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.”

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.” 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. 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.” 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.” 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. 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. In other words, the statement constitutes intentional or reckless conduct, whether by act or omission, that results in material misleading financial statements.

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.

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.
# CHAPTER 1 CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

## TABLE 1-1 Common Fraud Schemes

<table>
<thead>
<tr>
<th>Fraud Acts</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Misappropriation</strong></td>
<td></td>
</tr>
<tr>
<td>Cash</td>
<td></td>
</tr>
<tr>
<td>Larceny (theft)</td>
<td></td>
</tr>
<tr>
<td>Skimming (removal of cash before it hits books): Sales, A/R, Refunds, and Other</td>
<td></td>
</tr>
<tr>
<td>Fraudulent Disbursement</td>
<td></td>
</tr>
<tr>
<td>Billing Schemes - including shell companies, fictitious vendors, personal purchases</td>
<td></td>
</tr>
<tr>
<td>Payroll Schemes - ghost employees, commission schemes, workers compensation, and false hours and wages</td>
<td></td>
</tr>
<tr>
<td>Expense Reimbursement Schemes - including overstated expenses, fictitious expenses, and multiple reimbursements</td>
<td></td>
</tr>
<tr>
<td>Check Tampering</td>
<td></td>
</tr>
<tr>
<td>Register Disbursements including false voids and refunds</td>
<td></td>
</tr>
<tr>
<td><strong>Inventory and Other Assets</strong></td>
<td></td>
</tr>
<tr>
<td>Inappropriate Use</td>
<td></td>
</tr>
<tr>
<td>Larceny (theft)</td>
<td></td>
</tr>
<tr>
<td><strong>Corruption</strong></td>
<td></td>
</tr>
<tr>
<td>Conflicts of Interest (unreported or undisclosed)</td>
<td></td>
</tr>
<tr>
<td>Bribery</td>
<td></td>
</tr>
<tr>
<td>Illegal Gratuities</td>
<td></td>
</tr>
<tr>
<td>Economic Extortion</td>
<td></td>
</tr>
<tr>
<td><strong>False Statements</strong></td>
<td></td>
</tr>
<tr>
<td>Fraudulent Financial Statements</td>
<td></td>
</tr>
<tr>
<td>False Representations (e.g., employment credentials, contracts, identification)</td>
<td></td>
</tr>
<tr>
<td><strong>Specific Fraud Contexts</strong></td>
<td></td>
</tr>
<tr>
<td>Bankruptcy Fraud</td>
<td></td>
</tr>
<tr>
<td>Contract and Procurement Fraud</td>
<td></td>
</tr>
<tr>
<td>Money Laundering</td>
<td></td>
</tr>
<tr>
<td>Tax Fraud</td>
<td></td>
</tr>
<tr>
<td>Investment Scams</td>
<td></td>
</tr>
<tr>
<td>Terrorist Financing</td>
<td></td>
</tr>
<tr>
<td>Consumer Fraud</td>
<td></td>
</tr>
<tr>
<td>Identity Theft</td>
<td></td>
</tr>
<tr>
<td>Check and Credit Card Fraud</td>
<td></td>
</tr>
<tr>
<td>Computer and Internet Fraud</td>
<td></td>
</tr>
<tr>
<td>Divorce Fraud (including hidden assets)</td>
<td></td>
</tr>
<tr>
<td>Intellectual Property</td>
<td></td>
</tr>
<tr>
<td>Business Valuation Fraud</td>
<td></td>
</tr>
<tr>
<td><strong>Noteworthy Industry-Specific Fraud</strong></td>
<td></td>
</tr>
<tr>
<td>Financial Institutions</td>
<td></td>
</tr>
<tr>
<td>Insurance Fraud</td>
<td></td>
</tr>
<tr>
<td>Health Care Fraud</td>
<td></td>
</tr>
<tr>
<td>Securities Fraud</td>
<td></td>
</tr>
<tr>
<td>Public Sector Fraud</td>
<td></td>
</tr>
</tbody>
</table>

## 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
WHAT IS THE DIFFERENCE BETWEEN FRAUD AND ABUSE?

• 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. 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.\textsuperscript{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.

\textbf{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.

\textbf{CRITICAL THINKING EXERCISE}

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

\textit{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.2}

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.

\textbf{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
10 \textbf{CHAPTER 1 CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS}

\section*{DYNAMIC FORCES}

\begin{itemize}
  \item Auditing
    \begin{itemize}
      \item Risk Assessment
      \item Internal Controls
    \end{itemize}
  \item Financial Forensics
    \begin{itemize}
      \item Litigation Support - calculation of economic damages, marital dissolution, business valuation, etc.
    \end{itemize}
  \item Fraud Examination
    \begin{itemize}
      \item Planning
      \item Fraud Detection
      \item Fraud Prevention & Deterrence
      \item Gathering Evidence
      \item Interviewing
      \item Witnessing
      \item Reporting
    \end{itemize}
\end{itemize}

\section*{FIGURE 1-1 Auditing, Fraud Examination, and Financial Forensics}

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.

\section*{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.
Before 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
CHAPTER 1  CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

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:

<table>
<thead>
<tr>
<th>Fraud Perpetrator Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male, Well Educated</td>
</tr>
<tr>
<td>Middle-Aged to Retired</td>
</tr>
<tr>
<td>Accountant, Upper Management or Executive</td>
</tr>
<tr>
<td>With the Company for Five or More Years</td>
</tr>
<tr>
<td>Acts Alone</td>
</tr>
<tr>
<td>Never Charged or Convicted of a Criminal Offense</td>
</tr>
</tbody>
</table>

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. 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...
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.

**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.
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
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.

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.
CHAPTER 1 CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

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.

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](image)

**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.
CHAPTER 1  CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

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.

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

<table>
<thead>
<tr>
<th>Control</th>
<th>Percent of Cases Implemented</th>
<th>Yes</th>
<th>No</th>
<th>Percent Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surprise audits</td>
<td>25.5%</td>
<td>$70,000</td>
<td>$207,000</td>
<td>66.2%</td>
</tr>
<tr>
<td>Job rotation/mandatory vacation</td>
<td>12.3%</td>
<td>$64,000</td>
<td>$164,000</td>
<td>61.0%</td>
</tr>
<tr>
<td>Hotline</td>
<td>43.5%</td>
<td>$100,000</td>
<td>$250,000</td>
<td>60.0%</td>
</tr>
<tr>
<td>Employee support programs</td>
<td>52.9%</td>
<td>$110,000</td>
<td>$250,000</td>
<td>56.0%</td>
</tr>
<tr>
<td>Fraud training for managers/execs</td>
<td>41.3%</td>
<td>$100,000</td>
<td>$227,000</td>
<td>55.9%</td>
</tr>
<tr>
<td>Internal audit/fraud examination dept</td>
<td>55.8%</td>
<td>$118,000</td>
<td>$250,000</td>
<td>52.8%</td>
</tr>
<tr>
<td>Fraud training for employees</td>
<td>38.6%</td>
<td>$100,000</td>
<td>$208,000</td>
<td>51.9%</td>
</tr>
<tr>
<td>Anti-fraud policy</td>
<td>36.2%</td>
<td>$100,000</td>
<td>$197,000</td>
<td>49.2%</td>
</tr>
<tr>
<td>External audit of ICOFR</td>
<td>53.6%</td>
<td>$121,000</td>
<td>$332,000</td>
<td>47.8%</td>
</tr>
<tr>
<td>Code of conduct</td>
<td>61.5%</td>
<td>$126,000</td>
<td>$232,000</td>
<td>45.7%</td>
</tr>
<tr>
<td>Mgmt review of internal controls</td>
<td>41.4%</td>
<td>$110,000</td>
<td>$200,000</td>
<td>45.0%</td>
</tr>
<tr>
<td>External audit of financial statements</td>
<td>69.6%</td>
<td>$150,000</td>
<td>$250,000</td>
<td>40.0%</td>
</tr>
<tr>
<td>Independent audit committee</td>
<td>49.9%</td>
<td>$137,000</td>
<td>$200,000</td>
<td>31.5%</td>
</tr>
<tr>
<td>Mgmt certification of financial statements</td>
<td>51.6%</td>
<td>$141,000</td>
<td>$200,000</td>
<td>29.5%</td>
</tr>
<tr>
<td>Rewards for whistleblowers</td>
<td>5.4%</td>
<td>$107,000</td>
<td>$150,000</td>
<td>28.7%</td>
</tr>
</tbody>
</table>

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
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).

**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.
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?
CHAPTER 1 CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

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.”

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?
Situation: 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. 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.

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
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? 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?

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>H1</th>
<th>H2</th>
<th>H3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iraq will not retaliate.</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Iraq will sponsor some minor terrorist actions.</td>
<td>+</td>
<td>0</td>
<td>–</td>
</tr>
<tr>
<td>Iraq will plan and execute a major terrorist attack,</td>
<td>0</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>perhaps against one or more CIA installations.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
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.
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 to 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.


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.
CHAPTER 1 CORE FOUNDATION RELATED TO FRAUD EXAMINATION AND FINANCIAL FORENSICS

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.

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

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.


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.


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.


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.


22. Adapted from ACFE Fraud Examiners Manual.


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.