clark strongly suggests that employees who are dissatisfied with their jobs—across all age groups, but especially younger workers—are the most likely to seek redress through counterproductive or illegal behavior in order to right the perceived inequity. Other writers, notably anthropologist Gerald Mars and researcher David Altheide, have commented on this connection. Mars observed that among both hotel dining room employees and dock workers it was believed that pilferage was not theft, but was "seen as a morally justified addition to wages; indeed, as an entitlement due from exploiting employers."[65] Altheide also documented that theft is often perceived by employees as a "way of getting back at the boss or supervisor."[66] Jason Ditton documented a pattern in U.S. industries called "wages in kind," in which employees "situated in structurally disadvantaged parts [of the organization] receive large segments of their wages invisibly."[67]

Organizational Controls and Deviance Hollinger and Clark were unable to document a strong relationship between control and deviance in their research. They examined five different control mechanisms: company policy, selection of personnel, inventory control, security, and punishment.

Company policy can be an effective control. Hollinger and Clark pointed out that companies with a strong policy against absenteeism have less of a problem with it. As a result, they would expect policies governing employee theft to have the same impact. Similarly, they believed employee education as an organizational policy has a deterrent effect. Hiring persons who will conform to organizational expectations exerts control through selection of personnel. Inventory control is required not only for theft, but for procedures to detect errors, avoid waste, and ensure a proper amount of inventory is maintained. Security controls involve proactive and reactive measures, surveillance, internal investigations, and others. Control through punishment is designed to deter the specific individual, plus those who might be tempted to act illegally.

Hollinger and Clark interviewed numerous employees in an attempt to determine their attitudes toward control. With respect to policy, they concluded, "the issue of theft by employees is a sensitive one in organizations and must be handled with some discretion. A concern for theft must be expressed without creating an atmosphere of distrust and paranoia. If an organization places too much stress on the topic, honest employees may feel unfairly suspected, resulting in lowered morale and higher turnover."[68]

Employees in the study also perceived, in general, that computerized inventory records added security and made theft more difficult. With respect to security control, the researchers discovered that the employees regarded the purpose of a security division as taking care of outside—rather than inside—security. Few of the employees were aware that security departments investigate employee theft, and most such departments had a poor image among the workers. With respect to punishment, the employees interviewed felt theft would result in job termination in a worst-case scenario. They perceived that minor thefts would be handled by reprimands only.

Hollinger and Clark concluded that formal organizational controls provide both good and bad news. "The good news is that employee theft does seem to be susceptible to control efforts . . . . Our data also indicate, however, that the impact of organizational controls is neither uniform nor very strong. In sum, formal organizational controls do negatively influence theft prevalence, but these effects must be understood in combination with the other factors influencing this phenomenon."[69]

Employee Perception of Control The researchers also examined the perception—not necessarily the reality—of employees believing they would be caught if they committed theft. "We find that perceived certainty of detection is inversely related to employee theft for respondents in all three industry sectors—that is, the stronger the perception that theft would be detected, the less the likelihood that the employee would engage in deviant behavior."[70]

This finding is significant and consistent with other research. It suggests that increasing the perception of detection may be the best way to deter employee theft while increasing the sanctions that are imposed on occupational fraudsters will have a limited effect. Recall that under Cressey's model, embezzlers are motivated to commit illegal acts because they face some financial problem that they cannot share with others because it would threaten their status. It follows that the greatest threat to the perpetrator would be that he might be caught in the act of stealing because that would bring his nonshareable problem out into the open. The possibility of sanctions is only a secondary concern. The perpetrator engages in the illegal conduct only because he perceives there is an opportunity to fix his financial problem *without getting caught*. Therefore, if an organization can increase in its employees' minds the perception that illegal acts will be detected, it can significantly deter occupational fraud. Put simply, occupational fraudsters are not deterred by the threat of sanctions because they do not plan on getting caught.

Control in the workplace, according to Hollinger and Clark, consists of both formal and informal social controls. Formal controls can be described as external pressures that are applied through both positive and negative sanctions; informal controls consist of the internalization by the employee of the group norms of the organization. These researchers, along with a host of others, have concluded that—as a general proposition—informal social controls provide the best deterrent. "These data clearly indicate that the loss of respect among one's acquaintances was the single most effective variable in predicting future deviant involvement." Furthermore, "in general, the probability of suffering informal sanction is far more important than fear of formal sanctions in deterring deviant activity."[71] Again, this supports the notion that the greatest deterrent to the fraudster is the idea that he will be caught, not the threat of punishment by his employer.

Other Hollinger and Clark Conclusions Hollinger and Clark reached several other conclusions based on their work. First, they found that "substantially increasing the internal security presence does not seem to be appropriate, given the prevalence of the problem. In fact, doing so may make things worse."[72]

Second, they concluded that the same kinds of employees who engage in other workplace deviance are also principally the ones who engage in employee theft. They found persuasive evidence that slow or sloppy workmanship, sick-leave abuses, long coffee breaks, alcohol and drug use at work, coming in late and/or leaving early were more likely to be present in the employee-thief.

Third, the researchers hypothesized that if efforts are made to reduce employee theft without reducing its underlying causes (e.g., employee dissatisfaction, lack of ethics), the result could create a "hydraulic effect." Therefore, tightening controls over property deviance may create more detrimental acts affecting the productivity of the organization—that is, if we push down employee theft, we may push up goldbricking as a result.

Fourth, they asserted that increased management sensitivity to its employees would reduce all forms of workplace deviance.

Fifth, they concluded special attention should be afforded young employees, as these are the ones statistically the most likely to steal. However, it must be pointed out that although the incidence of theft is higher among younger employees, the losses associated with those thefts are typically lower than losses caused by more senior employees who have greater financial authority.

Hollinger and Clark asserted that management must pay attention to four aspects of policy development: (1) a clear understanding regarding theft behavior, (2) continuous dissemination of positive information reflective of the company's policies, (3) enforcement of sanctions, and (4) publicizing the sanctions.

The researchers summed up their observations by saying,

> *perhaps the most important overall policy implication that can be drawn . . . is that theft and workplace deviance are in large part a reflection of how management at all levels of the organization is perceived by the employee. Specifically, if the employee is permitted to conclude that his or her contribution to the workplace is not appreciated or that the organization does not seem to care about the theft of its property, we expect to find greater involvement. In conclusion, a lowered prevalence of employee theft may be one valuable consequence of a management team that is responsive to the current perceptions and attitudes of its workforce.*[73]

ETHICS[74]

Oreo Linderhoof, Loss Prevention Manager, takes a videotape labeled *Store 522 Backroom Surveillance*, and carefully places the videotape on top of his desk near the guest chairs. Jim Thomas, Store Manager for retail location 522, arrives for his interview with Oreo. When Jim arrives, Oreo escorts Jim to his office and almost immediately is interrupted by a call. He asks Jim to please excuse the interruption and heads out of the office. Oreo returns fifteen minutes later and Jim "spills his guts." He confesses to the theft of inventory, signs a written statement and is taken from headquarters in handcuffs by the local police.

The rest of the story . . .

Oreo knows that Jim Thomas is stealing high value inventory from the store but he doesn't know how. Based on examination of daily inventory counts correlated with scheduling over weeks, Oreo has concluded that Jim is the only person with the opportunity to have committed the theft. Despite surprise inventory counts, store surveillance and other loss prevention techniques, Oreo cannot figure out how Jim is perpetrating the theft. Surveillance suggests that the inventory is not leaving through the front door and that Jim does not have an accomplice. Cash register analysis suggests that Jim is not taking cash through voids and refunds, a method that would also leave the inventory short.

Oreo hatches a scheme to catch Jim . . .

Oreo calls Jim at the store and schedules an interview at corporate headquarters. Store employees being called to corporate headquarters is never a good sign, and Oreo is hoping that this visit will make Jim nervous. In advance, Oreo instructs the receptionist to call him as soon as he and Jim are in his office. After excusing himself, Oreo goes to the break room, gets a cup of coffee, and then visits with several fellow employees. Essentially, he wants Jim to see the videotape labeled *Store 522 Backroom Surveillance*, and as noted above, his scheme works. As soon as Jim sees the videotape, he believes that he has been caught "red-handed." The issue: the videotape was blank; there was no backroom video surveillance. Oreo, being one of the best professionals in his field, caught his man.

Question: Was Oreo's scheme to obtain Jim's confession ethical?

Ethics, trust, and responsibility are at the heart of fraud examination and financial forensics, and the above scenario highlights some of the dilemmas faced by professionals confronting persons perpetrating financial crimes. Ethics is defined as the branch of philosophy dealing with values relating to human conduct, with respect to rightness and wrongness of actions and the goodness and badness of motives and ends.[75] The definition of ethics has certain key elements:

1. Ethics involves questions requiring reflective choice and their consequences to the individual and others (decision problems).
2. Ethics considers the rules and regulations that are in place to guide behavior as well as the consequences for breaking those rules and regulations.
3. Ethics often relies on moral principles to guide choices of right and wrong. (These ethical frameworks are discussed in more detail below).
4. Ethics is concerned with outcomes, the assigned impact associated with making a decision where the impact reflects the underlying values of individuals and organizations.

A discussion of ethics goes hand-in-hand with that of criminology because fraudsters often make poor ethical decisions prior to committing criminal acts. Consider, for example, financial statement fraud: perpetrators frequently find themselves on an ethical slippery slope, using an accounting choice as a tool for earnings management to maximize bonuses and influence the financial markets. When earnings management isn't enough, the individual finds himself at a point of no return, moving from the slippery slope of earnings

management to fraudulent financial statements. When does the fraud examiner or forensic accountant face an ethical dilemma? Whenever there are several choices, all outcomes have somewhat negative effects, and the correct choice is not obvious. Such dilemmas arise when many people could be harmed and some may benefit while others will not.

Consider another scenario: is it ethical for a fraud examiner or forensic accountant to lie to a perpetrator during an interview to elicit a confession? Most people agree that lying is wrong. Most also agree that an embezzler should not get away with their crime. If lying is the only way to get a white-collar criminal to confess, is lying ok? The answer isn't obvious because both choices are imperfect: (1) not lying, but the perpetrator gets away; (2) lying and the perpetrator confesses. In either case, the fraud examiner or forensic professional must choose from a flawed set of options. Closely associated with ethics is the concept of values. Values are the personal and social criteria that influence choice: family, friends, peer groups, nationality, culture, and economic and social classes. Values are learned beginning in childhood and are the conventions upon which choices are evaluated.

Approaches to Ethical Problem Solving

Is it Legal, or Does the Conduct Violate Known Rules? The law and rules is one approach to resolving an ethical dilemma. Most codes of conduct and professional associations, for example, require that professions avoid breaking the law. This is a practical approach and a starting point for determining if certain conduct should be avoided. The law, however, is the lowest threshold for ethical decision making.

It may happen that a law might permit an action that is prohibited by a profession's code of ethics. As an example, for years the American Institute of Certified Public Accountants (AICPA) had rules of ethics that prohibited advertising by its members. The profession believed that 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, disagreed. They decided that the prohibitions against advertising violated the laws barring restraint of trade. The government forced the profession to eliminate its 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 dignity should be preserved).

The Means Versus the Ends A second approach to ethics suggests that it is ok to "fight fire with fire." As Sean Connery's character, Malone, asks Elliott Ness (Kevin Costner) in *The Untouchables*, "What are you prepared to do? . . . You wanna know how to get Capone? They pull a knife, you pull a gun. He sends one of yours to the hospital; you send one of his to the morgue." Essentially, this is an outcome-based ethical framework. This has the purpose of justifying actions that otherwise could be considered immoral, unethical, or illegal. 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.[76]

Ethical Principles

The Imperative Principle Ethical principles, on the other hand, refer to the process upon which an ethical decision is analyzed or evaluated. Inherently, values are incorporated into the principles that help guide choice. The imperative principle is one of three ethical principles that provide a framework for ethical decision making, and is based on the work of philosopher Immanuel Kant. Although the following characterization is overly simplistic, Kantian philosophy tends to ignore outcomes by providing directives and rules without exception that are in the best interest of society as a whole. For example, under Kantian imperatives, "lying is always wrong." A society cannot exist if it is based on lies. Furthermore, society should value telling the truth over lying because society cannot exist if everyone is told to lie all the time (the alternative imperative to never tell a lie).

This unconditional obligation assumes that all people are aware of the rule and all agree to follow the rule. The Kantian imperative is very strict but provides an easy to understand framework for ethical decision making. However, Kant himself recognizes that at times, all general rules must have exceptions. While the Kantian imperative is almost impossible to follow all of the time, in practice, when a person is faced with violating an imperative, it alerts persons that they are faced with an ethical problem. Once the dilemma is identified, then the fraud examiner or forensic accountants can seek out additional consideration for weighing the consequences.

The Utilitarian Principle The utilitarian principle, championed by John Stuart Mills, suggests that ethical problems should be solved by weighing the good consequences and the bad consequences. The correct course of action is that which provides the most good or minimizes the bad. Like Kantian imperatives, the consequences to society generally are more important than those to individuals. Mills identifies two forms of utilitarianism, "act" and "rule." Act utilitarianism suggests that it is the consequences of the act that matter. For example, "honesty (an action) is the policy," subject to the evaluation of the specific circumstances that might suggest that an alternative action, lying, provides better consequences in this particular situation. The individual making the decision has the power to decide, so their value system drives the evaluation process of possible outcomes (consequences) and the final decision.

In contrast, rule utilitarianism emphasizes the benefits to society of general rules (similar to a Kantian imperative) and suggests that the decision to break a rule is one that requires very careful consideration. Rule utilitarianism requires that society as a whole be able to determine which rules are important and ought to be followed. Rules then are also influenced by history, nationality, culture, social goals, and at some level economics.

The difficulty with utilitarianism is the variation in outcomes. In any situation, almost any act can be justified and the choice is always a product of from where a person (act) or society (rule) came: family, friends, peer groups, nationality, ethnic background, and economic and social classes. Furthermore, it is difficult for everyone to agree on universal principles.

The Generalization Principle The generalization principle is an attempt to marry Kantian imperatives with utilitarianism, and was proposed by Marcus G. Singer. The generalization argument is as follows:

> *If all relevantly similar persons acting under relevantly similar circumstances were to act a certain way and the consequences would be undesirable, then no one ought to act in that way without a reason.*

More simplistically, the generalization argument poses the following questions as a first assessment:

> *What if everyone acted that way?*

If the outcome is considered undesirable, then that conduct ought to be avoided unless the person has a very good reason. Generalization provides the flexibility needed to address the shortcomings of Kant and the specific direction that seems to be missing from utilitarianism. Of course, the success of the generalization argument is dependent on the specific value assessments of the individual decision makers. Furthermore, generalization is invalid when an argument is either invertible or reiterable. Invertibility occurs when both doing something and not doing something leads to bad consequences. In such a circumstance, no generalization argument can be formulated. Reiterability occurs when arbitrary times, places, persons, or other factors can be inserted into a generalization in such a way as to make the generalization outcome to be nonsensical.

Ethics, Trust, and Responsibility

Although the preceding principles provide a framework for ethical decision making, alternative decisions may result in variations of good and bad consequences. Therefore, the task is a difficult one and the choice must be left to individuals. It is impossible to provide a blueprint for every situation with laws, rules, and exceptions. The bottom line is that civilized societies are based on trust with underlying values and implicit codes of conduct that guide our behavior. The decision process is difficult, and the range of possible outcomes suggests that the right choice is not always obvious. Though doing the right thing can be difficult, as members of society, we have a responsibility to reach for that goal every day, without exception.

ETHICS IN PRACTICE

Ethics and Values as Drivers of Personal Behavior

To be successful, professionals in the specialized field of fraud examination and financial forensics must have an ethical framework for appropriate decision making. Although the preceding material has suggested approaches to solving ethical problems, the fraud and forensic professional needs to strive for the highest degree of ethics. This perspective requires that the individual think about possible difficult situations and develop their own framework for decision making and, to the extent possible, in advance. Next, the

individual needs to make the commitment required to follow their ethical values in all cases except those that have extreme consequences.

In practice, fraud and forensic professionals can start with rules, laws, and Kantian imperatives to identify ethical situations (ethical dilemmas) that require more in-depth evaluation. Once the ethical problems have been identified, the evaluation process begins and professionals can use their own framework for ethical problem solving, including using personal rules and processes for decision making. The fraud and forensic professional is not alone and should solicit the input and opinions of other practicing professionals. In some cases, guidance and advice from professional organizations and associations can assist the individual in making the best decision. After careful consideration of the alternative outcomes and the decision is made, the professional can then move forward to implement that decision. This process will help to ensure that the anticipated goals are realized while also attempting to mitigate any negative consequences.

Students who are considering entering the field of fraud examination and financial forensics must consider decisions that they made in the past. For example, some may have past criminal convictions that might exclude them from entry into the profession. While most offenses should not prevent a prospective student from exploring their options, they should be aware that honesty is the best policy. Get caught in a lie, and your career could be over. Tell the truth and explain the facts and circumstances of a less than perfect past, and at least the individual (applicant) will have created a foundation of trust to repair the damage caused by prior conduct.

Professional Conduct

Professions are set apart by five characteristics:[77]

1. A specialized body of knowledge.
2. Admission governed by standards and qualifications.
3. Recognition and acceptance by society (a characteristic that inflicts social responsibility back on the profession).
4. Standards of conduct for dealing with the public, other professionals, and clients.
5. An organizational body devoted to the advancement and responsibilities of the profession.

These characteristics inflict responsibility on both the profession and the individual professionals. Normally, such responsibilities are captured in the profession's code of conduct. For example, Certified Fraud Examiners (CFE), as designated by the Association of Certified Fraud Examiners (ACFE), have the following code of ethics:[78]

1. A Certified Fraud Examiner shall at all times demonstrate a commitment to professionalism and diligence in the performance of his or her duties.
2. A Certified Fraud Examiner shall not engage in any illegal or unethical conduct, or any activity which would constitute a conflict of interest. (Note that the Certified Fraud Examiner has no exception for cases where they may be unaware that a particular law exists.)
3. A Certified Fraud Examiner 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.
4. A Certified Fraud Examiner will comply with lawful orders of the courts, and will testify to matters truthfully and without bias or prejudice.
5. A Certified Fraud Examiner, 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.
6. A Certified Fraud Examiner shall not reveal any confidential information obtained during a professional engagement without proper authorization.
7. 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.
8. A Certified Fraud Examiner shall continually strive to increase the competence and effectiveness of professional services performed under his or her direction.

Ethics at Client Entities: The Foundation for Fraud Prevention and Deterrence

Whereas the prior sections dealt with ethics at the individual and professional level, ethics are an important part of organizational behavior. In fact, ethics is the foundation for fraud prevention both by individuals within an organization and the organization itself.

Tone at the Top and a Culture of Ethical Behavior Ethics at the organizational level starts with corporate governance. The Board of Directors, the Audit Committee, executives, managers, clerical support, and line personnel are the living, breathing embodiment of ethics within the organization. The Board of Directors, Audit Committee, and corporate officers set the "tone at the top." Tone at the top refers to a culture that is open, honest, and communicates the values of the organization to persons at all levels, both internal and external to the organization. The first step in developing an ethical culture is a code of ethics signed by all personnel. In addition, the company's position on ethics should be posted in visible places, such as lunchrooms, and communicated across the organization. Employee awareness programs such as periodic ethics training are effective tools, and, of course, leaders lead by example. Employees will take their cues from their managers, managers from executives, and executives from their interaction with board members, audit committee members, and auditors. It is important that individuals in leadership positions not only communicate the value of ethical actions, they must also practice what they preach. In addition, important financial, operational, and compliance information should be disseminated to individuals who need it and can act on it. Furthermore, individuals at the top must be willing to listen to those operating at lower levels of the organization.

Second, the organization should be committed to hiring honest executives, managers, and staff. While most organizations attempt to contact prior employers and resume references, many organizations provide only minimal information about former employees and are remiss to provide any negative feedback for fear of legal retribution. References provided by prospective employees are typically friends and professional acquaintances; so prospective employers should seek out prior supervisors. While costly, organizations should consider background checks on prospective employees. Due to cost constraints, organizations may want to restrict the positions for which background checks are completed. To avoid charges of discrimination, prospective employers need to complete such checks in a consistent manner and in compliance with corporate policy.

Once individuals are hired, they need to be properly supervised. The most common excuse by managers for inadequate supervision is time constraints. While "too much to do, in too little time" is a common complaint in today's business environment, proper supervision is essential to maintaining good internal controls.

Training is another area that needs adequate attention. Many companies spend a considerable amount of time and resources developing their employees' technical abilities, but little time or resources are generally spent developing supervisory skills.

Maintain an Environment Dedicated to Fraud Prevention and Deterrence Once an organization has created the infrastructure to minimize fraud opportunities, the system has to be maintained. Supporting the anti-fraud environment requires continuing education of fraud awareness. The fraud triangle indicates that one of the factors necessary for fraud to occur is rationalization. Failing to maintain a work environment that discourages fraud may enable an employee to justify unethical or illegal actions. Such rationalizations may include the following: an employer's failure to recognize a job well done, an employee's overall job dissatisfaction, an employee's perception that they are inadequately compensated for their work, an employee's perception that the company owes them, and the misperception that no one is being hurt by their actions.

Another part of a good anti-fraud maintenance program is to provide assistance for employees with problems. In smaller companies, the human resources department may serve this function. In larger companies, there may be specific personnel devoted to assisting employees in exploring their options to solve a problem. This gives the employee the comfort to know that they are not alone, that their problem is "shareable."

Part of maintaining a strong anti-fraud environment includes appropriate disciplinary procedures, such as prosecuting fraudsters where evidence suggests that such action is warranted. Effective discipline requires a well-defined set of sanctions for inappropriate behavior and strict adherence to those sanctions in order to avoid claims of discriminatory conduct.

One of the most effective anti-fraud deterrents is a hotline to receive anonymous tips from employees, customers, suppliers, vendors, contractors, and others. According to the 2006 ACFE Report to the Nation, tips and accidental discovery (candidates for tip reporting) account for almost 60 percent of fraud detection. Thus, anonymous tip hotlines are a tool that should be in place at all organizations of any size.

In cases where tips are made by employees, especially lower-level employees who report wrongdoing by their supervisors, whistleblower protections should be in place. Unfortunately, even those whistleblower protections that are established by law may not protect employees from subtle, informal retribution, such as exclusion from meetings or not being given important information pertinent to doing their job.

Creating an anti-fraud environment also means minimizing opportunities for fraud. To accomplish this goal, companies need to establish and maintain a good internal control environment; discourage collusion and monitor employee relationships for collusion opportunities; alert vendors and contractors to company policies; monitor employees and, as noted above, create tip hotlines; create expectations that fraudsters will get caught and will be punished; and proactively audit for fraud.[79] Best practices to deter fraud include job rotation, surprise audits and reviews, open-door policies by upper-level management, and periodic testing of internal controls. Actively creating an anti-fraud environment means considering the following questions before fraud occurs:

What?

- What could go wrong?
- What assets are most susceptible?

Who?

- Who has the opportunity to commit fraud?
- Who has partial opportunity and who might they collude with to commit fraud?

How?

- How could fraud be committed—asset misappropriation and financial statement fraud?
- How effective is the internal control environment—policies and procedures?
- How susceptible is the company to management override?

When (timing)?

- When is fraud most likely to occur?

Where?

- Where would the fraud occur?
- Where would red flags (symptoms) manifest themselves?

Why?

- Why might fraud occur? i.e., pressures (nonshareable problems) created internally such as performance bonus plans
- Why might certain employees be driven to commit fraud? i.e., pressures (nonshareable problems) observed in certain employees (e.g., gambling problems, debt, drug or alcohol abuse, or marital issues)

The *who, what, where, when, how*, and *why* are questions fraud examiners and forensic professionals often investigate once fraud is discovered. Those same attributes need to be considered, proactively, as companies develop their anti-fraud environment.

React to Early Warning Signs The last aspect of a good antifraud environment requires that the organization react appropriately to symptoms of fraud, red flags, badges of fraud, and other early warning signals. Dr. Steve Albrecht references six types of anomalies that should be investigated at the earliest point of recognition: accounting anomalies, weak internal controls, analytical anomalies, lifestyles symptoms, behavior symptoms, and tips from potential informants. These issues will be more formally explored in later chapters, but some of these anomalies are listed below.

Accounting Anomalies

Irregular, unusual, and missing source documents
Excessive voids and refunds
Faulty journal entries and journal entries with missing documentation
Missing cash or assets (with coincidental reduction in the G/L with a credit)
Unusual account debits that are frequently used to conceal at fraud
Inaccuracies in ledgers
Underlying account detail does not equal balance
Underlying account detail does not reconcile to the general ledger
Subsidiary ledgers with missing support
Two sets of books and records
False ledger entries or alterations
Back-dated and post-dated documents and transactions
False invoices
False applications
False financial statements elements
Invoice numbers that do not make sense
Failure to keep and maintain records
Concealment of records
Refusal to make records available
Unexplained variances between tax returns and underlying books and records
False interview statements
Interference with an audit, examination, and investigation
Failure to follow advice of attorneys and accountants
Less than full disclosure (e.g., masking the true financial impact)
Taxpayer knowledge
Testimony of employees and other witnesses
Destruction of books and records
Inappropriate transfer of assets
Patterns inconsistent over time
Attempts to bribe the auditor, examiner, or investigator

Weak Internal Controls

Lack of segregation of duties
Lack of physical safeguards for valuable assets (e.g., intellectual property)
Lack of independent checks and balances
Lack of proper authorization
Lack of proper supervision
Lack of proper documents and records (e.g., missing originals)
Observations of management overriding existing controls
Inadequate accounting and information systems
Related parties transactions

Analytical Anomalies

Unexplained inventory and cash shortages
Deviations from quality specifications (e.g., warranty liability down)
Excess scrap

Excess voids

Excess purchases compared to revenue levels

Ratios that don't make sense

Nonfinancial numbers that do not correlate with account balances and other numbers presented in the financial statements

Excessive late charges in accounts payable, notes payable, and company credit cards

Strange financial relationships

e.g., Revenues up; inventory down; A/R up; cash flows down

e.g., Increased inventory; A/P down

e.g., Increased volume; increased costs per unit

e.g., Increased inventory; decreased inventory holding costs

e.g., A/R up; bad debts down

Lifestyles Symptoms

New luxury cars

Pricey clothes

New or high-priced house

Expensive jewelry

High-end recreational toys, such as boats, vacation homes, motor homes

Behavior Symptoms

Can't look people in the eye

Embarrassment with friends, family

Irritable and suspicious

Defensive

Argumentative

Unusually belligerent in stating opinions

Needs to see a counselor, psychiatrist, etc.

Complains of being unable to sleep

Drinks too much

Using illegal, illicit drugs

Can't relax

Potential Informants

Employees

Customers

Suppliers

Family

Friends

Five-Step Approach to Fraud Prevention, Deterrence, and Detection

1. Know the exposures (brainstorming, risk assessment, audit planning).
2. Translate exposure into likely symptoms.
3. Always be on the lookout for symptoms.
4. Build audit and data-mining programs to look for symptoms.
5. Pursue these issues to their logical conclusion and ground decisions in the evidence (evidence-based decision-making).

REVIEW QUESTIONS

3-1 Describe occupational fraud and abuse.

3-2 Compare and contrast Cressey's and Albrecht's theories of crime causation.

3-3 Identify from Cressey's research the six situational categories that cause nonshareable problems.

3-4 Discuss the essence of organizational crime.

3-5 Give examples of behavioral indications of fraud.

3-6 Explain the relationship between an employee's position and the level of theft (according to Hollinger and Clark's research).

3-7 Analyze the role of corporate governance mechanisms in fraud prevention.

3-8 Describe corporate governance breakdowns in the facilitation of Enron's fraudulent acts.

3-9 Identify ethical issues, conflicts of interest, and noncompliance with corporate policies and procedures in the Enron case.

3-10 Discuss alternative courses of action in the Enron case within the framework of appropriate ethical conduct.

ENDNOTES

1. Source unknown
2. See Albrecht's Fraud Examination and the ACFE's *Fraud Examiners Manual*. Fraud statistics can be found in the ACFE's 2004 *Report to the Nation*.
3. Adapted from the ACFE's *Fraud Examiners Manual*, Section 1.21.
4. The Association of Certified Fraud Examiners, *The Report to the Nation on Occupational Fraud and Abuse* (Austin: ACFE, 2008).
5. "Thompson Memo," U.S. Department of Justice Memorandum, January 20, 2003: "Principles of Federal Prosecution of Business Organizations."
6. Jennings, Marriance M., *Business: Its Legal, Ethical and Global Environment* (Thompson-West 2006), 367.
7. Ibid., 377.
8. Ibid., 383.
9. Gilbert Geis, *On White Collar Crime* (Lexington, Lexington Books, 1982).
10. Larry J. Siegel, *Criminology*, 3rd Edition (New York: West Publishing Company, 1989), 193.
11. Donald R. Cressey, *Other People's Money* (Montclair: Patterson Smith, 1973), 30.
12. Ibid., 33.
13. Ibid., 34.
14. Ibid., 34.
15. Ibid., 35.
16. Ibid., 36.
17. Ibid., 36.
18. Ibid., 42.
19. Ibid., 42.
20. Proverbs 16:18.
21. Cressey, 47.
22. Ibid., 48.
23. Ibid., 52–53.
24. Ibid., 54.
25. Ibid., 57.
26. Ibid., 66.
27. Ibid., 84.
28. Ibid., 84.
29. Ibid., 85.
30. Ibid., 94–95.
31. Ibid., 93.
32. Ibid., 101–102.
33. Ibid., 102.
34. Ibid., 102.
35. Ibid., 120–121.
36. Ibid., 121.
37. Ibid., 122.
38. Ibid., 121.
39. Ibid., 122.
40. Ibid., 128.
41. Ibid., 129.
42. Ibid., 128–129.
43. Ibid., 133.
44. Ibid., 139.
45. W. Steve Albrecht, Keith R. Howe, and Marshall B. Romney, *Deterring Fraud: The Internal Auditor's Perspective* (Altamonte Springs: The Institute of Internal Auditor's Research Foundation, 1984).
46. Although such red flags may be present in many occupational fraud cases, one must reemphasize 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—whether nonoffenders have many of the same characteristics. If so, then the list may not be discriminating enough to be useful. In short, although one should be mindful of potential red flags, they should not receive undue attention absent other compelling circumstances.
47. Ibid., 13–14.
48. Ibid., 32.
49. Ibid., 39
50. Ibid., 5.
51. Ibid., 6.
52. Ibid., 5.
53. Ibid., 5.
54. Ibid., 6.
55. Ibid., 42.
56. Ibid., 15.
57. Richard C. Hollinger and John P. Clark, *Theft by Employees(* Lexington: Lexington Books, 1983**),** 6.
58. Ibid., 42.
59. Hollinger and Clark, p. 57.
60. Ibid., 57.
61. Ibid., 57.

62. Ibid., 63.
63. Ibid., 68.
64. Ibid., 77.
65. Ibid., 86.
66. Ibid.
67. Ibid.
68. Ibid., 106.
69. Ibid., 117.
70. Ibid., 120.
71. Ibid., 121.
72. Ibid., 144.
73. Ibid., 146.
74. Ethics should be considered pervasive, a common thread, and included in all aspects of the fraud and forensic accounting curricula.
75. Random House Webster's *College Dictionary* (1991).
76. Association of Certified Fraud Examiners, *ACFE Fraud Examiners' Manual* (2006).
77. Association of Certified Fraud Examiners, *Fraud Examiners Manual* (2005), 4.902.
78. Ibid., 4.901.
79. W. Steve Albrecht, Conan C. Albrecht, and Chad O. Albrecht, *Fraud Examination*, South-Western, 2002, p. 90–96.

CHAPTER 4

COMPLEX FRAUDS AND FINANCIAL CRIMES

LEARNING OBJECTIVES

After completing this chapter, you should be able to:

- **4-1** Differentiate between a predator and an ''accidental fraudster.''
- **4-2** Explain why collusion poses unique prevention and detection challenges.
- **4-3** Describe how the concept of an ''organization'' is involved in mixing illegal activities with legitimate ones.
- **4-4** Explain the difference between ''following the money'' and ''tracing the money.''
- **4-5** Discuss why financial statement fraud is often considered a complex fraud.
- **4-6** List different types of schemes associated with complex frauds.
- **4-7** Contrast the objectives of terrorists and organized criminals.
- **4-8** Identify and describe the different types of banks.
- **4-9** Explain the difference between tax avoidance and tax evasion.
- **4-10** List and discuss some of the more common securities fraud schemes.

CRITICAL THINKING EXERCISE

A woman came home with a bag of groceries, got the mail, and walked into the house. On the way to the kitchen, she walked through the living room. In the living room, she glanced in her husband's direction. Sadly, her husband had blown his brains out. She then continued to the kitchen, put away the groceries and made dinner.

What might explain this behavior?

''PREDATORS'' VERSUS THE ''ACCIDENTAL FRAUDSTER''

The common fraudster is usually depicted with the following characteristics: first-time offender, middle-aged, male, well educated, married with children, trusted employee, in a position of responsibility, and possibly considered a "good citizen" through works in the community or through a church organization. This individual is often described as having some nonsharable problem, typically financial in nature or that the problem can only be solved with money, which creates the perceived pressure. When aligned with opportunity and the ability to rationalize his or her actions, the otherwise good citizen succumbs to pressure, develops one or more fraud schemes and misappropriates assets or commits an act involving some form of corruption. This person might be characterized as the "accidental fraudster."

Not withstanding the fraud act, the accidental fraudster is considered a good, law-abiding person, who under normal circumstances would never consider theft, breaking important laws, or harming others. When discovered, family members, fellow employees, and other persons in the community are often surprised or even shocked by the alleged behavior of the perpetrator. Because many of these perpetrators are in positions of trust (which creates opportunity), well educated, and have leadership-level employment, Edwin H. Sutherland, in 1939 described them as "white-collar criminals."

White-collar crime, as designated by Sutherland, is crime in the upper, white-collar class, which is composed of respectable or respected business and professional men (and now, almost as often as not, women). White-collar crime is also referred to as occupational fraud or economic crime. The white-collar criminal's actions are consistent with the notion of a trust violator, and the crime is typically associated with an abuse of power. Despite some shortcomings with this type of descriptive terminology, white-collar

crime captures the essence of the type of perpetrator that one often finds at the heart of occupational fraud and abuse.

The fraud triangle was created with the accidental fraudster in mind. The fraud triangle helps investigators to understand who might commit fraud and why. The notion of perceived pressure and opportunity and the development of a rationalization for the crime provides a profile, not only to help understand the typical accidental fraudster, but also to help identify meaningful, nonfinancial, sociological, and psychological red flags that can be used as part of the investigatory process to determine who perpetrated the identified occupational fraud or abuse.

On the other hand, what if the person has committed an act of fraud at a prior organization? Franco Frande, ATF Financial Investigations Chief, often tells the story of ten-year-old Christopher Woods. Christopher Woods was killed by his father for life insurance money. His father strangled the boy and tossed him onto the side of the road near a lake. The father then started a fire in his home, but when inquiries were made by investigators and the TV news media, he blamed Christopher for accidentally starting the fire. He stated that his son had run away after starting the fire and Mr. Woods tearfully pleaded to the TV newscaster for his son's safe return home. At the time, no one except the father knew that Christopher Woods was dead. The father had set up the crime by talking with others about the "problem" he was having with his son's playing with matches. He also placed matches under the couch seat cushion where Christopher's mother would discover them during routine cleaning. The fire allowed the husband to collect additional insurance proceeds related to the home structure and contents. All of this was to repay his most recent former employer as restitution for a fraud that he had been perpetrating.

Mr. Woods' most recent employer had agreed to desist from filing charges against him or making any public disclosures of the fraud incident provided that Mr. Woods reimburse the company for the missing funds. What the employer did not know is that the current incident was the fourth time that Mr. Woods had perpetrated a fraud. In the prior three incidents, upon discovery, the previous employer had quietly terminated Mr. Woods. It's possible that Christopher Woods might be alive today if any of the prior employers had prosecuted Mr. Woods. The choice made by each of his former employers allowed him to quietly move on to his next victim.

Mr. Woods is not an accidental fraudster; he is a predator. The predator seeks out organizations where he or she can start to scheme almost immediately upon being hired. At some point, many accidental fraudsters, if not caught early on, move from behavior characterized by the description of an accidental fraudster to that of a predator. Financial statement fraud perpetrators often appear to start as accidental fraudsters or even as managers of earnings and, sooner or later, become predators.

Beyond the predator-type person who seeks to deliberately defraud organizations with seemingly little remorse, we also find individuals and organizations that have operational modus operandi where a complex fraud or financial crime is inherently part of their goals and objectives. Organizational crimes occur when public and private companies, nonprofits, and government entities, otherwise legitimate and law-abiding organizations, are involved in a pattern of criminal activity. Corporate violations include administrative violations that involve noncompliance with agency, regulatory, and legal requirements. In other cases, organizations are deliberately established with at least some nefarious purposes in mind. We often think about organized crime, drug trafficking, and terrorism financing for the more complex frauds and financial crimes involving organizations. Organized criminal activities often involve many individuals, organizations, shell companies, and cross-jurisdictional borders. Some of the crimes that are typically observed include conspiracy and RICO (Racketeer Influenced and Corrupt Organizations) Act violations, money laundering, and mail and wire fraud. With terrorism financing, illegal acts derived from the USA Patriot Act come into play.

The important point is that predators and organizations focused on criminal activities exist and that reference to these types of entities as predators helps us to better understand their activities and motives in order to better investigate allegations of fraud and financial crimes. Typically, these types of entities are involved in complex frauds, corruption schemes, and financial crimes. Because their activities are far more deliberate from the outset than those of the accidental fraudster, they are better organized, have better concealment schemes, and are better prepared to deal with auditors and other oversight mechanisms. The concern is that in many cases the fraud triangle may not apply to the predator. Nevertheless, the primary investigative approach that focuses on the elements of fraud and adheres to evidence-based decision making holds quite well. Investigations centered on the act (the complex fraud or financial crime), the concealment of the crime, and the conversion (the personal benefit derived by the perpetrator from his actions) will lead to the development of a solid case from which the judicial community may determine the best course of remediation. Complex fraud and financial crime schemes include the following: money laundering

associated with organized criminal activities, terrorism financing, money flows associated with drug trafficking, tax evasion, deliberate misrepresentation of an entity's financial performance, and deliberate bankruptcy misreporting. Violations arising from these schemes may include money laundering, corruption, tax fraud, financial statement fraud, conspiracy, and mail and wire fraud.

COLLUSION: MULTIPLE INDIVIDUALS, ORGANIZATIONS, AND JURISDICTIONS

One of the central elements to complex frauds and financial crimes is that of collusion. Collusion may be among individuals within an organization, individuals across organizations, and multiple organizations. Collusion often spans multiple jurisdictions, including local, state, federal, and international boundaries and related laws. ACFE's report to the nation indicates that when collusion is involved, dollar amounts associated with fraud losses increase dramatically. The losses caused by individual predators can be substantial, but when those individuals work in concert with others, the damage can be devastating and far more pervasive.

The primary concern when collusion is involved is that internal controls are generally ineffective in preventing fraud and other financial crimes. The primary internal control of segregation of duties helps to ensure that no individual controls every aspect of a transaction and separates the custody, accounting, and approval functions. Internal controls also include independent checks on performance and assurance of compliance with applicable laws and regulations. While internal controls cannot prevent collusive fraud and financial crimes, they may assist in the detection of such activities. In particular, independent monitoring may reveal that internal controls have been circumvented through collusion.

If the predators are organized around criminal activities, however, it is unlikely that monitoring will have any impact because part of the goals and objectives of an illicit organization is to disguise the nature of its real operations from outsiders, including auditors, regulators, and law enforcement. Persons inside the organization, across organizations, and across jurisdictions act in such a manner so that the true underlying nature of the organization and its activities cannot be discovered.

LEGITIMATE ACTIVITIES MIXED WITH ILLEGAL ACTIVITIES AND THE NEED TO ISOLATE ILLEGAL ACTIVITIES

Another element of complex frauds and financial crimes is that the perpetrators often mix legitimate business activities with their unlawful transactions. Money laundering provides an excellent example of a complex financial crime that is designed to mix monies from some legitimate and legal activity with proceeds obtained through some illegal activity. Understanding the essence of complex frauds and financial crimes requires attention to the definition of "the organization." Using the crime of money laundering as an example, assume that a local neighborhood tavern is used as a conduit for this activity. The operations of the tavern may be completely legitimate, except for the money laundering activity. The tavern is also part of a greater organization in which other persons and/or entities are transacting illegal business activities that generate illicit cash proceeds. This cash needs to be "laundered" to appear legitimate.

To understand the motivation of the tavern's owner, we refer to the M.I.C.E acronym: the motivation could be **m**oney, **i**deology, **c**oercion, or **e**go. While it is unlikely that the tavern owner would get involved in an illegal money laundering operation to satiate his ego, they may be willing to play a role to obtain a "piece of the action" (money), to further a cause in which they believe (e.g., to fund terror operations) or because they are being threatened (coerced). Examples of coercion could be threats of physical harm to the owner, patrons of the tavern, the owner's family, or the physical premises of the tavern. Investigators must also have some sense of the entire story: who, what, when, where, how, and why (if known). To attempt to prosecute the tavern owner without a sense of the greater story will be far more difficult because the investigator will be unable to communicate that understanding to prosecutors, defense attorneys, judges, and jurors. To tell a more complete story, fraud and forensic accounting professionals must know the greater "organization," even if the organization is not recognized as a legal entity.

Inherently, most complex fraud and financial crime schemes include a mixture of legitimate and illicit activities. One of the main challenges for investigators is to isolate the illicit from the legitimate activities. This is an essential element for successful remediation of the crime and can be accomplished by using the investigative tools and techniques highlighted in this textbook.

ASSET FORFEITURE AND SEIZURE AND DISMANTLING ORGANIZATIONS

Asset forfeiture or seizure is an important part of the process of dismantling an organization, particularly with complex frauds or financial crimes. As discussed above, the nature of the activities is such that collusion is likely involved. In more serious cases, the underlying design, goals, and objectives constitute illegal activities. By seizing assets, the perpetrators are being punished and the organization is dismantled to make it more difficult for another person in the chain of command to take over the remaining operations.

First, money and other assets must be identified during the investigative process. The investigation needs to show that the perpetrator(s) or the organization(s) involved received assets and what happened to those assets. This requires that all records—banking, public, business, personal, financial, and nonfinancial—are searched to identify assets available for seizure, and to help separate those related to illegal activities from those generated from legitimate sources. This is accomplished through a process of "following" or "tracing" the money. Chapter 15 discusses this process in detail.

Dismantling the organization by seizing operational assets, confiscating cash, and freezing funds is an effective tool for forensic professionals in the pursuit of their responsibilities. Criminal organizations, drug traffickers, and terrorists need money to achieve their goals because they must cover operating costs, including paying employees, investing in infrastructure, paying legal fees, and covering other costs comparable to those of a legitimate business enterprise. While criminal organizations cannot declare bankruptcy, the seizure of assets can have the effect of putting them out of business, at least for the short term.

SCHEMES AND ILLEGAL ACTS ASSOCIATED WITH COMPLEX FRAUDS AND FINANCIAL CRIMES

As noted above, the profile of perpetrators of complex frauds and financial crimes tends to align more with those of predators rather than the accidental fraudster. Their motivation and intent is generally more nefarious and deliberate, and their mode of operation more sophisticated. Furthermore, the perpetrators of complex frauds and financial crimes often collude with others who can provide additional resources or legitimacy for their activities.

Financial statement fraud is more often than not a complex fraud. It almost always involves the chief financial officer, controller, or some other sophisticated participant within the financial reporting structure. It also often involves top leadership in the organization such as the chief executive officer, chief operating officer, president, or others with significant levels of authority. While not always predatory, at least at the time of inception, it is almost always collusive. Executive-level individuals work in concert (collusively) to override the system of internal controls through the sophisticated use of journal entries, significant estimates, and other financial reporting choices, and through material, unusual, one-time transactions. Due to the unique nature of financial statement fraud, the large dollars involved, its impact on stakeholders, and its connection with the audit profession, it is addressed separately in Chapter 14.

Similarly, corruption schemes are addressed in Chapter 13. Corruption includes bribery, illegal gratuities, economic extortion, and conflicts of interest. Corruption is collusive by its very nature and tends to be predatory. At least one party, and possibly all parties, to the corruption scheme set out to achieve certain goals as a result of their activities. While illegal gratuities and conflicts of interest may fall close to being ethically questionable, specific laws make such activities illegal.

When one thinks of organized criminals, drug traffickers, and terrorists and their financiers, one typically thinks of strong organizations and carefully planned operational activities. These types of organizations are sophisticated and tend to be very disciplined. Furthermore, they tend to make extensive use of technology. The advent of disposable cell phones, Internet money transfers, money transfers via beaming (infrared) cell phone technology, the easy movement of money around the world, and banking and legal jurisdictions committed to secrecy and privacy have made tracking these types of criminals and their activities (financial and nonfinancial) challenging for those saddled with the responsibility of policing them and stopping such activities.

Organized Crime

The definition of organized crime is a hotly debated subject. The Organized Crime Control Act of 1970 defines the activity as "The unlawful activities of ... a highly organized, disciplined association." The traditional understanding is that organized crime or criminal organizations are entities controlled and

operated by criminals for the common purpose of generating positive cash flows from illegal acts. The term "organized" is central to the definition. Many of these organizations are professionally run as if they were a traditional for-profit business. Their operations include hiring (firing), training, mentoring, information systems, a hierarchical structure, and other attributes associated with effective and efficient business entities. As such, the organizations are opportunistic, diversified, and require political support (legal or otherwise) and capital investment. Racketeering is the act of engaging in criminal activity as a structured group, and organized criminal organizations are often prosecuted under RICO.

Most people think of the Italian Mafia (as portrayed in the film *The Godfather*), Al Capone, and similar images when organized crime is mentioned. Organized crime, however, is far more global and complex than these traditional images suggest. Organized crime can be found in even the tiniest and most remote regions of the world. Some of the more recognized organized crime activities in recent times include the rise of the Russian mob in the wake of the collapse of the Soviet Union, organized criminals from Africa who specialize in narcotics and financial scams, Asian crime organizations grounded in secret societies, and crime groups located in former Eastern Bloc countries. The FBI estimates the annual impact of organized crime profits to be approximately $1 trillion. Organized crime, when the opportunity presents itself, will manipulate and monopolize financial markets, particularly those in less developed areas; infiltrate labor unions; align itself with traditional businesses, such as construction and trash hauling; engage in the purchase of political support through bribery, extortion, blackmail, intimidation, and murder; as well as organize and carry out various financial frauds.

The more famous criminal enterprises are those associated with the Italian Mafia. Italian organized crime consists primarily of four major groups, estimated to have 25,000 members and more than 250,000 affiliates worldwide. In recent years, the Italian mob has collaborated with other criminal organizations. The Italian groups have been involved in heroin smuggling for decades, as well as money laundering activities. In addition to narcotics, the Italian mob, earning as much as $100 million annually, has been involved in bombings, counterfeiting, fraud, illegal gambling, kidnapping, murder, political corruption, and the infiltration of legitimate business. The four major organizations that make up the Italian mob consist of the Sicilian Mafia, the Camorra or Neapolitan Mafia, the Ndrangheta or Calabrian Mafia, and the Sacra Corona Unita or United Sacred Crown.

In the United States, the FBI is most concerned about La Cosa Nostra (LCN). The literal translation of La Cosa Nostra is "this thing of ours." LCN consists of several aligned family organizations and cooperates with the four groups identified above who operate out of Italy. LCN is involved in a multitude of criminal acts including corruption, drug trafficking, illegal gambling, infiltration of legitimate business, labor racketeering, loan sharking, murder, stock manipulation, and tax fraud. Labor racketeering has been a significant source of LCNs national profit, power, and influence.

Balkan organized criminal enterprises are associated with Albania, Bosnia-Herzegovina, Croatia, Kosovo, Macedonia, Serbia, Montenegro, Bulgaria, Greece, and Romania. The groups from these areas arose from their traditional protection and support needs that were provided for by various clans. Over time, these clans morphed into organizations entrenched in organized crime. Many of these countries were under the control of the Soviet Union until its collapse. At that time, these groups, which had been working in the black market, infiltrated and exploited the new democratic governing bodies. These groups are not as well organized as others, still holding to their clan roots, but are involved in fraud, gambling, money laundering, drug trafficking, human smuggling, robbery, murder, and other violence.

Asian crime groups grew out of triads, tongs, and street gangs. These groups arise from, and operate in, Asian countries such as China, Japan, Korea, Thailand, the Philippines, Cambodia, Laos, and Vietnam. The groups from China predominantly arose from triads or underground societies. In contrast, the organizational structure of the groups from the remaining countries were influenced by tongs, triad affiliates, and street gangs. These groups tend to commingle legal and illegal activities. The illegal activities often include extortion, murder, kidnapping, illegal gambling, prostitution, loan sharking, human trafficking, drug trafficking, theft of intellectual property, counterfeit computer, textile, and other products, money laundering, and financial fraud.

Eurasian criminal enterprises grew out of the Soviet prison system, emigrated to the West, and proliferated in the former Soviet Union after its collapse. Eurasians specialize in sophisticated fraud schemes, tax evasion, and public corruption. The activities of the Eurasian groups have destabilized the governments of the former Soviet Union. A major concern is the access of these groups to leftover Soviet nuclear weapons. Some of the fraud schemes include those associated with healthcare, auto insurance, securities and investment fraud, money laundering, human smuggling, prostitution, drug trafficking, auto theft, and the transportation of stolen goods.

African organized crime is most known for its efforts with illegal drug trafficking and online financial frauds. Nigeria is known as one of the hubs for organized crime enterprises in Africa. Other locales for organized criminals include Ghana and Liberia. Nigerian organized crime is famous for its financial frauds, which the FBI estimates cost Americans $1 billion to $2 billion annually. Some of the criminal activities include auto insurance fraud, healthcare billing fraud, life insurance scams, bank, check, and credit card fraud, as well as other sophisticated fraud schemes.

Middle Eastern crime groups are engaged in a variety of criminal acts including money laundering, cigarette smuggling, and identity theft. Generally, these groups are for-profit enterprises and are not overtly affiliated with terrorist groups such as Al Qaeda. Like the Balkan groups, these organized criminal groups are less well organized, and their affiliations tend to be based on tribal and family associations. These groups are known to be involved in auto theft, financial fraud, interstate transportation of stolen items, drug trafficking, document fraud, healthcare fraud, identity theft, cigarette smuggling, and the theft of baby formula for the purposes of cutting drugs.

Organized crime, including drug trafficking as discussed below, is investigated using traditional techniques such as undercover operations, surveillance, wire tapping, confidential informants, victim interviews and testimony, document review and analysis, examination of public records, and following the money (direct, indirect, and ad hoc financial analyses). With the exception of terrorists, the primary motivation of organized criminals is the ability to make more money through collaboration than when working alone or in smaller, less organized, and less disciplined groups. The flow of money, along with an understanding of the rest of the story line (how, what, when, where, how, and why), provides a solid investigative approach for case development.

Drug Trafficking

Drug trafficking is a specific example of an organized criminal organization. The primary difference is that these organizations specialize in trafficking narcotics for illegal sale in countries all over the world. Mexican drug traffickers have a significant market share of illegal drugs transported into the United States, including cocaine, marijuana, heroin, and methamphetamine. In recent years, the Mexican traffickers have become more professional and violent. Due to the significant profits associated with illegal drugs, drug producers, traffickers, and distributors are more likely to collaborate. Around the world, the United States and other nations forge partnerships to address the various problems associated with illegal drugs.

According to Drug-Free America, illegal drug trafficking costs the United States $70 billion annually. Mexican transporters exploit the 2,000-mile shared border between the United States and Mexico as the entry point for the majority of illegal drugs into America. During 2000, 89 million automobiles, 4.5 million trucks, and 293 million people entered the United States from Mexico.[1] In addition to border crossings, drug traffickers also utilize airplanes, high-speed boats, and cargo ships entering and exiting U.S. waters. The Drug Enforcement Agency (DEA) estimated in 2000 that 50 percent of the cocaine entering the United States, and 85 percent of methamphetamines, entered from Mexico.

Mexican traffickers are organized, have the skills necessary to be effective, and demonstrate high levels of professionalism. Some of the Mexican trafficking organizations include the Juarez Cartel, Arellano-Felix Brothers' organization, the Caro-Qunitero organization, and the Amezcua-Contreras organization, all of which control the Tijuana and Ciudad Juarez areas around the Gulf of Mexico. These groups have loosely organized themselves as the Federation. The partnership provides greater security and profitability to the membership. These groups are estimated to earn tens of billions of dollars annually.[2] The Mexican organizations appear to be more specialized (drug manufacturing and transportation, related money laundering, and unrelated robbery) than most organized criminal groups, which tend to be more opportunistic and engage in broader ranges of illegal activity.

Although the groups are not known for their violence within the borders of the United States, outside of the United States they have been known for corrupting and killing law enforcement and public officials who threaten their livelihood. Within the United States, their efforts are more directed to corruption, including massive bribes. These bribes, for example $50,000 for allowing one vehicle to cross the border unimpeded, are concentrated at the point of entry because once in the United States, the probabilities of being detected drop considerably until the illegal drugs are sold to end users. These groups are considered to be professionally operated with centralized decision making. While these groups are known for trafficking, they do not distribute the narcotics once the drugs are inside the United States. Most of that part of the operation is handled by organized criminal organizations rooted in Dominica and Columbia.

These groups are considered highly professional. The narcotics transfers from the traffickers to the distributors are carefully orchestrated and often include surveillance of local law enforcement anti-drug units to ensure that the transfers will not be disrupted. Like the bootleggers of Al Capone's time, the traffickers will also partner with legitimate cargo carriers and conceal the narcotics among legal goods. Traffickers also exploit the advances in technology by communicating over the Internet, using various forms of encryption as well as more traditional communications via fax, phone, and pagers. The sophisticated groups also employ accountants, lawyers, and other professionals that are necessary to conduct their operations. Mexican criminal organizations are not alone in the global efforts to supply drugs. Almost all organized crime groups from around the world including those from Asia, Eurasia, the Balkans, Africa, the Middle East, and the former Soviet Union are participants in drug manufacture, transportation, and distribution to some degree.

Recommendations for effectively attacking the drug trafficking problem in the United States include the following:

- Improving coordination among U.S. drug fighting agencies
- Strengthening the legal institutions in Mexico and other countries where drugs are produced and transported, including the development of effective and respected law enforcement, prosecution, and judicial systems that address both the illegal acts and the associated corruption
- Improving multilateral coordination between the United States and other nations involved in counter-narcotics efforts
- Continuing and expanding programs that emphasize demand reduction in the United States and other countries with large numbers of narcotics users

In short, bilateral and multilateral counter-narcotics efforts are the key effective responses to fighting drug trafficking. Only with coordinated and sustained efforts, including those centered on information and intelligence sharing, will law enforcement worldwide be able to successfully combat illegal drugs.

Terrorism Financing

Even before September 11, 2001, the United States faced unprecedented challenges in this area. Terrorists, determined to undermine our way of life, made security a primary concern for government entities such as the CIA and Department of Defense. Because terror organizations need funds to operate and purchase guns, explosives, and other supplies; require training; and often function loosely or efficiently as organizations; fraud professionals and forensic accountants are integral to following and tracing their funding sources. The goal of fraud examiners and financial forensic professionals is to deny terrorist groups access to the international banking system. This has the affect of impairing their ability to raise funds, thus exposing, isolating, and incapacitating their financial networks.

Terrorism, as its main objective, is designed to intimidate a population or to compel a government to do or abstain from doing any act. Terrorists attempt to intimidate or coerce persons, governments, and civilian populations through the use of force or violence, real or threatened, to achieve political or social objectives. While drug traffickers and organized criminals are organized around deriving financial gain from their activities, terror groups' objectives are publicity, legitimacy, and influence. Like all entities, however, terrorist groups must build and maintain infrastructure and operations to achieve their objectives. Money is required to attract and retain personnel, to support their activities, and to pay for training facilities, firearms, explosives, media campaigns, political influence, and even to support social projects such as schools and hospitals in order to further their ideological objectives. Terrorists often live modestly, a characteristic in contrast with that of drug traffickers and organized criminals. Although the international banking system is required for successful terrorist activities, funding requirements for the organization may be relatively small by comparison. The small nature of the transactions makes the investigation similar to looking for a needle in a haystack.

Two primary sources of terrorist financing are state sponsorship and revenue generating from legitimate and illegitimate activities. Iran, North Korea, Syria, and others are often denoted as state sponsors of terrorism. Each of these countries, for differing reasons, awards resources to active terrorist organizations. Due to bank secrecy laws and other impediments to transparent financial transactions, the Cook Islands, Dominica, Egypt, Grenada, Guatemala, Hungary, Indonesia, Israel, Lebanon, the Marshall Islands, Myanmar, Nauru, Nigeria, Niue, Philippines, Russia, St. Kitts and Nevis, St. Vincent, the Grenadines, and the Ukraine are considered places where terrorists may find some safety. In a post-9/11 world, these countries

appear to have improved their efforts to assist international law enforcement in tracking and prosecuting criminals. Nevertheless, their laws do not afford the reporting requirements and financial reporting transparency commonly found within the United States.

Osama bin Laden, leader of the al-Qaeda terrorist network, is one of fifty-three children of a Saudi construction magnate. He inherited the foundations for his fortune, which is estimated at $5 billion. Beyond his inheritance, Osama bin Laden has invested in legitimate companies including a bakery, a furniture company, and a cattle-breeding operation. Osama Bin Laden is an example of an individual sponsor of terror, whereas his legitimate business operations are organizational examples.

Charities may be an additional source of terrorist funding. Examples include the Holy Land Foundation in Texas (now disbanded), and the Al-Aqsa Foundation in Germany. Each of these has been investigated for funneling donations to terrorists. In many cases, the donors to these "charities" do not know that they are funding terrorist activity.

Terrorists also obtain funds from both legitimate and illegitimate revenue generating activities; by mixing funding from legal business activities and unlawful acts, terrorist organizations appear similar to other criminal organizations. Related to criminal behavior, terror organizations support themselves with kidnapping, extortion, and protection money. For example, terrorist organizations such as FARC (Revolutionary Armed Forces of Columbia) and the AUC (United Self-Defense Forces of Columbia) in Columbia, are characterized by the kidnapping of both governmental and nongovernmental persons for ransom. FARC and AUC also enforce the payment of "taxes" on cocaine production. Criminal activities by terror organizations have been observed in the United States and include large-scale identity theft, smuggling, fraud, theft, robbery, and narcotics trafficking. Consistent with other criminal organizations, funds from legitimate sources are commingled with those from illegitimate sources. Legitimate sources of income may include donations, membership dues, sale of publications, cultural and social events, and solicitations and appeals to wealthy individuals with similar ideological beliefs.

When a criminal activity generates income, like other criminal organizations, terror groups must find a way to position the money for its intended use without attracting attention to the terrorist organization, the persons involved, or the underlying unlawful behaviors. Criminals do this by money laundering: disguising the sources, changing the form, and moving the funds to places where they are less likely to attract attention. In addition, terrorist groups have been known to utilize less restrictive overseas banks, to use informal banking systems such as Hawala, to smuggle cash, to structure banking transactions to sufficiently small amounts, and to use travelers' checks and money orders.

Countries like the United States attempt to monitor and track terrorists and their supporting organizations on several fronts, including the monitoring of financial transactions. Similar to the fraud triangle for the accidental fraudster, the "terrorism triangle" is necessary as a precursor set of conditions for terrorism activities to exist. Terrorists and their related activities exist only under the conditions of opportunity, ideological motivation (versus pressure), and ideological rationalization. Inherently, terrorists have the ideological motivation to inflict terror; similarly, most terrorists show little remorse and rationalize their activities based on their ideological beliefs. This observation is true not only for al-Qaeda, but also for Timothy McVeigh and Ted Kaczynski, the Unabomber. Opportunity may be the most important attribute for investigators because without the opportunity to generate, move, and control cash flows, the financing of terror cannot occur.

The elements of fraud provide a solid structure to investigate attempts at terror financing and to identify illegal financial activities associated with terror: the act, the concealment, and the conversion. First, the terrorist financier must commit an illegal financial or fraud act, for example, identity theft. Knowing that an illegal act has taken place and tracing the funds associated with the act back to the perpetrator is a traditional investigative tactic. Secondly, terrorists and their sponsoring organizations must conceal their illegal activities so that no one knows the act has taken place, or if the act is discovered, the act cannot be traced to terror. Finally, the perpetrator needs to obtain benefit (conversion) from committing the act. In the case of the terrorists, the funds must become available for unrestricted use to attract and retain the knowledge, skills, and abilities required to carry out terror acts. Like traditional fraud detection activities, fraud professionals and forensic accountants need to be observant, searching for accounting anomalies, internal control weaknesses, and lifestyle symptoms such as:

1. Movement of funds through the Cook Islands, Dominica, Egypt, Grenada, Guatemala, Hungary, Indonesia, Israel, Lebanon, Marshall Islands, Myanmar, Nauru, Nigeria, Niue, Philippines, Russia, St. Kitts and Nevis, St. Vincent and the Grenadines, and Ukraine.

2. Money flowing to foreign beneficiaries located in Persian Gulf States, particularly those known for state-sponsored terrorism.
3. The use of wire transfers for business activities that would not normally generate the wire transfer activity.
4. Financial activities inconsistent with the stated purpose of the business.
5. Financial activities not commensurate with the stated occupation of the individual.
6. The use of multiple accounts at a single bank with no apparent legitimate purpose.
7. Use of high-dollar currency and travelers' checks not commensurate with the business's purpose, or the individual's lifestyle or occupation.
8. The structuring of deposits at multiple branches of the same bank to avoid CTR (currency transaction reporting) requirements.
9. The use of false identities, documents, or "straw men."
10. Exploiting the privacy and secrecy benefits of sympathetic international jurisdictions.

Money Laundering

Money laundering is the disguising of the existence, nature, source, ownership, location, and/or the disposition of assets derived from criminal activity. More simply, money laundering is a ***PROCESS*** to make dirty money appear clean. The world is a smaller place due to technology and travel options. People and assets can move all over the world at almost any time with minimal legal restrictions, moving by air, land, and sea. Money, communications, and information can move even easier by traveling inside small fiber optic cables as pulses of electricity.

Fundamental to understanding money laundering is the need to define money. Money is "anything of value" that can be easily transferred from person to person and is such that most persons would accept it as an item of value or as a form of payment for goods, services, and debts owed. Money, or at least the concept of money as it applies to money laundering, can be currency, diamonds, gold, credit cards, money orders, stocks, bonds, cashier's checks, rare coins, wire transfers, gift cards, prepaid phone cards, debit cards, prepaid credit cards, etc. As long as it has value, is considered an acceptable form of payment, and is transferable among participants for a transaction it can be characterized as money.

The process of money laundering relies upon movement and takes place in three distinct stages:

Placement: The initial stage of money laundering involves placing it into the financial system. This stage requires some mechanism or vehicle for getting the money into the financial system without being noticed. At least three general methods are available for placement:

1. A cash-based or cash-heavy business can be integral to the placement stage of money laundering. Banks and other financial institutions are used to receiving large sums of cash from cash-based businesses. Restaurants, bars, laundromats, nightclubs, vending machine businesses, and check cashing businesses, as examples, operate with large amounts of cash and can be used as a means to place cash into the financial system through periodic deposits.
2. Structuring of cash deposits to fall under federal reporting guidelines can be a means of placing cash into the financial systems. Federal standards require that any cash deposit in excess of $10,000 to a financial institution be reported through a CTR. Furthermore, any cash payment to any business in excess of $10,000 must be reported to the federal government on a Form 8300. By structuring deposit transactions to be below the federal reporting guidelines, cash can be placed into the financial system.
3. Carrying the money offshore to a country with bank secrecy and privacy laws can be used to place the money into the worldwide financial system.

Once in the financial system, a paper trail (actually, an electronic trail) of the money and its movement begins. Most money laundering schemes are most vulnerable to detection at or before the placement stage.

Layering: Layering is the second stage and is used to hide or disguise the source of the money. An inherent goal of layering is concealment of the true source and business to business, account to account, etc. in an attempt to disguise the money source and confuse investigators because the amounts are no longer equal to those originally received. Furthermore, the transactions may have seemingly legitimate

business reasons and may even have paper documentation that lends seeming legitimacy to the nature of the transaction. Layering may involve foreign countries, especially those countries where bank secrecy and privacy laws make it difficult, if not impossible, for investigators to continue to follow the money trail. Once in a foreign locale with a strong commitment to bank secrecy, the money can be moved to another bank account, possibly in another country that also with strong bank secrecy laws, with complete anonymity. By this time, the funds are ready for the last stage of money laundering (integration). By using currency and offshore bank accounts, a perpetrator can make it almost impossible to follow any sort of money trail.

Integration: Integration, the third and final stage, is the attempt to convert the placed and layered money back into the hands of the perpetrator in a form that the perpetrator can use without risk of prosecution for being associated with dirty money. As examples, integration can take the form of payment for consulting services to a business or individual to which the perpetrator appears to have no association. Integration may take the form of a loan for which the repayment terms may range from legitimate to non-existent. Recall that even if the perpetrator repays the loan, he or she is only repaying the proceeds to their own business or bank account. The main issue with integration is ensuring that the source of the money and the transaction itself appears to be legitimate.

The good news for investigators is that perpetrators have two choices: spend money that they cannot show came from legitimate sources or launder the ill-gotten proceeds so that it appears that the sources of their money are legitimate. If necessary, some perpetrators may even pay taxes on laundered funds to further the appearance of legitimacy and make it appear that the perpetrator is a normal, tax-paying citizen. One nice attribute of money laundering is that ultimately the money must start and end at the same spot. Thus, if the investigator identifies the ultimate beneficiary, he or she knows that the same person is controlling the activity on the front end. Likewise, if the investigator identifies the source of the laundered funds, he or she knows who ultimately must benefit from the money laundering activity.

While the Bank Secrecy Act of 1970 improved the financial reporting and record keeping associated with cash transactions, the Money Laundering Control Act (MLCA) of 1986 was the first time that money laundering itself was considered a prosecutable offense. The MLCA has been amended over the years to strengthen the laws and eliminate various loopholes as follows:

- 1988—Anti-Drug Abuse Act
- 1992—Annunzio-Wylie Anti-Money Laundering Act
- 1994—Money Laundering Suppression Act
- 1996—Terrorism Prevention Act
- 1996—Health Insurance Portability and Accountability Act
- 2001—USA Patriot Act

In order to prove money laundering, the government must demonstrate (1) that a financial transaction was either attempted or conducted, (2) that the defendant knew that the proceeds derived from some unlawful act, (3) the property derived from a specified unlawful act, and (4) that the defendant attempted to accomplish one of the following objectives:

1. Promote a specified unlawful act (SUA).
2. Conceal the nature, source, location, ownership, or control the proceeds of a SUA.
3. Attempted to avoid federal reporting requirements (e.g., $10,000 for a CTR).
4. Attempted to evade taxes.

Furthermore, if the money laundering activity involves the international movement of money, the perpetrator can be charged with violation of international money laundering sections of the federal statutes.

One of the principal goals behind money laundering laws and regulations is that of seizure. The principle is consistent with that described earlier: to deprive the criminal of the use of their ill-gotten gains. The legal basis of the forfeiture is that the claim is made not against the alleged criminal, but against the property itself. Forfeiture requires probable cause that connects the property to an illegal act. The civil litigation threshold is a direct association between the criminal act and the property subject to seizure. In the criminal realm, courts will allow substitute property to be seized. Civil forfeiture funds are used to supplement the budgets of law enforcement agencies and are usually shared among the law enforcement agencies that participate in the investigation (providing an incentive to participate in a meaningful way).

Under federal law, all property involved in money laundering, as well as violations of the Bank Secrecy Act involving currency reporting, are forfeitable. To seize the funds of a money launderer, the federal government must be able to prove the elements of the money laundering offense. If money from a specifically unlawful act (SUA) is commingled with funds generated from legitimate sources, all of the funds are subject to confiscation. If the laundered money is then converted into other assets (e.g., stocks, bonds, homes, cars, etc.), the other assets are subject to forfeiture. Furthermore, if the other assets are in the names of persons other than those involved in the money laundering or criminal activity, the assets would still be subject to forfeiture. Criminal, civil, and administrative seizures are facilitated with a seizure warrant. In some cases where the property or its value may be at risk, a temporary restraining order may be obtained to prevent the transfer of title to the property or encumbering the property in some other manner.

Internationally, foreign countries have not always been as willing or able to attack money laundering in the manner in which it has been in the United States. In a post-9/11 world, more countries have started to cooperate in identifying and investigating money laundering activities. Some of the international commitment to anti-money laundering is demonstrated through such entities as the International Criminal Police Organization (INTERPOL) headquartered in France, the United Nations' Narcotics and Vienna Conventions, the British Commonwealth, which includes countries beyond Great Britain, a number of whom have been known as bank secrecy and tax havens, and the Organization of American States (OAS). In addition, the Financial Action Task Force (FATF), formed in July 1989 by the G7 (Britain, Canada, France, Germany, Italy, Japan, and the U.S.), the European community, and eight other nations analyzes international money laundering and makes recommendations for changes in banking and criminal laws. In recent years, the FATF also has started to investigate terrorism financing. The FATF has identified three times when money laundering is ripe for detection:

- Domestic entry into the financial system (placement)
- Transfers of fund abroad for the purposes of integration (layering)
- Transfers back to the originating country for repatriation (integration)

The Egmont Group is an association of financial intelligence units from around the world that share financial intelligence. Overall, it is now easier to obtain information from the international financial community than ever before. In addition, the United States is often able to gain or coerce assistance in the retrieval of moneys located in foreign lands. The mechanism for information sharing and money retrieval is the MLAT system or Mutual Legal Assistance Treaty.

Racketeering Influence and Corrupt Organizations Act (RICO)

Criminal organizations need a process to clean up their money. They also need an "organization" and bank accounts for money to enter the financial system and from which to initiate the money laundering placement stage. While money laundering is about the process used to make dirty money appear legitimate, RICO addresses the ***ORGANIZATIONS*** involved. Thus, RICO, enacted in 1970, the same year as the Bank Secrecy Act, is closely aligned to money laundering laws and regulations. While the original goal was to allow investigators to go after businesses and other entities involved in organized crime, it has been used to prosecute a wide variety of organizations including those associated with corrupt public officials, drug dealers, gangs, labor unions, and others.

Portions of the RICO Act outlaw:

- Investing illegal funds in another business
- The acquisition of a business through illegal acts
- The conduct of business affairs with illegal acts

Essentially, it is illegal for any person who has received funds that derived directly or indirectly from a pattern of racketeering to invest or acquire any other business that is involved in interstate or foreign commerce. It is also unlawful for persons involved in a racketeering activity to acquire or maintain any interest or control of any entity where the entity is involved in interstate or foreign commerce using illegal means such as fraud, extortion, bribery, or money laundering. Finally, a person employed by or associated with an entity involved in interstate or foreign commerce may not be involved in the operations of an enterprise's affairs in a pattern consistent with racketeering or the collection of unlawful debt.

RICO provides for criminal penalties up to $25,000 and twenty years in prison. Like the money laundering statutes, RICO also provides for the forfeiture of assets used in racketeering crimes and permits

treble damages in civil cases. Individuals, corporations, and loosely organized "entities" may be prosecuted civilly and criminally under the RICO statutes. Racketeering acts include:

- Violent crimes such as kidnapping, murder, arson, and robbery
- Other felonies such as unlawful gambling, bribery, extortion, the distribution of obscene material, and controlled substance trafficking
- Violations of money laundering laws
- Violations of the Bank Secrecy Act
- Mail and wire fraud
- Labor offenses
- Securities fraud

RICO and the money laundering statutes are somewhat circular in that money laundering laws and regulation identify RICO violations as a SUA and RICO specifically names money laundering as a RICO offense.

Conspiracy

As noted above, criminals in complex crimes, frauds, and financial activities require a process, money laundering, to clean up their funds and require entities as a means of accomplishing their operational goals, laundering money, and as an integration option. The organizations and the money laundering process also require individual participants. Whereas money laundering statutes go after the process and RICO goes after the organizations, conspiracy targets the individuals involved in the illegal activity. Thus, conspiracy deals with the ***PEOPLE***.

A conspiracy involves three elements:

1. The coconspirators must have an agreement (actus reus) between them.
2. The coconspirators must act or demonstrate an inclination to commit a crime.
3. The participants must mentally commit to the act through their state of mind (mens rea or intent).

From a practical perspective, prosecutors need to prove:

1. The existence of a conspiracy.
2. Willing participation in the conspiracy.
3. The defendant's knowledge of the conspiracy.
4. At least one overt act was completed in carrying out the conspiracy.

Independent acts toward common criminal purpose may be linked together as a single conspiracy. Related to money laundering, conspiracy may be involved assuming that the coconspirator knew that the funds were coming from at least one specified unlawful activity. Conspiracy is also a specifically prohibited conduct under RICO.

The acts and statements of one coconspirator may be admissible against others involved in the conspiracy. Thus, lawyers and prosecutors will use conspiracy as a means of linking persons together and obtaining convictions of each of the coconspirators related to the underlying offense. The overt act required to prosecute conspiracy need not be illegal itself and may seem innocuous, such as sending an email or making a phone call, as long as the act is integral to the conspiratorial activity. While conspiracy charges have far-reaching implications, an entity and its employee cannot be coconspirators because they are legally viewed as one. However, an entity may conspire with another entity or with independent, third-party individuals.

USA Patriot Act

The USA Patriot Act is formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. Terrorism, like many crimes, is rooted in money. Money provides control, operating funds, and the means to acquire and maintain infrastructure. It is not coincidental that the 9/11 attacks chose to target Washington, D.C., the political hub of the United States and also to target New York, the U.S. financial center. At least one of the goals for targeting New York was to disrupt the international financial markets and wreak havoc on the American and Western economies worldwide.

Title III of the USA Patriot Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. Overall, the Patriot Act identified new types of money laundering crimes and increased the penalties associated with them. Specifically, the Patriot Act outlaws money laundering as follows:

- Funds generated from foreign crimes of violence or political corruption
- Funds generated from cybercrime
- Funds generated from offenses related to supporting terrorist organizations
- Funds related to bulk cash smuggling

In addition, the Patriot Act sets out the procedure for the forfeiture of bulk cash that had been smuggled. The felony penalty for bulk cash smuggling is five years. The anti-money laundering provisions of the Patriot Act supplement those discussed above. The Act also eliminated a prior requirement that the defendant knew that the proceeds being laundered had been generated from illegal business operations. Furthermore, the attempted transport of more than $10,000 in currency or monetary instruments into or out of the country is illegal if the funds are concealed and the transporter was attempting to avoid the U.S. federal reporting requirements.

The Patriot Act is particularly aggressive on the forfeiture of assets related to terrorism. The Act permits the confiscation of all property of an individual or entity who participates in the planning of a terrorist attack. Furthermore, any proceeds used to facilitate an act of terrorism or derived from a terrorist act are subject to forfeiture. If an individual or entity has assets in a foreign country and U.S. officials are unable to obtain those funds, the Patriot Act allows the seizure of funds from any correspondent banks where the terror organization has correspondent bank accounts. These provisions provide a significant incentive for financial institutions to avoid transactions associated with terrorists.

One of the techniques of terrorists and others interested in money laundering is to utilize shell banks, or banks that have no physical presence in any jurisdiction. The USA Patriot Act prohibits U.S. financial institutions from allowing correspondent account transactions with shell banks. The USA Patriot Act also increased the availability of banking records to investigators, increased due diligence requirements for banks, and established standards for customer identity verification. U.S. financial institutions are also required to have anti-money laundering programs in place. The U.S. Department of Justice has reported a number of successes as a result of the money laundering regulations that were improved by the USA Patriot Act, and these successes go beyond terrorism and terrorism financing to include the capture of fugitives, the prosecution of child pornography, the dismantling of complex cybercrime schemes, and the prosecution of drug and illegal weapons traffickers.

The Bank Secrecy Act

Like RICO, the Bank Secrecy Act (BSA) was passed in 1970 to assist in the investigation of illegal acts associated with drug trafficking and tax evasion. The BSA requires that financial institutions maintain adequate records and that financial institutions report certain types of transactions to the federal government. Any currency transaction in excess of $10,000 must be reported to the Department of the Treasury on IRS Form 4789, or the Currency Transaction Report (CTR). In addition, financial institutions may also report other transactions when the nature of the financial transactions or the activities of the persons involved appears to be suspicious. Such transactions or activities are reported on the Suspicious Activity Report (SAR). Because the CTR reporting requirements are more specific, the number of submissions tends to far exceed those of the SAR. In addition to financial institutions, businesses whose customers initiate transactions with more than $10,000 in currency and coin are required to file an IRS Form 8300. This form was originally designed to identify potential tax evaders and thus, the information was maintained within and only utilized by the IRS. Subsequent to 9/11, however, the information disclosed on Form 8300 has been made more widely available to law enforcement. The data from these submissions is collected and disseminated by the Financial Crimes Enforcement Network, otherwise known as FinCen.

Beyond the CTRs, SARs, and Form 8300s, the BSA has the following additional reporting requirements:

- The movement of more than $10,000 into or out of the United States must be filed on FinCen Form 105, Report of International Transportation of Currency or Monetary Instruments. Monetary instruments include negotiable checks, travelers' checks, and bearer money equivalents

- The CTRC must be filed by casinos (the "C" tacked on to the end of CTR) when a person conducts a transaction in more than $10,000 in currency. Casinos are known for their elaborate and sophisticated surveillance methods and have the ability to track suspicious transactions
- The FBAR requires that each U.S. person who has a foreign bank account report its existence on Treasury Form 90-22.1, or Foreign Bank Account Report
- Any person who owns or controls a money transmitting business must register that business within 180 days of its creation. These businesses are required to maintain records and obtain customer identification for transactions in excess of $3,000, including the person's name, address, passport number or taxpayer identification number, transaction date, amount, currency names, country, and total amount of each type of currency

The BSA attacks the placement stage of the money laundering process. It is at this stage where the money launderer is most vulnerable because they have control over funds from unexplained sources. Once the money launderer starts layering and integrating the proceeds, money laundering is difficult to identify because the true source of the funds has been concealed.

Mail Fraud

Mail fraud statutes may be invoked any time that a scheme to defraud someone has been devised by false or fraudulent pretenses, representations, or promises and such fraud takes place in any U.S. Post Office, U.S. mail depository, or through transport by the U.S. Postal Service. The person needs only to cause the mail service to be used to facilitate the fraud act, and the item sent or delivered may be transported by private or commercial carrier in furtherance of the fraud act. The violation is punishable by not more than a fine of $1,000,000 and imprisonment of up to thirty years. Thus, any time that the mail is used to facilitate a fraud, no matter how large or small a part the mail aspect may be, mail fraud may have been committed. Mail fraud is one of the workhorses of federal white-collar prosecutions and is available among other offenses to investigate and prosecute complex frauds and financial crimes. As an example, a person who mails a fraudulent tax return to the Internal Revenue Service has not only committed tax fraud but also committed a mail fraud offense. The mailing itself does not need to contain any fraudulent representation but must be integral to the overall fraud scheme. The scheme does not need to succeed or the intended victim suffer any loss for the mail fraud statute to be applicable.

Wire Fraud

While mail fraud occurs when a fraudster or other criminal utilizes the various mail services to facilitate a fraud, the use of wire, radio, or television to communicate false or fraudulent pretenses, representations, or promises is a violation called wire fraud. Unlike mail fraud, the electronic transmission must be associated with interstate or foreign commerce for wire fraud statutes to apply. The electronic communications may be writings, signs, signals, pictures, or sounds used to further the fraud scheme. Like mail fraud, a wire fraud violation is punishable by not more than a fine of $1,000,000 and up to thirty years of imprisonment.

THE U.S. BANKING SYSTEM

The banking system in the United States provides a number of services including mortgages, secured property loans (e.g., cars, recreational vehicles, trucks, boats, etc.), secured cash loans, credit cards, personal lines of credit, business loans, business lines of credit, letters of credit for overseas transactions, student loans, overdraft protection options, home equity loans, demand deposit accounts, time deposits, check writing and cashing services, periodic account statements, cashiers' checks, certified checks, money orders, bank drafts, travelers' checks, and exchanges documents. Banks also facilitate currency exchanges, have trust department services, and provide personal banking services for high net worth individuals.

The benefit of the U.S. banking system is that everything is written down and most transactions and their backup documentation are captured on microfiche or some form of electronic imaging. Loan applications are the initiating point for bank loans. The bank then evaluates the applicant's ability to repay the loan (debt capacity), the person's willingness to repay the loan (character), the collateral offered by the borrower (if any), and other conditions such as the borrower's employment history, prior loan experience with the type of loan sought, the overall economy, and any other conditions that might be applicable. As part of evaluating capacity to repay, the lending institution will obtain a credit report on the prospective borrower, prior tax returns, borrower W-2s and pay stubs, borrower investment statements, and other

borrower financial records. As such, the loan application file has a wealth of financial information included. Once the loan is approved, the loan documents are signed, and funds are transferred, the financial institution maintains meticulous records concerning repayment. If an investigator is able to obtain a subpoena for the loan records, these should be reviewed carefully not only for the financial information but also for leads to other individuals, accounts, businesses, etc.

Banking records for regular checking accounts owned by individuals and entities also contain a wealth of information. The signature card contains the names, Social Security numbers, and signatures of all persons able to withdrawal funds from the account. The initial deposit may be an employment check or a check drawn on another account. In either case, this information can be quite valuable. Once the account is opened, the detailed activity can be analyzed from the monthly statement and supporting documentation that accompanies that statement to develop patterns of spending habits, a profile on the account holder, the financial condition of the account holder, changes in activity patterns, and the timing of those changes. All of this information can be useful during an investigation. The depository activity should also be analyzed. Deposits may come from employers, in the form of cash, from investment accounts, friends, businesses, business associates, ATM deposits, wire transfers, mail, and other sources within the bank. While each of these may hold important clues and linkages to businesses, people, and places, wire transfers, particularly those into and out of the country, should warrant special attention.The check itself may contain valuable information.

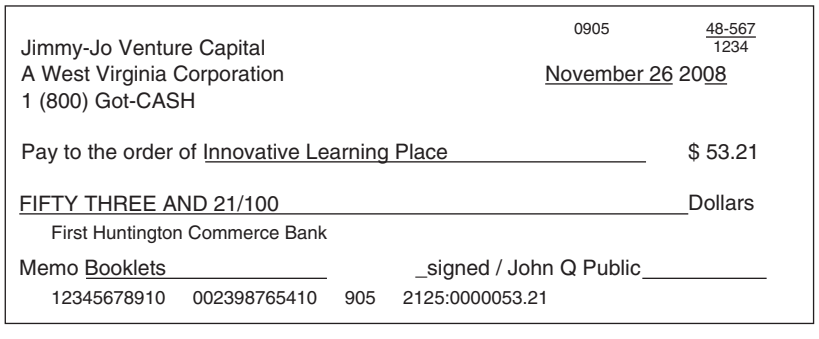
In the example in Figure 4-1, the 0905 is the check number that also appears on the bottom line. The 48–567 over the 1234 is a code that identifies the issuing bank. The numbers above the line, 48–567 are the ABA (American Bankers Association) transit number: the first number, 48, represents the state where the bank is located and the second, 567, is a code that ties to the issuing bank's name. The number below the line with the numbers 1234 is the Federal Reserve Routing Code: the first two digits represent the Federal Reserve District, the third number identifies the District Office, and last digit indicates when the cash proceeds should be made available, assuming that the issuing account has sufficient funds. The payee is Innovative Learning Place. The amount or face value of the instrument is $53.21. The paying bank is First Huntington Commerce Bank. The following string of numbers are magnetic ink character recognition or MICR numbers:

12345678910 002398765410 905 2125 : 0000053.21

12345678910 is a combination check routing number (1234) and, ABA transit number (567 plus 8910). The numbers 002398765410 represent the checking account number of Jimmy–Jo Venture Capital. The number 905 is the check number in MICR format. The number 2125 is the process code and the number 0000053.21 represents the check amount or face value.

Check 21, Check Clearing for the 21st Century Act, went into effect on October 28, 2004. This Act effectively allows the first bank to touch a check to image the front and bank of the check and then shred the original. Investigators will have access to the electronic images that can serve as evidence. The check is then processed almost instantly. With the advent of efficient and effective EFT (electronic funds transfer), electronic payment via the Internet, and debit cards, the paper check will become scarce over time. Although the backs of checks will change, the front of paper checks will contain the same information under Check 21 as they have in the past. The items reviewed above may provide valuable clues such as connections between individuals, businesses, and physical locations as well as other clues. This information should be carefully evaluated to further the investigation.

Cashiers' checks, money orders, and travelers' checks are favorites of money launderers. Once purchased, these monetary instruments facilitate the easy movement of large sums of money. Cashiers' checks,



0905 48-567/1234

Jimmy-Jo Venture Capital
A West Virginia Corporation
1 (800) Got-CASH

November 26 2008

Pay to the order of Innovative Learning Place $ 53.21

FIFTY THREE AND 21/100 Dollars

First Huntington Commerce Bank

Memo Booklets _signed / John Q Public

12345678910 002398765410 905 2125:0000053.21

FIGURE 4-1 Sample Check

money orders, and travelers' checks are very transportable and are accepted by most financial institutions. The primary drawback is that the initial transaction has a significant amount of documentation with it.

Cashiers' checks are often used as a down payment for big–ticket items such as homes, cars, boats, etc. Despite the amount of documentation available, because the check is tied to a bank's checking account instead of that of an individual, the tracing of these instruments can be complicated. Cashiers' checks come with three copies, the original check (top copy), a copy for the bank's records, and a copy for the customer. In addition, the bank teller logs the check in a ledger. If the acquisition involves cash greater than $3,000, that fact will be noted in the log. Cash in excess of $10,000 generates a CTR. If the proceeds are generated from the customer's bank account, tracing the check becomes a little easier. If the goal of the investigator is to identify all checks with the customer's name associated with it, the bank will usually require the branch name and the approximate date as a starting point. Because the only record is the log or ledger, tracing cashiers' checks can be difficult.

Money orders typically have limited dollar amounts. For example, at the U.S. Post Office the largest money order is $700. Travelers' checks can be traced only by serial number, so the investigator needs a starting point there as well. Otherwise, tracing travelers' checks can be very difficult. Bank customers may also rent a safe deposit box. Banks have no means of knowing the contents of these boxes, and access is strictly limited. An investigator cannot gain access without the use of a search warrant. The safe deposit box records include a rental application, and the bank keeps detailed record of access to the box including the date, time in, time out, and the person signing in.

Investigators may run across a number of different types of banks. Commercial banks are those most persons are familiar with. Other persons have accounts at federal savings banks (also known as savings and loan banks). Savings and loans got into significant financial trouble in the 1970s and 80s by speculating in commercial real estate. Since that time, regulation of these banks has been changed to avoid a similar crisis.

Offshore banks exist in foreign countries. It is not uncommon for high net worth U.S. citizens to bank internationally to take advantage of the various banking and tax laws. Criminal types, however, often attempt to exploit the secrecy laws of other countries' banking systems to hide their own nefarious activities, including money laundering. An investment bank underwrites the securities of companies issuing stocks and bonds to investors. The investment banker buys the securities and then resells them to the investing public at a preordained date.

Private banks are established by individuals and businesses to facilitate transactions. Many U.S. banks offer private banking to high net worth individuals. Private banking arrangements often come with various privileges and services not provided to regular clientele.

Central banks, such as the U.S. Federal Reserve, are responsible for maintaining and protecting the country's currency. Correspondent banks provide banking services for another bank's customers where the other bank does not have a local branch operation or other physical presence. Cyber banks are available on the Internet. Other banking arrangements include credit unions, auto finance companies, bank holding companies, and securities brokerages.

Businesses competing internationally will usually require international banking services as well as those located domestically. Typically, international banking customers do so for privacy reasons, to enhance security (especially true for unstable countries and their local banking options), convenience, and financial benefits such as tax breaks, better interest rates, longer float, etc.

MOVING MONEY INTERNATIONALLY

In order to transact business internationally, most companies also need to issue forms of payment that complement normal check disbursements through the domestic checking account. Some businesses located in foreign locales require cash payments in advance. This cash flow timing is advantageous for the provider of goods and services but has the potential to put the buyer in a cash flow crunch. As a substitute for cash in advance, some providers of goods and services accept documentary letters of credit. This is a common form of international payment because both the buyer and seller are afforded some protection.

The bank operates as the honest third-party broker. The bank essentially guarantees the provider of goods and services payment, assuming contractual performance as soon as the buyer confirms that the terms and conditions have been met. In advance of the transaction, the buyer specifies the documentation required in order for the seller to be paid. Such details may be the subject of negotiation between seller and buyer. Once the goods and services have been provided, the seller provides the required documentation to

the bank, including the sign-off of third-party shippers and other agents to the transaction. Upon receipt of the documentation, funds are transferred from the buyer to the seller as agreed upon in the contract. The documentation typically includes a bill of lading issued by the transporter, a certificate of inspection by an agent of the buyer, certificate of manufacture by the seller, certificate of origin, commercial invoice, the draft bill of exchange, a copy of the export license of the seller, the buyer's import license, and any insurance documents required as part of the transaction.

Documentary collection, a third form of international payment, is similar to domestic cash on demand (C.O.D.). Essentially, title for goods purchased is held until payment is made. Upon payment to the seller, the intermediary bank provides the documentation to the buyer. Because this is a documents-only transaction, the buyer has little protection against poor quality. Open account is the fourth international payment method and is virtually the opposite of cash in advance; under this arrangement, the seller is at risk until the buyer pays.

Trillions of dollars move around the world every day. The knowledge of how much money flows also indicates the difficulty that persons engaged in anti–money laundering activities face. Most of the trillions of dollars in money movement are legitimate. The number of transactions and relative dollars that are associated with money laundering are relatively few in number and small in amount (estimated to be 1 percent or less of all international movements). This money moves around the world electronically, in the form of electronic funds transfer (EFT). Cyber banking, smart cards, prepaid phone, debit, credit, and gifts cards and other similar methods for the movement of money will only ensure that the amount of money moving around the world increases as time goes by. As examples, electronic money flows are engaged by banks, businesses, credit card companies, money transmitters, governments, investment brokerages, stock exchanges, and commodity dealers.

Any electronic transmitter of money located in the United States must register with FinCen as a money services business (MSB). Money transmitters can be large, such as American Express, CitiBank, Bank of America, or can be relatively small businesses. Transmitters use a messaging system. The message communicates that money has been received on one end of a transaction and is available at some other place around the world for pickup. Typically, the person picking up the money must identify himself by name or some other security measure. The transmitters who facilitate the transaction for their customers collect a fee for their service. Federal law requires identification by the customer if the transfer involves cash in excess of $3,000. A CTR is required for cash transfers in excess of $10,000. Because of the ease and speed of movement and relative anonymity, electronic funds transfer around the world is a favorite tool for use by money launderers.

In addition to relatively small money transmitters, three systems exist for major money movement. First, Fedwire is the primary mechanism for domestic wire transfers in the United States and connects all of the twelve Federal Reserve Banks in the United States and approximately 12,000 domestic financial institutions. Fedwire may process 300,000 transactions a day, encompassing hundreds of billions of dollars. The second system involved in electronic funds transfer is the Clearing House Interbank Payments System (CHIPS). CHIPS serves as the main EFT system for processing international electronic transfers of money. CHIPS handles almost a trillion dollars a day in transfers among over 130 banks in more than thirty countries. CHIPS fund transfers are supported by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT is the messaging system that handles the communications by banks that accompany most CHIPS transactions. SWIFT is analogous to an email system. The messages over SWIFT initiate most of the transfers made with the CHIPS system. Telex provides a similar system to SWIFT to which businesses can subscribe.

Numerous records are generated with an electronic funds transfer. First, the person requesting the transfer must complete a transfer request. At the completion of the transactions, a confirmation is generated. In addition, debit and credit memos and various other documents, logs, and ledger transactions are created during the transaction.

In addition to the formal bank systems, domestic and international, informal arrangements exist as well. Hawala is an informal banking system originally created to support immigrants located around the world. Hawala (meaning "trust") allows transfers of money between individuals with no record of the transaction. This money transmittal system is international, informal, and unregulated. A person that wants to move money goes to his local contact and gives the money to the person, as well as instructions concerning who will collect the funds at the destination. The local Hawala representative then makes a call to his contact at the destination and communicates the instructions for collection. The Hawala representative at the destination then provides the funds to the recipient. Of course, the Hawala representatives collect fees for their services. The Hawala system is based on trust and is fast, efficient, unregulated, and maintains

almost no paperwork so the transactions are made in a relative vacuum. The value of such a system to money launderers cannot be overemphasized.

To investigate money movement through wire transfer, the investigator generally needs a lead and a customer bank account. Thus, the focus is on the beginning point of the wire transfer. From there, the investigator can obtain a subpoena and visit local branches to determine whether such movement has taken place. The data gathered, if found, should include the name and address of the originator, the amount, date, remittance instructions, the beneficiary, the recipient bank, and any other pertinent information captured during the transaction.

OTHER COMPLEX FRAUDS AND FINANCIAL CRIMES

Tax Evasion and Fraud

The Internal Revenue Service (IRS) is responsible for determining, assessing, and collecting taxes imposed by Congress. The IRS is divided into four major divisions:

- Wages and Investment
- Small Business/Self-Employed, including Excise Taxes
- Large and Mid-size Business Division (in excess of $10 million in assets)
- Tax-exempt and Governmental Entities

The IRS also has smaller divisions that deal with appeals, communications, and liaisons and criminal investigations. The Criminal Investigations Division (CID) is the law enforcement arm of the IRS. The IRS has responsibility for a number of taxes imposed by Congress including personal income taxes, corporate income taxes, employment taxes, including FICA (Social Security), Medicare, and federal unemployment tax (FUTA), excise taxes, and estate and gift taxes. In addition to federal income taxes, states, counties, cities, and other municipalities also assess and collect taxes including personal income taxes, corporate income taxes, state unemployment taxes, personal property taxes, sales and use taxes, and other taxes as required by those jurisdictions.

The primary distinction in whether an individual or entity has committed tax fraud or simply committed an error is the intent of the individual. The intent of the party to the tax return will determine the difference between tax errors and tax evasion. Tax avoidance consists of using legal means and methodology to minimize taxes within the existing framework of tax rules and regulations. Tax evasion is the intentional wrongdoing to evade taxes believed to be owed. Tax evasion is fraud and implies bad faith, intentional wrongdoing, and a sinister motive.[3] One defense against tax fraud is an objectively reasonable "good faith" misunderstanding of the law. The belief that taxes are unconstitutional is not considered objectively reasonable. Thus, tax evasion (fraud) requires an intentional wrongful doing with the specific purpose of evading a tax known or believed to be owed. Furthermore, tax fraud requires that the defendant have taxes owing, and evasion requires at least one "affirmative act" to demonstrate intent. Affirmative Acts are compelling and are actions that establish intent (deliberate action), often focusing on concealment. Common tax evasion schemes include:

- Deliberate understatement of taxes owed
- The omission of taxable transactions and activities
- Fictitious events and activities
- Hidden events and activities
- False statements made to tax agents
- False documentation to support fraudulent tax filings

Examples of affirmative acts include the following:[4]

- Deceit—Lying when giving statements
- Subterfuge—An artifice to hide an act (evade a rule)
- Camouflage—To hide
- Concealment—To hide
- Coloring events to making them appear different
- Obscuring events to making them appear different

In contrast to affirmative acts, affirmative indicators are not deemed compelling in and of themselves, but are considered badges of fraud, red flags, symptoms, or signs of potential fraudulent conduct. Badges of fraud arise in a number of areas:

- Actions of the Taxpayer:[5]
  - Previous tax filings but the taxpayer stops without reasonable cause
  - The taxpayer correctly classifies transactions for some suppliers/vendors but not for others (e.g., unusual source)
  - Taxes have been passed on to customer but not reported or paid
  - The taxpayer handles identical products but considers one to be taxable and the other nontaxable
- The Treatment of Income:[6]
  - Omissions of specific revenue sources
  - Omission of revenues from specific products
  - Omission of revenues from product lines
  - Omissions of entire sources of revenue
  - Unexplained failure to report revenue
- The Treatment of the Books and Records:[7]
  - Two sets of books and records
  - False entries or alterations
  - Backdated or postdated documents and transactions
  - False invoices
  - False applications
  - False financial statements
  - Invoice numbers that do not make sense
  - Failure to keep and maintain records
  - Concealment of records
  - Refusal to make records available
  - Unexplained variances between returns and the underlying books and records
- Related Parties[8]
- Conduct of Taxpayer:[9]
  - False statements
  - Interference with tax agent's examination
  - Failure to follow the advice of attorneys/accountants
  - Less than full disclosure
  - Taxpayer knowledge (e.g., taxpayer has an accounting degree)
  - Testimony of employees or other unrelated third-party individuals
  - Destruction of books and records
  - Transfer of assets to conceal their true nature or their ownership
  - Patterns inconsistent over time
  - Attempts to bribe the examiner

The process of investigating tax fraud starts with first indications (badges of fraud) and concludes with either a finding of no fraud or a finding of tax evasion due to the presence of affirmative act(s). Consistent with other fraud examinations, when attempting to prove intent, investigators may find it helpful to consider the following:

- Present evidence in chronological order, particularly examining the timing of key transactions
- Identify altered, concealed, or destroyed documents or evidence (e.g., deliberate backdating)
- Carefully record false statements by the taxpayers

- Look for pattern or repetition of suspicious behavior
- Obtain the testimony of coconspirator
- Obtain a confession from the taxpayer

If predication exists that tax fraud may be present, the following is a seven-step process to convincingly resolve any badges of fraud.[10]

Step 1—Consider the risk of fraud by brainstorming, considering how and where tax return information might be susceptible to fraud, how and where tax return fraud might be hidden, and exercising professional skepticism.

Step 2—Obtain information needed to identify the risk of fraud by interviewing owners, management, internal auditors, and clerks, and carefully documenting their statements, considering the results of analytical and preliminary examination procedures and any other observed badges of fraud.

Step 3—Consider policies, procedures, and controls in place to prevent fraud by understanding the internal control environment; evaluating whether policies, programs, and controls are operational; evaluating whether policies, programs, and controls address the identified risks of fraud; and drawing conclusions about the risk of fraud.

Step 4—Respond to the results of the risk assessment steps. Specifically, as the risk of fraud increases, the agent or criminal investigator should respond with more creative procedures and investigative techniques, utilize more nonfinancial performance metrics, consider the need to gather additional evidence, and consider altering the nature and extent of examination procedures.

Step 5—Evaluate the evidence by continually assessing the risk of fraud throughout the examination, evaluating results of analytical and examination procedures performed, and reevaluate the risk of fraud near completion of fieldwork.

Step 6—Draw conclusions by obtaining taxpayer explanations for errors, misstatements, omissions, and other irregularities, corroborating explanations, and making any necessary judgments. Step 6 may need to be completed in concert with the investigator's manager or one of the IRS's Fraud Technical Advisors.

Step 7—Communicate about the tax evasion (fraud) by making sure that all aspects of the investigation have been properly documented, and write the required reports. After consultation with a Fraud Technical Advisor, the investigator prepares an IRS Form 2797 (Referral Report of Potential Criminal Fraud Cases) that includes a detailed factual presentation including:

- Affirmative acts
- Taxpayer's explanation
- Estimated criminal tax liability
- Method of proof used to determine taxes owed

When an examiner discovers failure to file, he or she must document the affected taxable periods, the explanations of the taxpayer, and determine if badges of fraud exist. Investigators should be careful about accepting the taxpayer's assertions or explanations without grounding the statements in the evidence.

Like other frauds, the burden of proof falls on the investigating agent. Tax-evading persons can be pursued civilly or criminally. The primary determinant is what the investigating agent and their supervisors and managers believe that they can prove. Civil cases never rise to the level of overtly deliberate acts to evade taxes, and criminal cases involve behavior deemed too deliberate to be dealt with civilly. For example, the failure to cooperate or the maintenance of two sets of books and records might be considered so egregious that criminal pursuit is the only proper disposition.

Taxpayers have several defenses that should be evaluated as the investigator winds up his or her investigation. First, the taxpayer may argue that no taxes are due. Second, the taxpayer may claim that their scheme was set up to avoid rather than evade taxes owed. Third, the taxpayer may claim that the unpaid taxes were based on an objectively reasonable position based on a reasonable evaluation of the tax law, regulations, and prior court findings. Fourth, related to taxable revenues, the taxpayer may claim that they did not have unrestricted access or rights to the funds. Other defenses that may be presented and need to be evaluated include the mental competence and capacity of the taxpayer, the competence of paid bookkeeping services, ignorance of a complicated tax law, the innocent spouse defense, and reliance on an accountant or attorney. The innocent spouse defense is particularly applicable now that returns can be filed electronically without the signature of all parties to the return.

Bankruptcy Fraud

All bankruptcy cases are filed in federal court at the local district of the U.S. Bankruptcy Court. The Office of the Trustee, within the Department of Justice, is responsible for administering bankruptcy cases including appointing trustees, examiners, 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. Within the Office of the Trustee, special investigative units investigate criminal referrals and complaints in bankruptcy cases. These units sometimes work with the Internal Revenue Service and FBI when the circumstances warrant cooperation as well as when jurisdictional issues arise.

Examiners are sometimes appointed in reorganization (Chapter 11) bankruptcy cases, particularly when assertions of fraud and misconduct by the debtor in possession have been alleged. In reorganization, the debtor in possession's primary goal is to preserve and protect the assets and operations while the plan of reorganization is developed and subsequently confirmed by the bankruptcy judge. Secured and unsecured creditors hold claims against the bankrupt entity. Secured creditors hold some claim of collateral, which acts to protect the value of their claim against the bankrupt entity. Because security claims are typically filed at the state level (e.g., UCC (uniform commercial code) filing), the bankruptcy court must examine and rely on state law to determine the validity of secured claims against collateral. At the time of the bankruptcy filing, an automatic stay precludes any creditor, secured or otherwise, from taking any action detrimental to the health and well–being of the bankrupt entity. When the bankrupt estate is settled, secured creditors' claims have priority over those of the unsecured creditors.

The bankruptcy code of the United States has several chapters:

- Chapter 1 contains general provisions
- Chapter 3 provides guidelines for bankruptcy case administration
- Chapter 5 establishes the rights and obligations of the creditors, debtors, and the estate
- Chapter 7 deals with the liquidation of the debtor's assets, including individuals and businesses
- Chapter 9 applies to municipalities
- Chapter 11 contains provisions for those debtors hoping to reorganize and emerge from bankruptcy
- Chapter 12 is designed to address the needs of farmers and fishermen
- Chapter 13 contains reorganization bankruptcy provisions for high net worth individuals who cannot qualify for Chapter 7 liquidation.

The bankruptcy court has the right to appoint a trustee in cases where there are claims of fraud, dishonesty, incompetence, or gross mismanagement if such appointment is in the best interest of the creditors, equity holders, and others with an interest in the estate. When a trustee is appointed, allegations of fraud and gross misconduct often underlie the appointment. In Chapter 7 cases, the trustee must investigate the affairs of the debtor. In Chapter 11, the duties and responsibilities are more far-reaching and include taking control of the business and making operational decisions.

One of the roles of the trustee is to attempt to identify missing assets and locate them, if possible. To do so, the trustee normally has access to the bankrupt entity's attorneys as well as the accountants and their work papers, tax returns, and client books and records. To fulfill their fiduciary responsibilities, the trustee may need to gather information, not only from the bankrupt entity's books and records, but also from banks, customers, related parties, suppliers, employees, pension funds, and others as needed. Once gathered, the trustee may consider the following investigative procedures:[11]

- Reconstruct cash receipts and disbursements journals and general ledgers
- Identify new bank accounts, related party transactions, and hidden or concealed assets
- Take depositions of uncooperative witnesses
- Take depositions of third-party witnesses and others who can authenticate and corroborate documents, records, transactions, and other information
- Take declaration testimony from cooperative witnesses
- Interview witnesses
- Prepare an investigative report
- Submit a copy of the report to the U.S. Attorney's Office if allegations of fraud appear justified

Bankruptcy crimes are investigated by the FBI and prosecuted by the U.S. Attorney's Office, if warranted. The penalty for each bankruptcy offense is a fine of up to $500,000 and imprisonment for up to 5 years, or both. Title 18 of the U.S. code identifies nine offenses:

Paragraph 1—Knowingly and fraudulently concealing property from a custodian, trustee, marshal, or other officer of the court. Property is defined not only as assets, but also as books, records, and anything of value.

Paragraph 2—Knowingly and fraudulently giving false oath or account, including oral testimony during depositions, hearings, and trials.

Paragraph 3—Knowingly and fraudulently giving false declarations, certifications, verifications, or statements, including written documents such as the debtor's petition, bankruptcy schedules, statement of affairs, interim statements, operating reports, and declarations in court such as court filings and motions.

Paragraph 4—Knowingly and fraudulently giving false proof of claims against the bankruptcy estate by creditors, agents, attorneys, or others on behalf of a claimant.

Paragraph 5—Knowingly and fraudulently receiving any material amount of property from the bankruptcy estate, including creditors or any other person.

Paragraph 6—Knowingly and fraudulently giving, offering, receiving, or attempting to obtain money, property, remuneration, compensation, reward, advantage, or promises for acting or agreeing not to act, including the bribery or attempted bribery of a court official.

Paragraph 7—Knowingly and fraudulently transferring or concealing any property in contemplation of a bankruptcy filing (i.e., pre-bankruptcy actions).

Paragraph 8—Knowingly and fraudulently destroying and altering documents during or in contemplation of a bankruptcy filing, including concealing, mutilating, falsifying, or making false entries in the books, records, documents, or papers relating to the bankrupt estate's property or financial affairs.

Paragraph 9—Knowingly and fraudulently withholding books, records, documents, or papers relating to the bankrupt estate's property or financial affairs from a custodian, trustee, marshal, or other officer of the court.

Title 18 also outlaws embezzlement against the estate. Bankruptcy fraud includes schemes to file a false bankruptcy petition, file documents during a proceeding, or make false or fraudulent statements, representations, claims, or promises before or after the filing of a bankruptcy petition. This applies not only to the actions of debtors and claimants during a legitimate bankruptcy, but also to the efforts of perpetrators to use bankruptcy as part of a scheme to defraud others, such as a bust-out scheme. Common bankruptcy schemes include concealing assets (most common), the planned bust-out, multiple voluntary bankruptcy filings, the credit card bust-out, forged filings, and filings by petition mills on behalf of unsuspecting clients. The planned bust-out includes the setting up of a seemingly legitimate business, buying goods on credit, selling those goods, closing the business, and disappearing while leaving the creditors unpaid. The credit card version is similar except the fraud beneficiary is the individual cardholder instead of the business.

FROM THE FRAUDSTER'S PERSPECTIVE

Adapted from the whitecollarfraud.com blog by Sam E. Antar
Tuesday, October 16, 2007

A Warning to Wall Street Analysts from a Convicted Felon

To Wall Street Analysts:

During my years at Crazy Eddie, I found that securities analysts often did not know how to ask intelligent questions. When they asked intelligent questions, they did not know how to formulate the proper followup questions to our deceptive answers. Most Wall Street analysts were too trusting of the answers that they received from us.

Good questioning will often result in irritable behavior from company management. However, you are not doing your job to be in management's good graces. Your job is to obtain not readily apparent facts, analyze them properly, and communicate them accurately and effectively to your readers. Top-notch financial journalist Herb Greenberg advises that you consider "what many companies don't say as they spin the story their way."

For example, be careful of corporate managements that

- accentuate positive information and spin and deflect negative information
- blame others for their company's problems
- attempt to intimidate you

Beware of companies that exclude critics and provide "selective" access to management. Too often, Wall Street

analysts in their quest to gain access to management end up corrupting their required professional skepticism and cynicism. I played this game very well with Wall Street analysts, as the CFO of Crazy Eddie.

It's not about gaining access at the cost of your professional integrity. It's about understanding what is really happening and communicating it accurately and effectively to your readers.

I played you analysts very well by rewarding you with selective access as the CFO of Crazy Eddie. I had you eating out of my hand with "selective" disclosures and "favored" access. While you craved for access and wrote your glowing reports in gratitude for your coveted access, you unwittingly helped make the frauds that we perpetrated at Crazy Eddie easier.

If you had any backbone, you would all boycott any presentation that excludes the more skeptical professionals among you. Frankly, after reading many transcripts lately, you guys look like amateurs with your lack of questioning skills, your inability to ask proper follow-through questions, and obtain straight, clear, unambiguous, and honest answers.

You seem like hand-picked patsies as I read your unchallenging questions and the lame answers that management gives you without any challenge or follow up. You never seem to learn as you compete with one another for the affections of management and let access to them rule your work at almost any cost.

Eventually you will run into a guy like I was. You will wish you asked the proper questions and follow-up questions too. You will wish that your other peers attended the meetings and asked questions you would not ask or could not ask. The questions that will never be asked by you and others will cause you to miss detecting the lies and deceit being spun upon you.

When the "earnings surprises" eventually come out, your previous work will be considered negligent and amateurish. Your future work will always be under a cloud of suspicion. You will be remembered for the glowing reports you made as management ran circles around you. Do you want people to think you are fools?

The managements that spread deceit and lies to the selective few who gain coveted access are not your friends. They are using your humanity against you as a weakness to be exploited in furtherance of their crimes. They know about how your efforts at coveted access end up corrupting your professionalism. They don't care about what happens to you as a result of their actions. As a criminal, I never cared about you, too.

You have been warned.

Respectfully,

Sam E. Antar (former Crazy Eddie CFO & convicted felon)

P.S. I see that nothing much has changed since my time. Keep it up. When a company that you wrote a glowing report on ends up a train wreck, will these same managements rescue you?

Securities Fraud

The Securities Act of 1933 is otherwise known as the "truth in securities act." This Act deals primarily with the initial issuance of securities including stocks, bonds, treasury stock, debentures, investment contracts, puts, calls, straddles, options, some oil and gas investments, and other investment vehicles known as securities, focusing on full and fair disclosure. The Securities Exchange Act of 1934 focuses on the regulation of investment securities after their initial offering to the public. The 1934 Act contains a full range of anti-fraud measures. The 1933 and 1934 Acts were followed by the Investment Advisor Act of 1940, the Investment Company Act of 1940, and the Sarbanes–Oxley Act of 2002. The following outlines some of the more common securities fraud schemes.

Pyramid Schemes. In a pyramid scheme, fees or dues are paid by new members to join the organization. The new member, upon joining, is expected to attract and sign up new members and collect their membership fees on behalf of the organization. The organization generates cash flow, not by selling goods and services to clientele but by the collection of membership fees from new members. The membership fees are then distributed in part to the old members as a form of return on investment (e.g., dividend) to keep the old members attracting new members and to keep the scheme from collapsing. The scheme is dependent not only on the distribution of cash to old members, but also on the solicitation of new members and the collection of their membership fees as a source of funding distributions to old members. If the old members either fail to see returns on investment or fail to solicit and sign up new members, the scheme collapses, as they all invariably do.

"Prime Bank" Fraud. Though this fraud scheme, like most others, has various derivations, usually, investors are promised high rates of return with little inherent risk by investing in "prime bank" notes. The underlying methodology is supposed to be an offshore trading program that yields extremely high rates of return. The investment prospectus is usually confusing and makes reference to legitimate banks and recognized financial institutions from around the world. The prospective investor is usually required to sign a nondisclosure agreement. Of course, the entire investment is a sham and the investor will lose all of their money in the process.

Churning. Churning is the excessive sale of securities by a broker for the purposes of generating commissions. To prove churning, the alleged victim must prove that the broker controlled the trading in the account, the volume of activity was excessively high when compared to the investor's trading objectives, and the broker acted with intent to defraud or with reckless disregard for the investor's interests. According to the ACFE Fraud Examiners Manual, the best method for evaluating a claim of churning is to calculate the percentage of monthly commissions generated from the average account balance. Given this calculation by month, the investigator can look for signs of churning such as these:

- The percentage of commission increases during periods of less market volatility
- The percentage of commission increases over time but not in relation to the average account balance (which presumably stays the same)
- The gross commissions for some months are substantially higher than other months, and the underlying rationale for the trades is questionable
- The average gross commissions exceed 5 percent of the average monthly account balance
- The trades generated gross commissions but generated little or no realized investment gains
- The pattern of price changes in the securities sold, subsequent to the sale of the securities, is inconsistent with a need to sell the securities

And the investigator can ask these questions:

- Was the broker acting alone or as a result of investment recommendations and appropriate analysis?
- Did the broker make unauthorized trades?

Unsuitable Recommendations. Securities professionals are supposed to understand their customer's investing objectives, their customer's financial profile, and the customer's level of sophistication. Placing customers in inappropriate investment vehicles is prohibited, and brokerages are supposed to have due diligence procedures in place to ensure that brokers are not abusing their trading responsibilities.

Parking. Parking is a technique used by an investor to avoid ownership reporting requirements and net capital rules. The parking investor sells the security to another individual with the intent and ability to repurchase the security at a later date with the intent of avoiding ownership reporting requirements and net capital rules.

Front Running. Front running is a derivation of insider trading. The perpetrator, possibly a back office clerk or exchange floor order filler, becomes aware of a large buy or sell order, a trade large enough to move the market. In advance of executing the large order, the perpetrator makes a trade in his or her account so as to benefit from the large order trade and the subsequent movement in the market.

Bucket Shops. Bucket shops act as a normal licensed brokerage business, but neither the enterprise nor its employees are registered or licensed. Such operations are illegal and usually created with the intent to defraud prospective clientele.

Misuse or Misappropriation of a Customer's Securities. This scheme involves the theft of investment securities from a client's account or the use of those securities as collateral for other transactions such as loans or margin trading. Periodically, such abuses are observed in trust accounts where few persons are monitoring the investments or the account activity.

Market Manipulations. Market manipulations usually occur in penny or micro-cap stocks, those with very small market capitalization. The manipulation occurs when trading activity is designed to artificially move the security price in one direction or another to give the appearance of activity and momentum to entice others to buy or sell.

Insider Trading. The use of nonpublic information by insiders with fiduciary responsibilities to their company and its shareholders in order to profit from the purchase and sale of securities is illegal.

REVIEW QUESTIONS

4-1 What is the difference between a predator and an "accidental fraudster?"

4-2 Why does collusion pose unique prevention and detection challenges?

4-3 How is the concept of an "organization" involved in mixing illegal activities with legitimate ones?

4-4 What is the difference between "following the money" and "tracing the money?"

4-5 Why is financial statement fraud often considered a complex fraud?

4-6 What are the different types of schemes associated with complex frauds?

4-7 How are the objectives of terrorists and organized criminals different?

4-8 What are the different types of banks in the U.S. banking system? How are they different?

4-9 What is the difference between tax avoidance and tax evasion?

4-10 How have some of the more common securities fraud schemes been perpetrated?

ENDNOTES

1. James O. Finckenauer, Joseph R. Fuentes, and George L. Ward, "Mexico and the United States of America: Neighbors Confront Drug Trafficking," *Forum on Crime and Society* 1, no. 2 (2001) http://www.ncjrs.gov/pdffiles1/nij/218561.pdf
2. Ibid., 4
3. ACFE *Fraud Examiners Manual*, 1.1401 (2005)
4. *Internal Revenue Manual*, 25.1.1.2.4
5. *Internal Revenue Manual*, 4.24.8.3
6. *Internal Revenue Manual*, 25.1.2.2
7. *Internal Revenue Manual*, 25.1.2.2
8. *Internal Revenue Manual*, 25.1.2.2
9. *Internal Revenue Manual*, 25.1.2.2
10. Modified and adapted from SAS No. 99
11. 2005 ACFE *Fraud Examiners Manual*, section 1.309