Core Foundation Related to Forensic Accounting and Fraud Examination

1

FRAUD NEWS

In January 2022, according to *The New York Times*, Elizabeth Holmes, the founder of the failed blood testing start-up Theranos, was found guilty of four of 11 charges of fraud. Each sentence carries a maximum sentence of 20 years in prison (see "Elizabeth Holmes is found guilty of four counts of fraud," January 3, 2022).

Forensic accounting is simply defined as the intersection of accounting and the law. Consider an insurance claim whereby the insured is claiming that a contractor provided inferior work in March 2017 by placing an exposed water pipe in an unheated attic. In the first week of February 2018, during a two-day cold spell when temperatures dropped below freezing, the water pipe burst causing hundreds of thousands of dollars of water damage throughout 70% (4200 of 6000 square feet) of the building. Some questions to ponder include:

- Is the contractor liable for the water pipe failure 11 months later?
- What if there was a three-day cold spell in January 2018 and the pipe did not break? Would the contractor still be liable for the cost of damages from a water pipe break in February 2018?
- What if the water damage occurred at a retail establishment that needed to be closed for three months to repair the damage? Further consider that the business is located in "spring break territory" and earns 50% of its annual income (profit) during February, March, and April?
- Should the damages include lost profits?
- Is the extent of the damage (70% of the total square footage) relevant?
- Was there a contract between the contractor and the claimant?
- What parts of the contract might be relevant?
- Was there a warranty, implied or in writing (contractual)?

There are two overarching questions: (1) Is the contractor liable, and (2) If so, for how much? Further, notice that the calculation of damages involves not only dollars but also contractual obligations, down time, and peak dates, as well as the extent of damage (i.e., relevant nonfinancial issues).

Forensic accounting also considers employment damages arising from unfortunate events such as a work injury, an auto accident where the victim is unable to work, partially disabled, or has died as a result of the accident. Assume that a victim is rear-ended in an auto accident by an insured. Little doubt exists about the liability of the person, who caused the accident, and his insurance company. In such a case, forensic accounting professionals use a variety of financial information—such as W-2s and tax returns—along with relevant nonfinancial data, such as expected future number of years in the workforce and life expectancy—to place a value on the damages to the victim.

As noted in the previous two examples, forensic accounting issues can be complex and require more than basic accounting data. Now consider the following case.

David Williams, 54, from Fort Worth, Texas, was arrested on October 12, 2017, by FBI special agents on a federal charge of engaging in a scheme to defraud insurance companies by submitting more than $25 million in false and fraudulent claims for medical services.[1]

> ***According to the criminal complaint affidavit between November 2012 through August 2017, Williams advertised on his website (getfitwithdave.com) that he offered in-home fitness training and therapy through his company, "Kinesiology Specialists." Williams identified himself as "Dr. Dave" and stated that he served clients in most of Texas, Las Vegas, Denver, Tucson, Seattle, and Orlando. Through his website, Williams told potential clients that he was accepting most health care insurance coverage plans.***
>
> ***In order to bill insurance companies for his services, Williams registered as a health care provider with the Centers for Medicare and Medicaid Services. In completing the application, Williams falsely certified that he was a health care provider. Williams enrolled as a health care provider at least nineteen times under different names or variations of his name and his company names, and falsely certified that he was a health care provider in each application. Williams would then bill the insurance companies as if he were a medical physician and as if he had provided care requiring medical decision- making of high complexity when Williams actually provided fitness and exercise training to his clients.***

According to the criminal complaint affidavit, Williams recruited potential clients through the use of flyers, the Internet, and word-of-mouth. Once recruited, Williams would typically meet with, or speak to, the new client over the phone and review their health history and goals for their planned fitness training. Williams would then typically assign a personal trainer to that individual. The personal trainer typically met with the client between one and three times a week for approximately one hour and provided fitness training. Williams would then bill insurance companies for each training session using inaccurate codes and on certain occasions, billed for services that neither he, nor his staff, ever provided.

Between November 2012 through August 2017, Williams was paid in excess of $3.9 million in connection with his fraudulent billing of United HealthCare Services, Inc., Aetna, Inc., and Cigna.

We'll examine these topics across several modules. Those modules, along with the learning objectives, include the following:

- Module 1 examines fraud, its legal elements, major categories, common fraud schemes, and introduces the concept of abuse. The objective is for readers to be able to describe occupational fraud and abuse and to appreciate the complexities of pursuing legal action against fraudsters.
- Module 2 defines forensic accounting and contrasts forensic accounting engagements to fraud examinations. The goal in this module is for readers to be able to articulate the role of forensic accountants.
- Module 3 takes a look at some of the skills necessary to be a forensic accountant or fraud examiner. The goal is for readers to be able to identify the portfolio of required professional skills and to determine the alignment of their personal characteristics.
- Module 4 compares and contrasts auditing with fraud examination and forensic accounting. While understanding the similarities and differences between auditing, fraud examination, and forensic accounting take time, the take-away from module 4 will be the reader's ability to describe the role of each field and identify the similarities, differences, overlaps, and unique space of each.
- Module 5 offers an overview of the basics of fraud. Topics include the societal costs of fraud and litigation, as well as key metrics and fraud statistics from the Association of Certified Fraud Examiners' Report to the Nations, a biannual survey of fraud cases. The goal is for readers to recognize the cost of fraud and to develop profiles of fraud schemes, perpetrators, victims, and other relevant fraud-related attributes.
- Module 6 takes an initial look into the examination (investigation) of forensic accounting and fraud issues. The goal is to launch readers on a path toward the detection, investigation, and remediation of forensic accounting issues and fraud's red flags.
- Module 7 provides an overview of the key elements of fraud examination. Fraud examination is more than just investigation of allegations, it also includes prevention, deterrence, detection, and remediation. Readers will be able to describe predication and articulate the activities associated with fraud examination.

Module 1: What Is Fraud?

Imagine that you work in the accounts payable department of your company, and you discover that your boss is padding his reimbursable travel expenses with personal expenses. Consider this: Walmart legend, Thomas 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 Walmart'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. Walmart 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."[2]

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: by 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."[3] 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.[4] 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."[5] 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 willfully 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." 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*, 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. As you

see later in Chapter 1, our recommended investigative approach does not require that you identify the specific law that was violated. Rather, the goal is to examine the relevant evidence with an eye toward demonstrating three attributes of the fraud:

- The scheme or fraud act
- The concealment activity
- The conversion or benefit

This approach ensures a careful and thorough examination of the issue without causing the forensic accountant to make decisions better suited to an attorney's expertise. We'll also use a thorough and careful examination of evidence associated with forensic accounting issues; again, this approach permits legal professionals to make determinations of which specific laws are relevant to the case facts and circumstances.

Major Categories of Fraud

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

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

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

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

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

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

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

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

Financial Statement and Reporting Fraud	
Net Worth/Net Income Overstatements	Net Worth/Net Income Understatements
Fictitious revenue (and related assets)	Understated revenue (and related assets)
Improper timing of revenue and expense recognition	Improper timing of revenue and expense recognition
Concealed liabilities and expenses	Overstated liabilities and expenses
Improper asset valuation, including inappropriate capitalization of expenses	Improper asset valuation, including inappropriate asset write-offs
Improper disclosures	Improper disclosures

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 the early 2000s, the financial press 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 2022 Report to the Nations on Occupational Fraud and Abuse noted that financial statement fraud tends to be the least frequent of all frauds, accounting for only about 9%. However, the median loss for financial statement fraud is approximately $593,000, almost six times larger than the typical asset misappropriation and almost four times larger than the typical corruption scheme. In addition, when financial statement fraud has been identified, other types of fraud are also being perpetrated.

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.

TABLE 1-1 Common Fraud Schemes

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

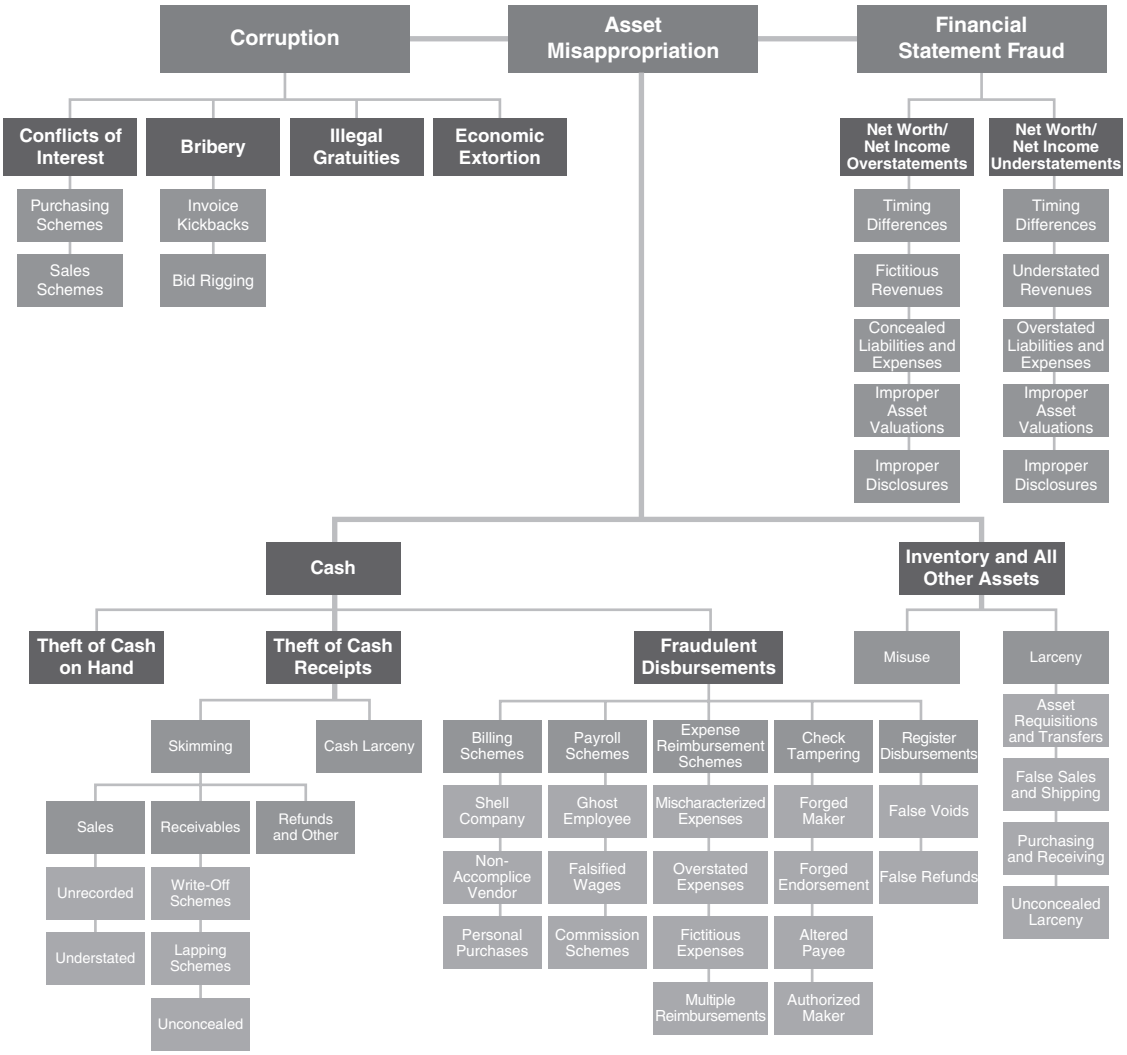


FIGURE 1-1
Occupational fraud and abuse classification system (fraud tree)

The Fraud Tree was developed in 1996 by Dr. Joseph T. Wells, Founder and Chairman of the ACFE (Figure 1-1). This tool for classifying major categories of fraud has withstood the test of time. It helps readers understand fraud based on the type of scheme (asset misappropriation, corruption, and financial statement fraud) as well as important subcategories. Each type of fraud has specific elements required to perpetrate and conceal the fraud. As such, detection can be targeted by likely symptoms, and investigation can be tailored accordingly.

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 for personal use
- Surf the Internet while at work
- Attend to personal business during working hours
- Take a long lunch, or a break, without approval
- Arrive at work late, or leave early
- Use sick leave when not sick
- Do slow or sloppy work
- Use employee discounts to purchase goods or services 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 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? Here is an example to illustrate: 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. In the case of the embezzlement, the employee would likely be terminated; there is also a possibility (albeit remote) that she would be prosecuted. But in the case in which the employee misuses her sick time, she would likely be reprimanded, or her pay might be docked for the day.

We can also change the abuse example slightly. Let's say the employee works for a governmental agency instead of the private sector. Sick leave abuse—in its strictest interpretation—would be 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 or theft of public funds in any form is a serious matter, and the prosecutorial thresholds are surprisingly low.

The Crazy Eddie Case

Adapted from The White Collar Fraud website 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 eighteen 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."

Module 2: 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

Forensic accounting 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 forensic accounting professional as an expert or consultant
2. Investigative services, which make use of the forensic accounting professional's skills and may or may not lead to courtroom testimony

Forensic accounting may involve either an attest or consulting engagement.[9] According to the AICPA, Forensic and Valuation Services (FVS) professionals provide educational, technical, functional, and industry-specific services that often apply to occupational fraud, corruption, and abuse and to financial statement fraud cases. FVS professionals may assist attorneys with assembling the financial information necessary either to bolster a case (if hired by the plaintiff) or to undercut it (if hired by the defendant). 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 involve services for criminal, civil, or administrative cases that entail economic damage claims, workplace or matrimonial disputes, or asset and business valuations.[10]

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.

Nonfraud Forensic Accounting 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, cost measurement and any other aspect related to a litigant's finances, financial performance and/or financial condition. 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 may be 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
Antitrust actions
Intellectual property infringement and other disputes
Environmental issues
Tax disputes
Employment issues related to lost income and wages

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.

Module 3: The Professional's Skill Set

Forensic accounting and fraud examination require at least three major skill types: technical competence, investigative, and communication.

First, the technical skills of accounting, auditing, finance, quantitative methods, and certain areas of the law and research provide the foundation upon which theories of the case are examined.

Critical Thinking Exercise

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

> *Anthony and Cleopatra are lying dead on the floor in a villa. Nearby on the floor is a broken bowl. There is no mark on either of their bodies, and they were not poisoned. With this information, determine how they died*[11]

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 identified as assumptions; but the questioning of assumptions that investigators are making without realizing they 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.

Note: This critical thinking exercise is revisited in the end of chapter assignments.

Second, forensic accountants and fraud examiners use investigative skills for the collection, analysis, and evaluation of evidential matter, and critical thinking to interpret the findings.

Third, the ability to effectively and succinctly communicate the results of her work is critical to the professional's success.

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. Forensic accountants and fraud examiners operationalize these skills using the "fraud theory" approach which incorporates the hypothesis-evidence matrix.

Module 4: The Role of Auditing, Fraud Examination, and Forensic Accounting

Fraud examination, forensic accounting, 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 seeks 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 (AU Section 316), 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 forensic accounting intersect.

However, each discipline also encompasses separate and unique functional aspects. For example, fraud examiners are generally called in after there is reason to believe that fraud has occurred or is occurring, and often assist in fraud prevention and deterrence efforts that do not involve the audit of nonpublic companies or the legal system. Forensic accounting 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 the legal system. Thus, as graphically presented in Figure 1-2, auditing, fraud examination, and forensic accounting often use the same tools, but they also have responsibilities independent of the other.

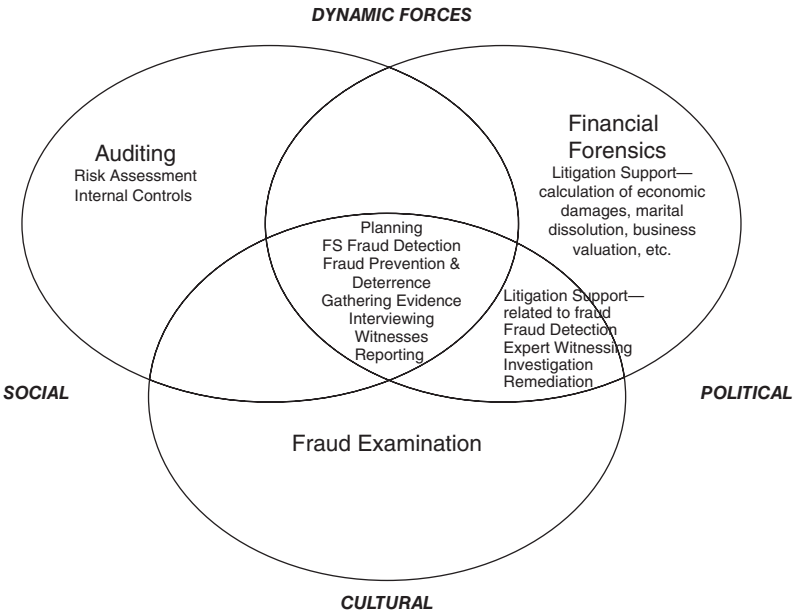


FIGURE 1-2
Auditing, fraud examination, and forensic accounting

TABLE 1-2 Differences Between Auditing, Fraud Examination, and Forensic accounting

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

The interrelationship among auditing, fraud examination, and forensic accounting is dynamic and changes over time because of political, social, and cultural pressures. Independent auditors operate in an environment impacted by Dodd–Frank, SOX, and SAS 99; consequently, they are expected to have adequate knowledge and skills in the area of fraud detection and deterrence. In addition, auditors, fraud examiners, and forensic accountants often have skill sets in multiple areas and are able to leverage their skills and abilities from one area when working in others.[12]

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 about investigation findings, and assisting in the general detection and prevention of fraud. Fraud examination has overlap with the field of forensic accounting—the latter also uses financial knowledge, skills, and abilities for courtroom purposes. Forensic accounting may involve not only the investigation of potential fraud, but a host of other litigation support services.

Similarly, fraud examination and auditing are interrelated, but fraud examination encompasses much more than just the review of financial data. It 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 these interrelationships and differences.

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

Module 5: The Basics of Fraud

Brian Lee excelled as a top-notch plastic surgeon. Lee practiced out of a large physician-owned clinic of various 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.

Because plastic surgery is considered by many health insurance plans to be an elective procedure, patients were required to pay their portion of the surgical fees in advance. The case that ultimately nailed Brian Lee involved Rita Mae Givens. Givens had elective 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 surgery 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 surgical procedures, for which

billing records were not required, particularly when payment was made in cash or by a check made 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.[13]

The Cost of Fraud and Other Litigation

Based on 2021 world GDP, the ACFE estimated that the cost of fraud may be as high as $4.7 trillion 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% 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 $1000 (a computer, for example), the company would need to sell an additional 5000 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 expenses of fraud and litigation are hidden, even if a portion of the cost is reflected in the profit and loss figures. The indirect costs of fraud and litigation can have a far-reaching impact—employees may lose their jobs; the company may have difficulty getting loans, mortgages, and other forms of credit; the company's reputation may be adversely affected; and the company may become the target 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 organization has already incurred substantial costs.

ACFE 2022 Report to the Nations 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 2022 Report to the Nations 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.

Fraud Schemes Corresponding With the Fraud Tree

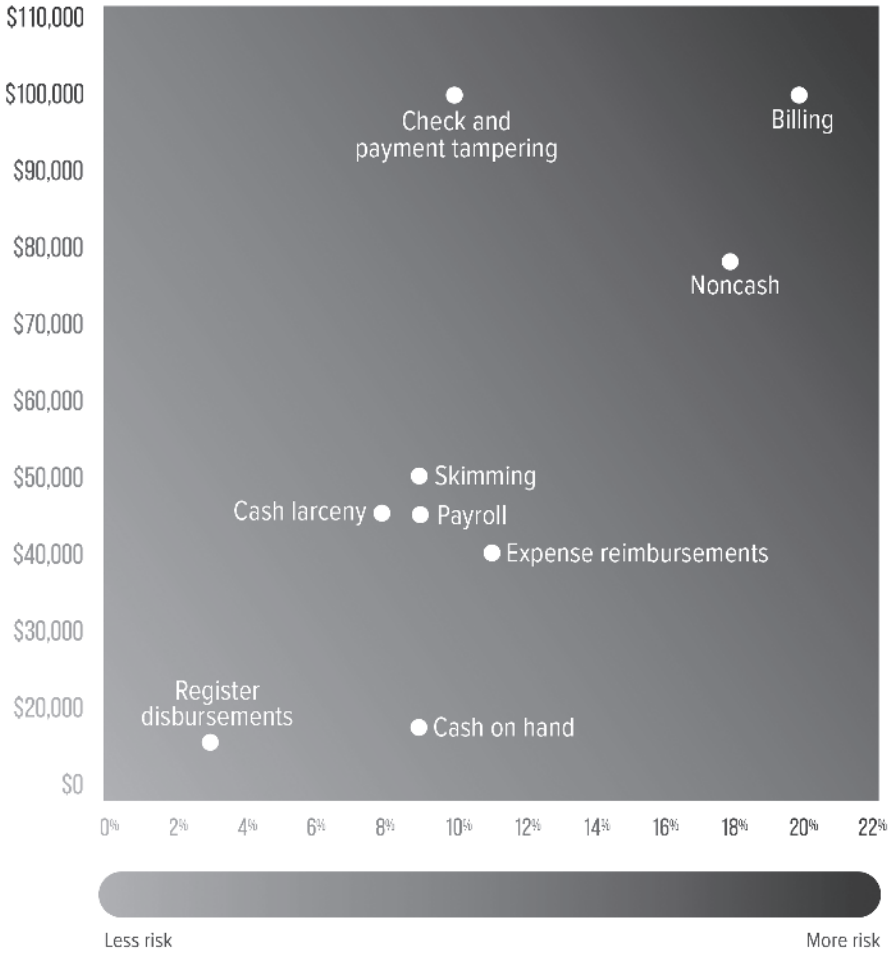
The ACFE highlights three major types of occupational fraud and abuse: asset misappropriation, corruption, and financial reporting fraud. The relative frequency and losses associated with each are as follows:

Fraud Scheme Category	Percentage	Median Losses
Asset Misappropriation	86	$100,000
Corruption	50	$150,000
Financial Reporting Fraud	9	$593,000

These percentages do not add up to 100% because many frauds involve multiple schemes. Within asset misappropriation, which has the most diversity, the heat map of frequency and loss (Figure 1-3) provides a broader view of the risk to victims.

Corruption is hypothesized to be especially common in cultures where "gratuities" are part of the business climate. It is, by far, the most common occupational fraud scheme in all regions of the world. The ACFE 2022 Report to the Nations offers insight into the frequency of corruption schemes reported in each of the following world regions. (Figure 1-4)

Regional Focus	Corruption Schemes
Asia-Pacific	57%
Eastern Europe & Western/Central Asia	64%
Latin America & the Caribbean	59%
Middle East & North Africa	59%
Southern Asia	71%
Sub-Saharan Africa	62%
United States & Canada	37%
Western Europe	44%



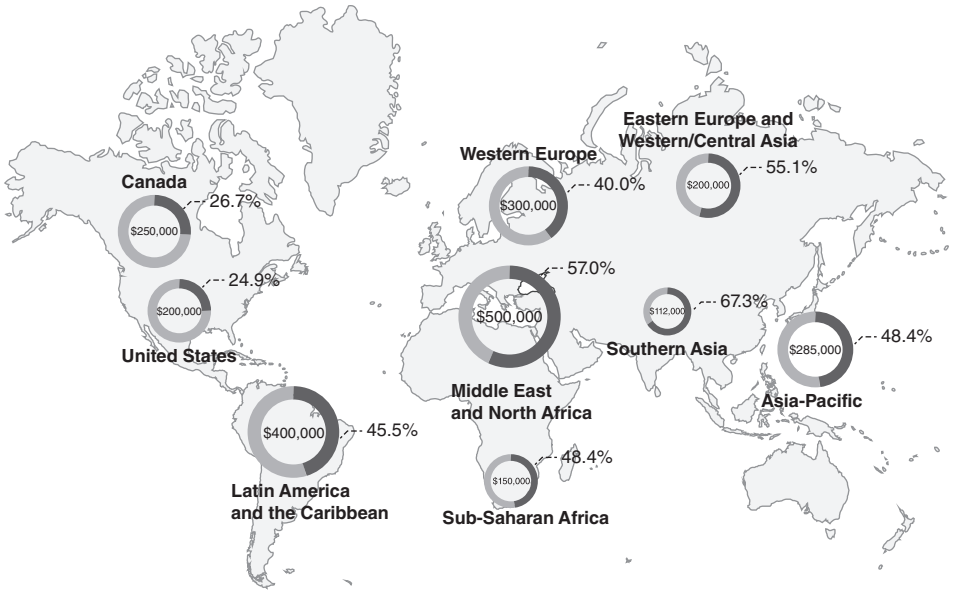
Category	Number of cases	Percent of all cases	Median loss
Billing	416	20%	$100,000
Noncash	385	18%	$78,000
Expense reimbursements	232	11%	$40,000
Check and payment tampering	208	10%	$100,000
Cash on hand	199	9%	$15,000
Skimming	198	9%	$50,000
Payroll	198	9%	$45,000
Cash larceny	169	8%	$45,000
Register disbursements	58	3%	$10,000

FIGURE 1-3
Frequency and median loss of asset misappropriation sub-schemes
Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

As the duration of a fraud shortens, the cost decreases, as noted in Figure 1-5. Organizational efforts to detect fraud earlier have resulted in smaller losses over the past decade. The median fraud currently lasts about twelve months, according to the ACFE.

The 2022 survey queried CFEs on the most common tactics to conceal fraud schemes. As the graphic in Figure 1-6 depicts, the most common concealment schemes are "old fashioned" document-based efforts. Across time, antifraud professionals might see more electronic (technological) concealment. In the near term, traditional red flags are likely going to be grounded in physical evidence. While some differences across fraud categories were observed, generally, concealment is similar for asset misappropriation, corruption, and financial fraud schemes.

Tips (i.e., whistleblowing, hotlines) remain firmly as the most frequent means by which fraud is detected as shown in Figure 1-7. In the 2022 data, internal audit (16%) edged out management review (12%) as the second-most common detection method. Historically, external audits detected only about 4% of frauds. This is likely due to the materiality threshold incorporated into the external audit process. As noted above, the median loss, especially for asset misappropriation which is the highest frequency of fraud at 86%, is relatively low. As such, external auditors may not sample and examine transactions associated with the fraud scheme included in the ACFE study. The role of the external audit, as it relates to detecting fraud, is the subject of much professional and researcher attention.



**For each region, the percentage shown indicates the proportion of cases in the region that involved corruption, and the dollar figure represents median loss for the corruption cases in the region.*

FIGURE 1-4
Frequency and median loss of corruption cases by region

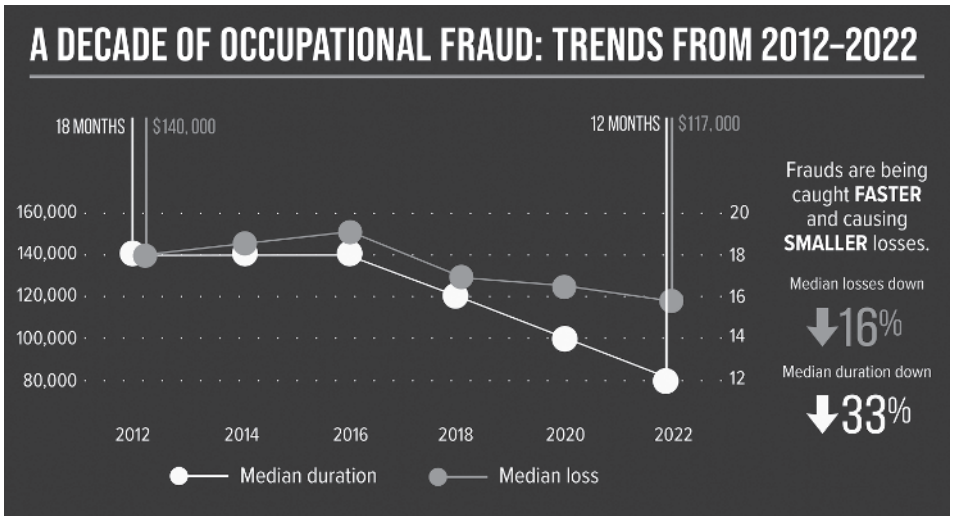


FIGURE 1-5
Frequency and median loss based on duration of fraud

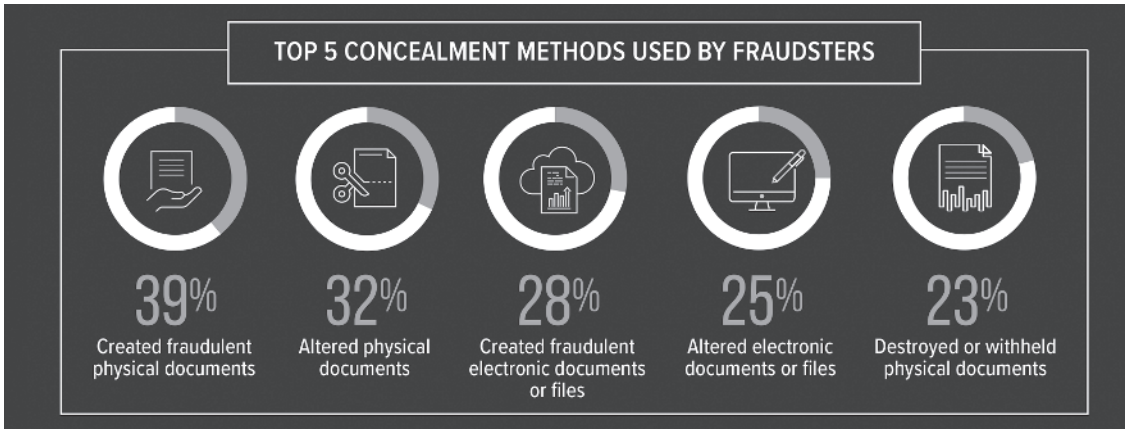


FIGURE 1-6
Concealment method by scheme type

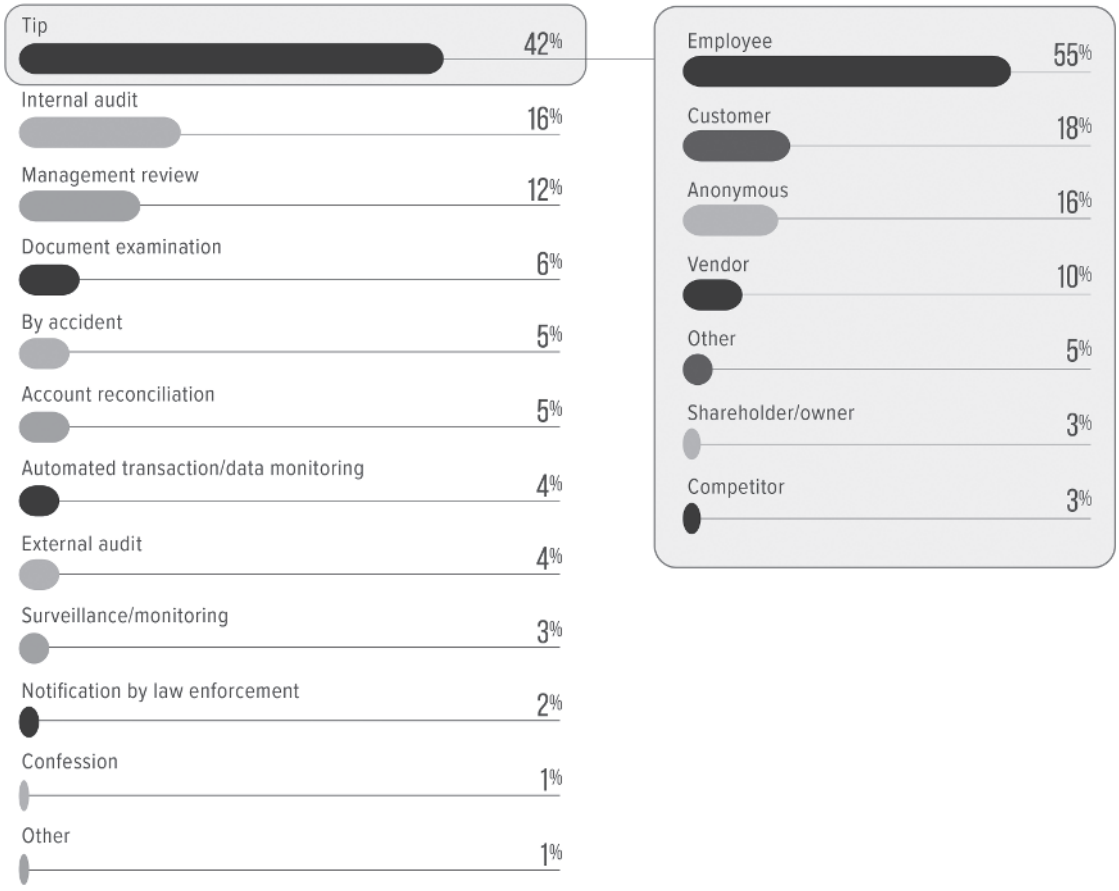


FIGURE 1-7
Initial detection of occupational frauds
Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

The following chart offers a deeper look at tips by identifying the source of the tip.

Source of the Tip	Percentage
Employee	55
Customer	18
Anonymous	16
Vendor	10
Other	5
Shareholder/Owner	3
Competitor	3

The Perpetrators of Fraud

Another goal of the ACFE survey was to gather demographics on the perpetrators: How old are they? How well educated? What is the gender breakdown of offenders? Were there any identifiable correlations with respect to the offenders? Participants in the 2022 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 (see Figure 1-8). 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' position and the size of fraud losses.

The lowest median loss of $50,000 was found in frauds committed by employees. Although the median loss in schemes committed by male managers reached $125,000, the median loss skyrocketed to $446,000 for male executives/owners, more than twice the median loss for female executives/owners. Approximately 23% of the schemes are committed by executives/owners, but they caused the largest losses.

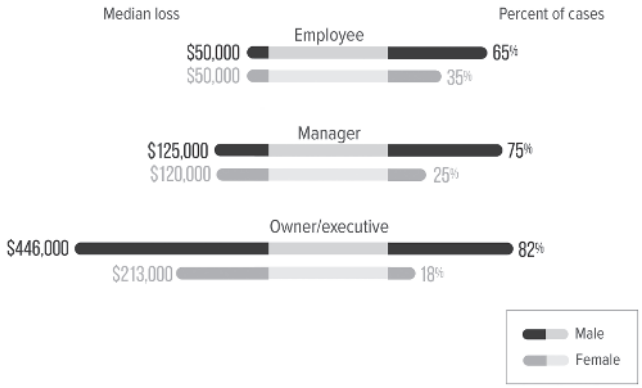


FIGURE 1-8 Position of perpetrator—frequency and median loss

Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

The Effect of Gender on Median Loss

The 2022 ACFE Report to the Nations showed that male employees were responsible for almost twice as many cases of fraud (65%) as female employees (35%); the median loss in a scheme caused by an employee was $50,000, regardless of gender. At the owner/executive level, however, men perpetrated more than four times the number of cases than women (82% vs. 18%); and the median losses for male owner/executives were more than twice those of women ($446,000 vs. $213,000). 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 73% of the cases, as Figure 1-9 shows.

The Effect of Age on Median Loss

The age range of fraud perpetrators in the study ran the gamut from young to senior citizen. There was a strong correlation between the age of the perpetrator and the size of the median loss (see Figure 1-10), which was consistent with findings from previous reports. Although there were very few cases committed by employees over the age of sixty (3%), the median loss in those schemes was $800,000. By comparison, the median loss in frauds committed by those twenty-five or younger was $40,000. As with position 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 older age groups were the most costly on average, almost two-thirds of the frauds reported were committed by employees 31–50 years old. The median age among perpetrators was 40.

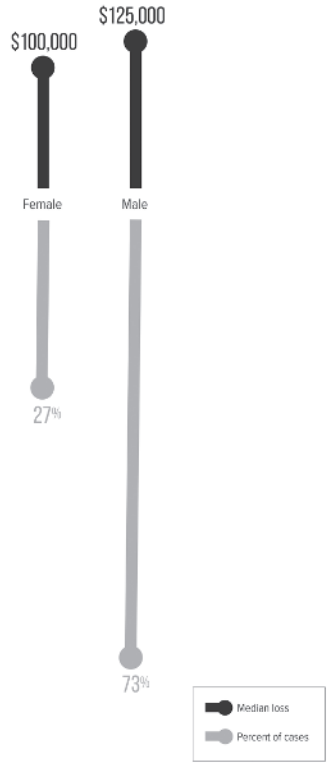


FIGURE 1-9 Gender of perpetrator—frequency

Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

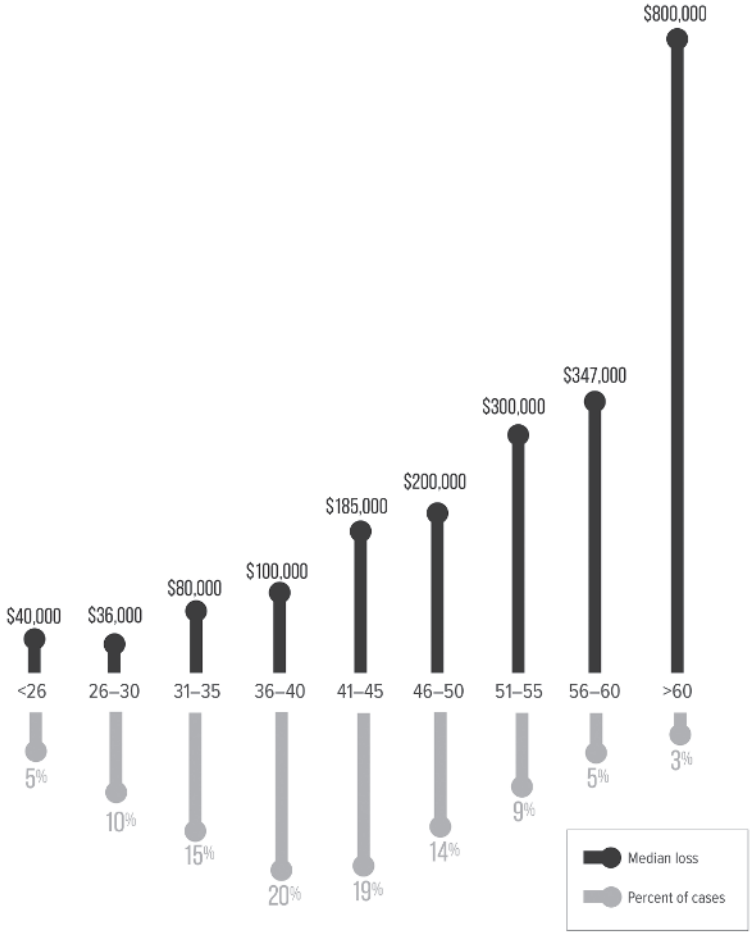


FIGURE 1-10
Age of perpetrator—frequency and median loss
Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

The Effect of Education on Median Loss

As employees' education levels rose, so did the losses from their frauds (Figure 1-11). The median loss in schemes committed by those with only a high school education was $65,000, whereas the median loss caused by employees with a postgraduate education was $135,000. This trend was to be expected, given that those with higher education levels tend to occupy positions with higher levels of authority.

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. Many of the 2022 survey cases (42%) only involved a single perpetrator, but when two or more persons conspired, the median loss was considerably higher (see Figure 1-12).

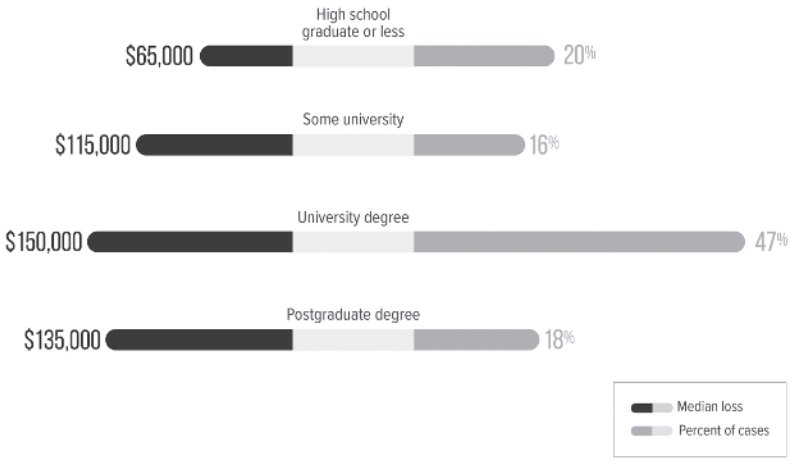


FIGURE 1-11
Education level of perpetrator—frequency and median loss
Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

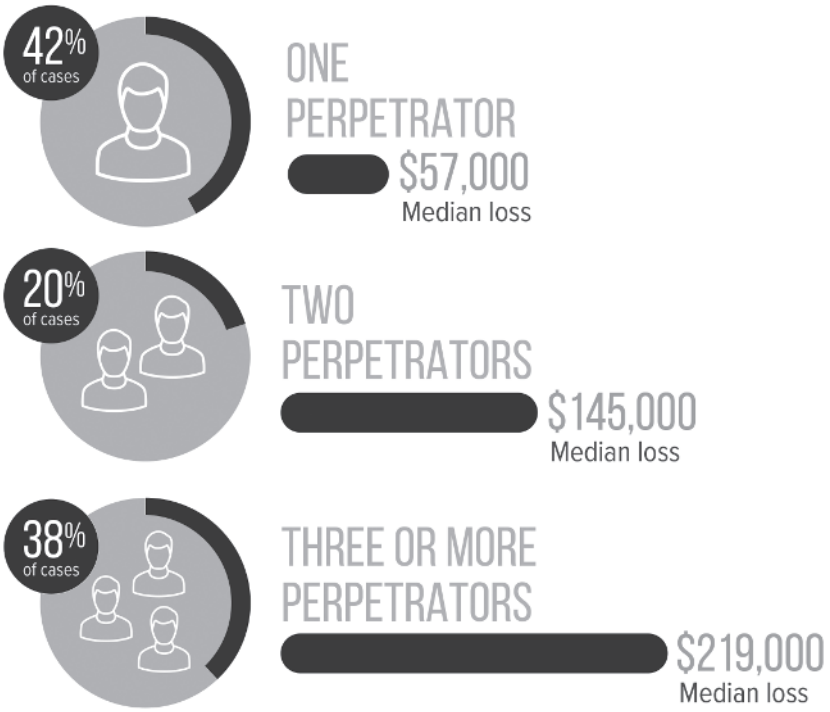


FIGURE 1-12 Number of perpetrators—frequency and median loss

Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

Criminal History of the Perpetrators

Most people who commit occupational fraud are first-time offenders. Only 6% of the perpetrators identified in the 2022 study were known to have been convicted of a previous fraud-related offense. Another 7% of the perpetrators had previously been charged but never convicted. These figures are consistent with previous studies. It is also consistent with Cressey's model, in which occupational offenders do not perceive themselves as lawbreakers. With regard to employment history, approximately 8% had been previously terminated for fraud-related offenses.

The ACFE presented survey respondents with a list of 17 common behavioral red flags associated with occupational fraud and asked them to identify which, if any, of these warning signs had been displayed by the perpetrator before the fraud was detected. In more than 85% of cases, at least one behavioral red flag was identified prior to detection, and in 51% of cases two or more red flags were seen. The behavioral red flags and their frequency are presented in Figure 1-13.

The Victims

The victims of occupational fraud are organizations that are defrauded by those they employ. The ACFE's 2022 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.

Median Loss Based on Type of Organization

Private companies can face challenges in deterring and detecting fraud that differ significantly from those of other organizations. The data show that these private organizations tend to suffer disproportionately large fraud incidents—the median loss for fraud cases attacking private organizations was $120,000, almost comparable to that of public companies ($118,000). This exceeded the median loss for cases in nonprofit organizations, but was surpassed by the losses in government and other organization types (Figure 1-14).

Median Loss Based on Size of the Organization

Small businesses (those with fewer than 100 employees) tend to suffer disproportionately larger median losses, similar to findings in prior reports (see Figures 1-15 and 1-16). One exception: companies with 100–999 employees (for the 2016 survey only) had median fraud losses that exceeded those of smaller organizations by $36,000.

The data for median loss per number of employees confirm what was always suspected. Antifraud professionals logically conclude that small organizations are particularly vulnerable to occupational fraud and abuse. The results from fraud surveys bear this out: losses in the smallest companies were comparable to, or greater than, those in organizations with the largest number of employees. It is suspected that this phenomenon exists for two reasons. First, smaller businesses have fewer divisions of responsibility; therefore, 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 to 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.

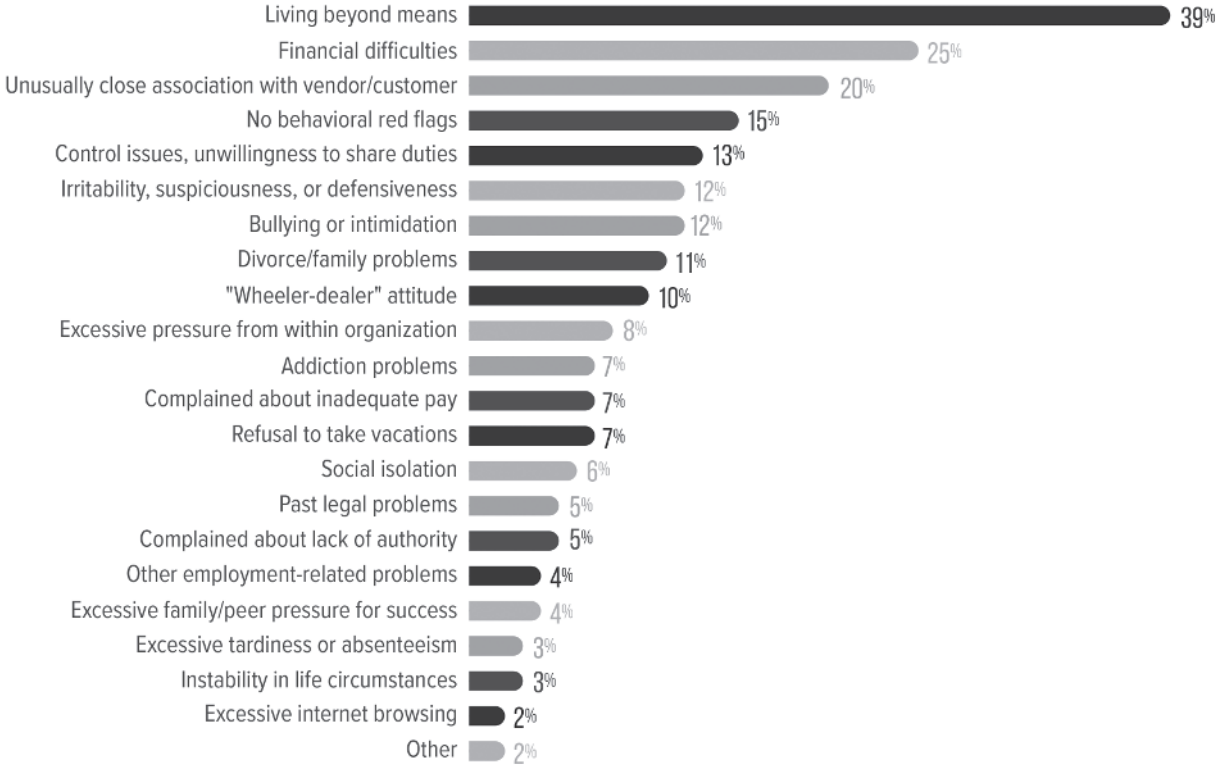


FIGURE 1-13
Behavioral red flags displayed by perpetrators
Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

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 one another personally. None of us like to think that our coworkers would, or do, commit these criminal offenses. Our defenses are 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 element in business—we can, and do, make handshake deals every day. Economic transactions simply cannot occur without trust. The key is seeking the right balance between too much, and too little, trust.

The Impact of Antifraud Measures on Median Loss

CFEs who participated in the ACFE's fraud surveys were asked to identify which, if any, of several common antifraud 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 antifraud measures were the external audit of financial statements, and a formal code of conduct, each of which were utilized by 82% of victim organizations (Figure 1-17). Organizations that implemented these and other controls, noted smaller fraud losses and quicker detection of frauds than organizations lacking these controls The five controls associated with the largest increase in use over the past 10 years were hotlines (16% increase), fraud training for employees (14%), anti-fraud policies (13%), fraud training for managers/executives (12%), and formal fraud risk assessments (11%).

Remediation

A crucial step in the remediation process is understanding how a fraud occurred, as well as how to prevent and deter future occurrences. In hindsight, it can be difficult to pinpoint the exact system breakdowns that allowed a fraud to occur. However, learning from past fraud incidents is necessary to better prevent and detect future fraud schemes. Consequently, the ACFE survey asks respondents for their perspective on the internal control weaknesses at the victim organization that contributed to the fraudster's ability to perpetrate the scheme. A clear lack of internal controls was cited as the primary issue by 29%, followed by another 20% stating that internal controls were present but had been overridden by the perpetrator, and a lack of management review (16%) (see Figure 1-18).

Remediation: Case Results

Another step in the remediation process is for the antifraud professional to assist with the civil and criminal processes. 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 has contributed to an increase in fraud occurrences—or so the argument goes—because potential offenders are not deterred by weak or

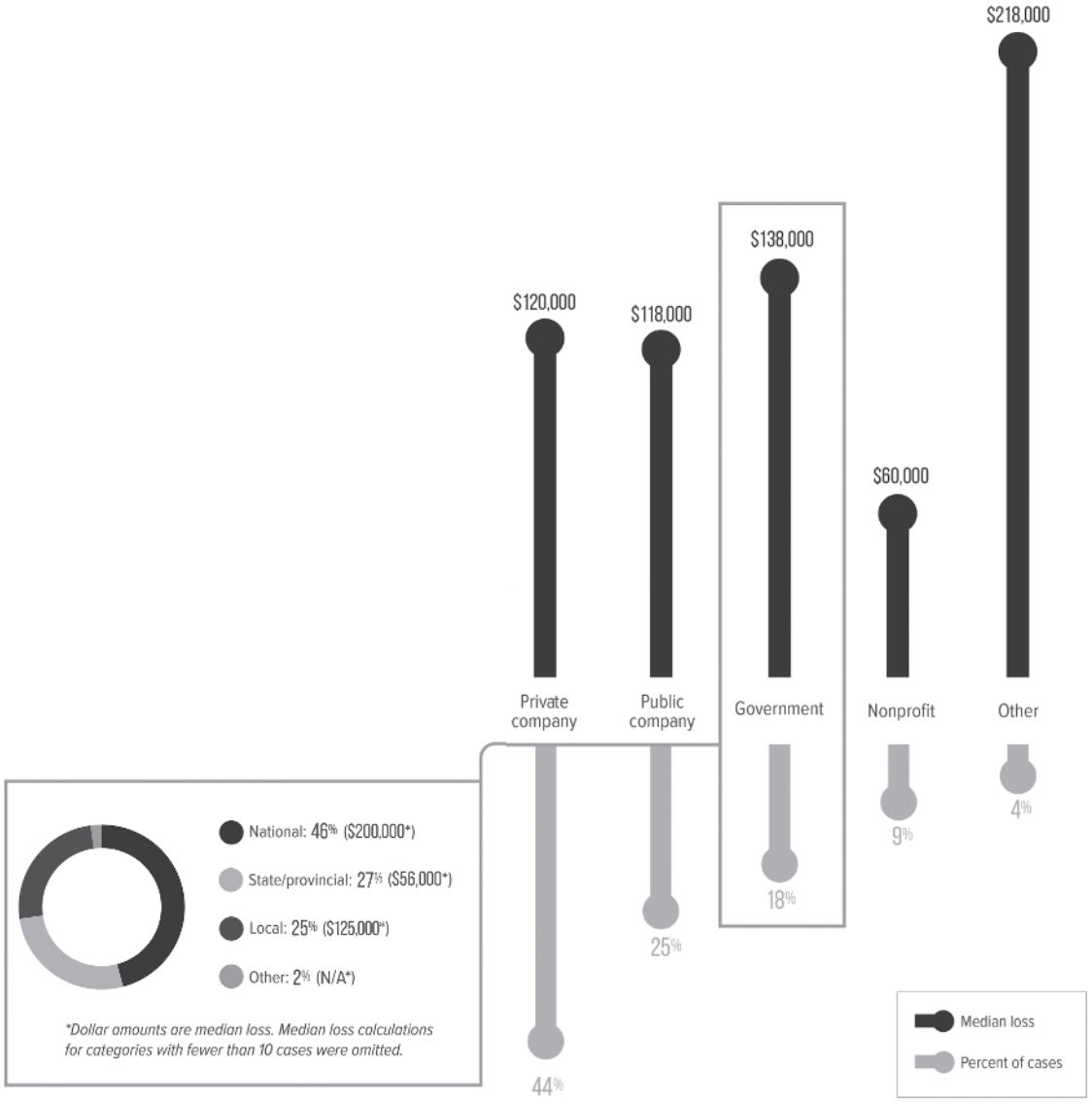


FIGURE 1-14 Type of victim organization—frequency and median loss

nonexistent sanctions faced by those caught committing fraud. Leaving aside the debate as to what factors are effective in deterring fraud, the survey sought to measure how organizations responded to 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. (Figure 1-19)

Criminal Prosecutions and Their Outcome

In 58% of the cases, the victim organization referred the case to law enforcement authorities.

For those cases that were resolved, the percentage of defendants who pleaded guilty or no contest has remained fairly constant over time. The rate of cases in which authorities declined to prosecute increased from 12% in 2020 to 17% in 2022. Combining guilty pleas and convictions at trial, 66% of cases submitted for prosecution resulted in a finding of guilt in 2022, while 10% of such prosecutions ended in acquittal. Although the percentage of cases referred to prosecution decreased from the 2016 to the 2022 reports, the percentage of cases that prosecutors successfully pursued increased.[14]

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, the survey provided respondents with a list of commonly cited explanations and asked them to mark any that applied to their case. Figure 1-20 summarizes the results. Internal discipline was sufficient (50%) and was the most commonly cited reason, followed by fear of bad publicity (30%) and a private settlement being reached (28%).

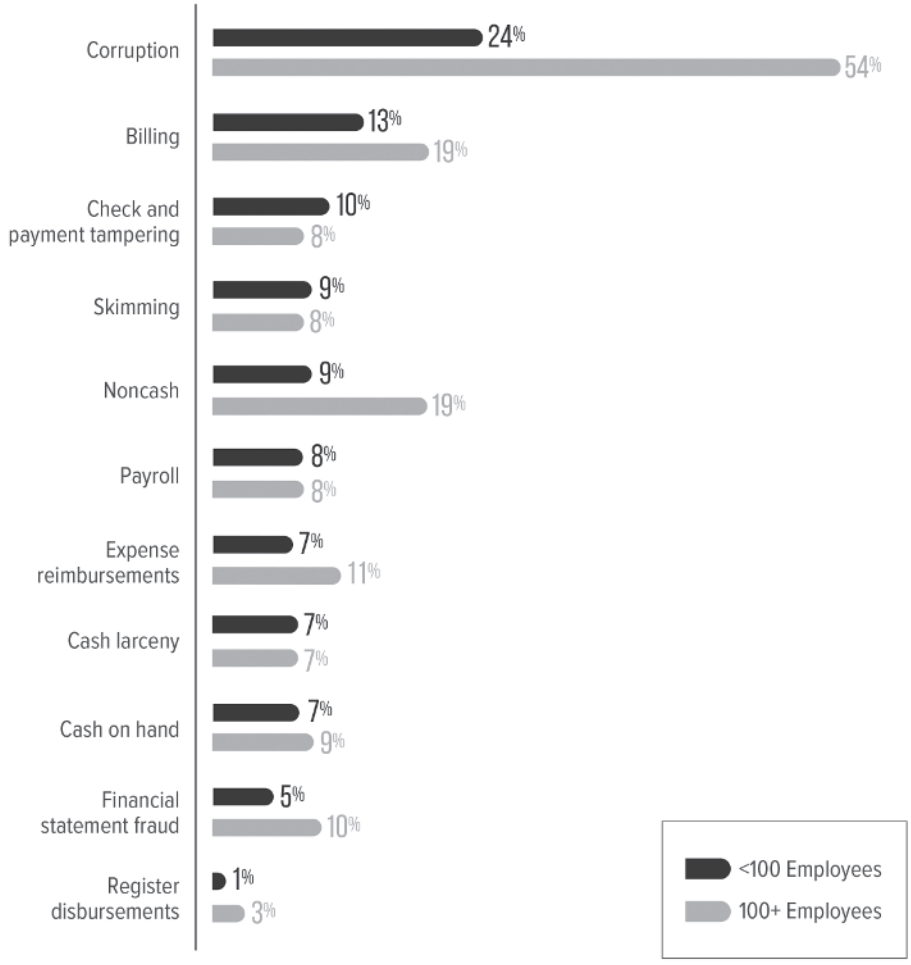


FIGURE 1-15
Size of victim organization—frequency
Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

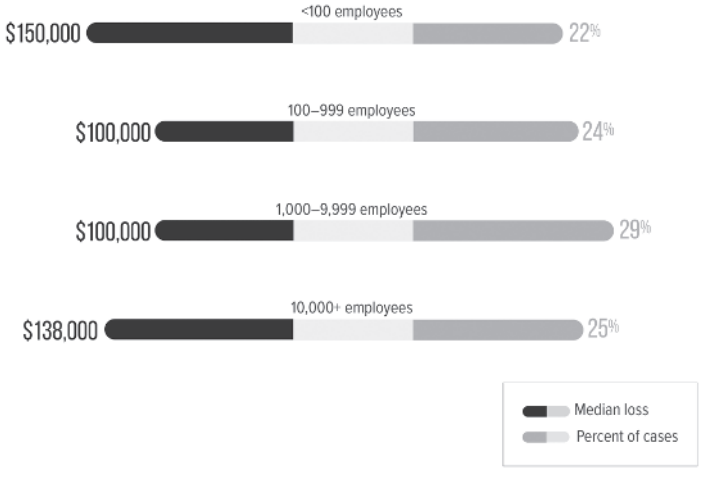


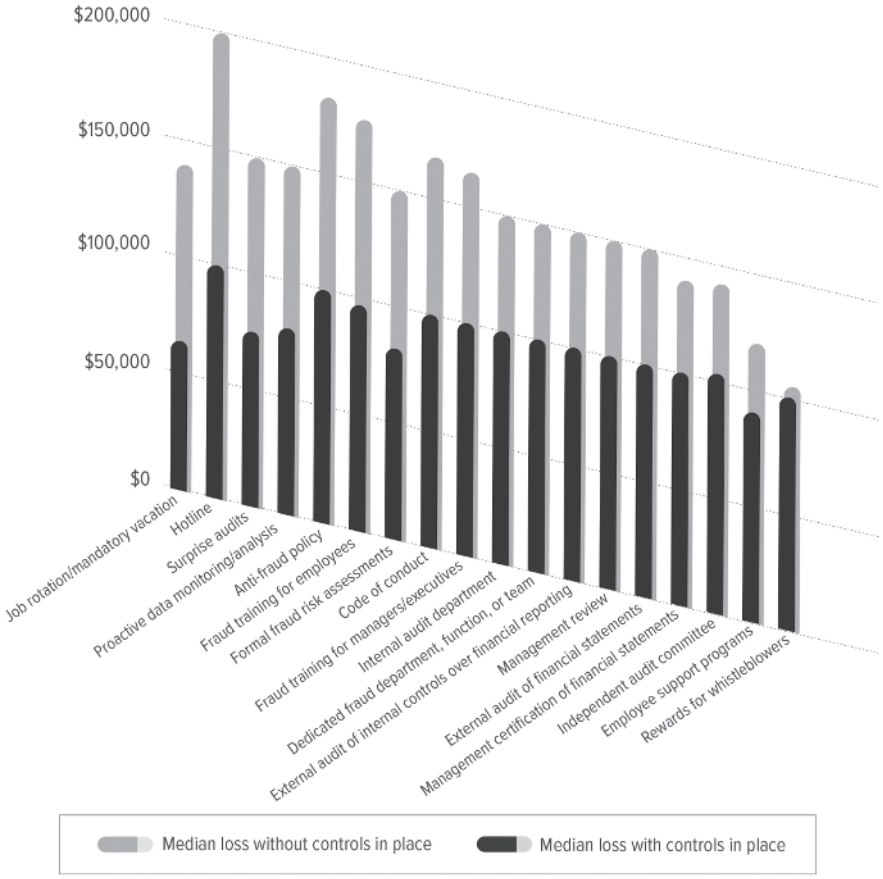
FIGURE 1-16
Size of victim organization—median loss

Module 6: The Investigation

The Mindset: Critical Thinking and Professional Skepticism

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

It can be challenging to conduct a forensic accounting engagement or fraud examination unless the investigator is prepared to look beyond his or her value system. In short, the most effective way to catch a fraudster, is to think like one. In a forensic accounting engagement, such as a breach



Control	Percent of cases	Control in place	Control not in place	Percent reduction
Job rotation/mandatory vacation	25%	$ 64,000	$140,000	54%
Hotline	70%	$100,000	$200,000	50%
Surprise audits	42%	$ 75,000	$150,000	50%
Proactive data monitoring/analysis	45%	$ 80,000	$150,000	47%
Anti-fraud policy	60%	$100,000	$183,000	45%
Fraud training for employees	61%	$ 97,000	$177,000	45%
Formal fraud risk assessments	46%	$ 82,000	$150,000	45%
Code of conduct	82%	$100,000	$168,000	40%
Fraud training for managers/executives	59%	$100,000	$165,000	39%
Internal audit department	77%	$100,000	$150,000	33%
Dedicated fraud department, function, or team	48%	$100,000	$150,000	33%
External audit of internal controls over financial reporting	71%	$100,000	$150,000	33%
Management review	69%	$100,000	$150,000	33%
External audit of financial statements	82%	$100,000	$150,000	33%
Management certification of financial statements	74%	$100,000	$140,000	29%
Independent audit committee	67%	$103,000	$142,000	27%
Employee support programs	56%	$ 90,000	$120,000	25%
Rewards for whistleblowers	15%	$100,000	$105,000	5%

FIGURE 1-17
Effectiveness of controls

of a contract, the examiner needs to focus on what actions were taken, when they were taken, and if the underlying facts and circumstances are consistent with the actions of the plaintiff or defendant.

PCAOB AS 2401.13 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

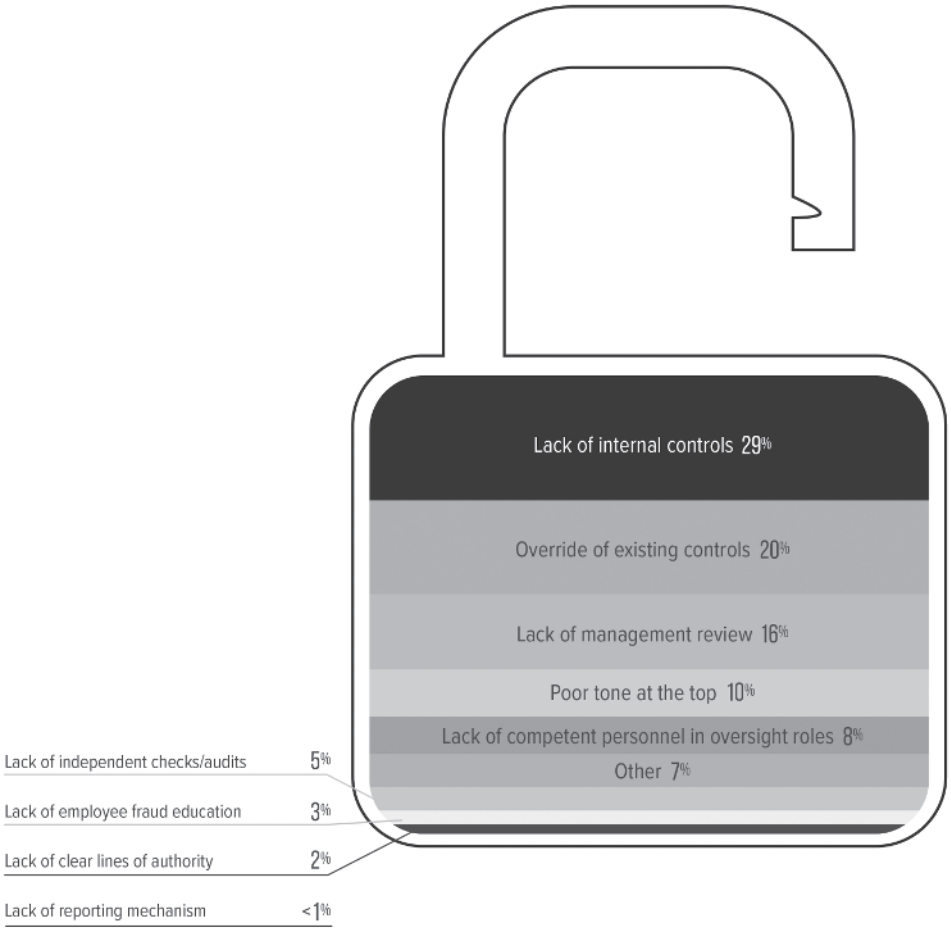


FIGURE 1-18
Primary internal control weakness observed by CFE

At a minimum, professional skepticism is a neutral but disciplined approach to detection and investigation. AS 2401 suggests that an auditor neither assumes that management is dishonest nor assumes unquestioned honesty. Professional skepticism, conceptually, drives forensic accounting engagements; keeping an open mind and letting the evidence guide one's opinions and conclusions. 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 threads: 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 of dollars.

Fraud Risk Factors and "Red Flags"

What do these loose threads look like in practice? Fraud professionals and forensic accountants refer to loose threads as anomalies, relatively small indicators, facts, figures, relationships, patterns, and 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."***[15]

Fraud professionals and forensic accountants use the term *red flags* 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.

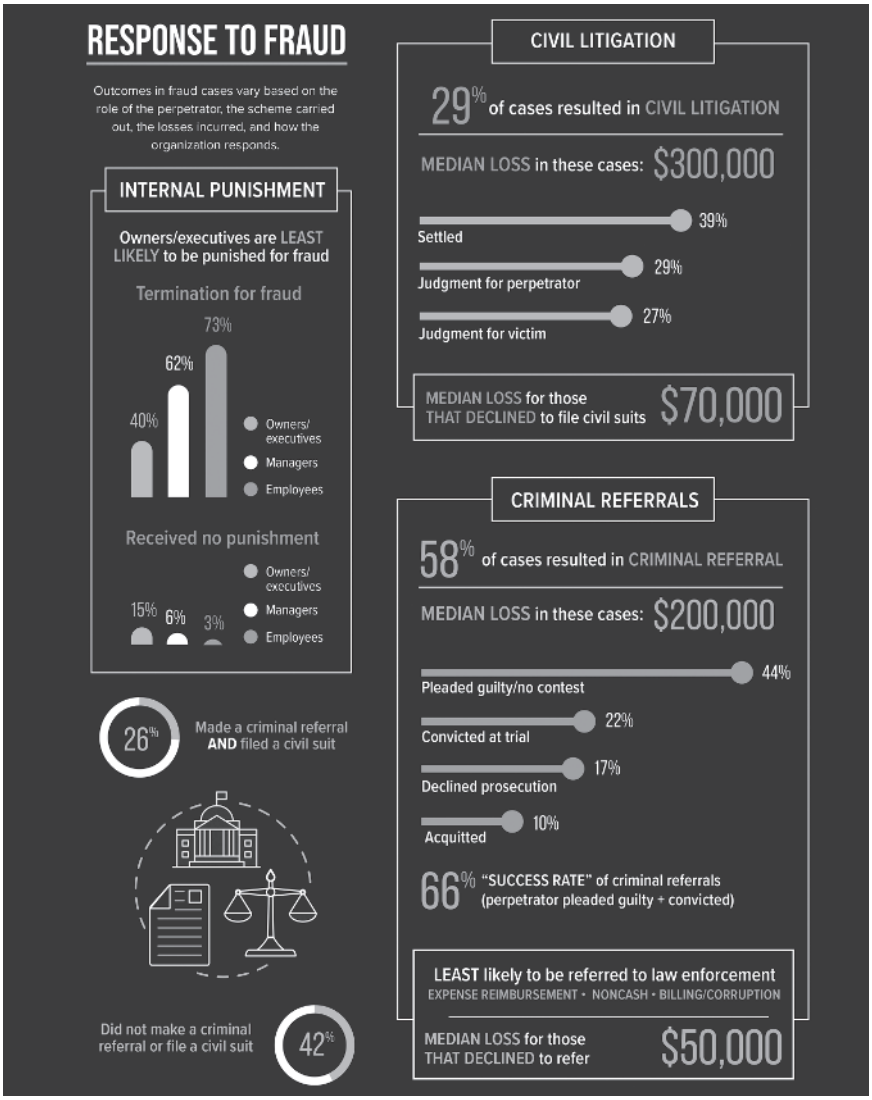


FIGURE 1-19
Results of cases referred to law

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 counter to their client's claims. Opposing council is always looking for weaknesses in your client's case, so whether the professional is investigating fraud or other litigation issues, it is critical that the forensic accountant maintain a sense of professional skepticism, look for red flags, and pull on loose threads.

Fraud risk factors generally fall into three categories:

- Motivational: Is management focused on short-term results or personal gain?
- Situational: Is there ample opportunity for fraud?
- Behavioral: Is there a company culture for a high tolerance of risk?

Evidence-Based Decision Making

Evidence and other legal issues are explored in depth in a later chapter. For now, we'll use the information in *Black's Law Dictionary*, which defines evidence as anything perceivable by the five senses and any proof—such as testimony of witnesses, records, documents, facts, data, or tangible objects—legally presented at trial to prove a contention and induce a belief in the minds of a jury.[16] 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 fails 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, therefore, must be the perpetrator or have done something wrong. Unfortunately, this approach fails to win the hearts and minds of prosecutors, defense lawyers, and juries, and it can result in significant embarrassment for fraud professionals or forensic accountants.

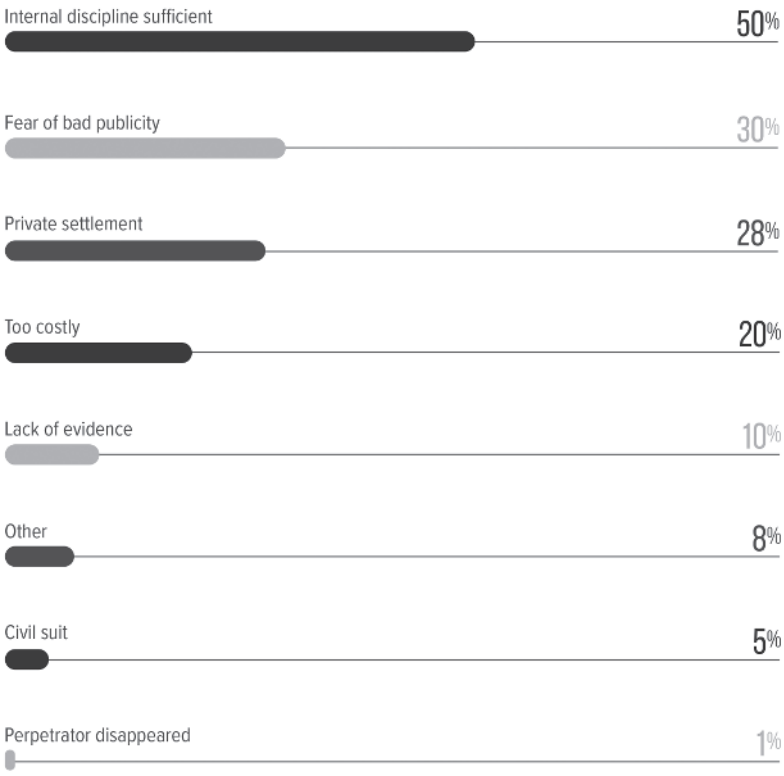


FIGURE 1-20
Reason(s) cases not referred to law enforcement

Occupation Fraud 2022: A Report to the Nations / Association of Certified Fraud Examiners, Inc

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 help prosecutors, defense lawyers, and juries to understand the full scheme under investigation. However, 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.

Scope of the Engagement

One of the biggest challenges that new forensic accountants and fraud examiners face is limiting their work to the scope of the engagement. For most fraud allegations, the engagement is much more limited in comparison to an audit. A financial statement audit is about the fairness of the financial reports (balance sheet, income statement, and statement of cash flows); this is a much broader scope than an investigation related to allegations of inappropriate expense disbursements, for example. Audits are conducted in compliance with generally accepted auditing standards (GAAS).

Regarding tax engagements: The AICPA's Statements on Standards for Tax Services (SSTSs Standards Nos. 3 and 4) and Treasury Department Circular 230, *Regulations Governing Practice Before the Internal Revenue Service* (IRS), identify tax preparers' responsibilities related to practice before the IRS. The responsibilities are different, for example, than those associated with the narrow allegations of missing deposits and inappropriate expense disbursements. Tax preparers' generally are not required to search for malfeasance, as long as they have no reason to believe that the books and records, provided by the client to prepare tax returns, have been tainted.

Whether the engagement is based on allegations associated with a civil litigation claim or a tip about a fraud act, the forensic accountant or fraud examiner needs to ensure that they have a clear understanding of the concerns. These allegations or concerns define the initial scope of the engagement. The professional needs to focus on, and examine, evidence likely to help him draw conclusions regarding the allegation(s). Not surprisingly, a fraud allegation concerning a billing scheme might spread to include travel reimbursement fraud; however, the initial effort should focus on the allegation(s) asserted, while the discovery of new evidence might lead to an expanded engagement. Similarly, in a civil litigation case, the allegations are outlined in the complaint filed with the court, and are clarified or updated over time with pleadings, discovery responses, motions and disclosures. The effective forensic accountant stays focused on the allegations and works in concert with attorneys to obtain the relevant evidence and examine the claims.

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

Although the fraud triangle helps to explain the conditions necessary for fraud to occur, to prove fraud, the investigator has to deal with the issue 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 triangle of

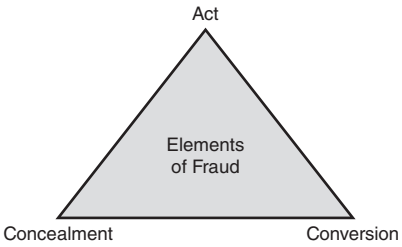


FIGURE 1-21
The triangle of fraud action: elements of fraud

fraud action, also known as the elements of fraud, is critical to the investigative process, whether the engagement includes fraud or litigation issues. The elements of fraud shown in Figure 1-21 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 the accused (the defendants) 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 breach of contract, the elements of fraud remain important: for example, what evidence suggests that a tort occurred (The Act), how did the tortuous actors benefit from their action (Conversion), and how did the tortuous actors cover up their activities (Concealment).[17]

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, document examination, and computer searches. Further, conversion can be documented by using public records searches, tracing 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, concealment, and 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., discussed in Chapter 2. 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 may take various sources of incomplete circumstantial evidence assembled into a solid, coherent case that either proves or disproves the existence of fraud. Civil litigation, by its very nature, suggests that there are at least two competing stories, that of the plaintiff and another of the defendant. Thus, as a starting point in civil litigation, the forensic accountant normally has at least two competing hypotheses. It is incumbent on the professional to use the evidence to test each of the hypotheses, as well as others that may arise based on reasonable, objective interpretation of the evidence.

To conclude an investigation without finding all the evidence related to a case is not unusual 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, these professionals utilize the fraud theory approach. 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 of what might have occurred, based on the known facts. Then that assumption is tested to determine whether it is plausible and able to be proven. The fraud theory approach involves the following steps, in the order of their occurrence:

Gather related data/evidence.
Analyze available data.
Create hypotheses.
Test the hypotheses.
Refine and amend the hypothesis.
Draw conclusions.

The Hypothesis-Evidence Matrix

Integral to the fraud theory approach is the analysis of competing hypotheses that are captured in a tool called the hypotheses-evidence matrix. This tool provides a means of testing alternative hypotheses in an organized, summary manner. 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?[18] 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 war with the United States.
Increase in frequency/length of monitoring by Iraqi agents of regional radio and TV broadcasts. Iraqi embassies instructed to take increased security precautions.

Assumption: Failure to retaliate would be an unacceptable loss of face for Saddam.
Each piece of data needs to be evaluated in terms of each hypothesis as follows:

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

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

Hypotheses:

H1	Iraq will not retaliate.	0	No diagnostic value for the hypothesis
H2	Iraq will sponsor some minor terrorist actions.	–	Does not support the hypothesis
H3	Iraq will plan and execute a major terrorist attack, perhaps against one or more CIA installations.	+	Supports the hypothesis

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

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

Notice also the direction of the "proof." We can never prove any hypothesis; in contrast, we can have two findings: (1) we have no evidence that directly refutes the most likely hypothesis and (2) we have evidence that seems to eliminate the alternative hypotheses. As an example, one of the key elements of the fraud triangle is opportunity. By charting the flow of activity and interviewing personnel, we may not be able to show with certainty that person "A" took the money, but we could eliminate those employees who 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—that is, 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 Examinations and Forensic Accounting Engagements

Essentially three tools are available, regardless of the nature of the fraud examination or forensic accounting engagement. First, the fraud examiner or forensic accountant must be skilled in the examination of financial statements, books and records, and supporting documents. Data analytics—the process of examining data to understand cause and effect—has been used successfully. In many cases, these provide the indications of fraud and/or the motivations of the parties under review. Related to such evidence, the fraud examiner must also have familiarity with the legal ramifications of evidence and how to maintain the chain of custody over evidence. For example, if it is determined that Linda Reed Collins was taking payoffs from a supplier, contracts, purchase orders, invoices, checks and other financial records related to the case must be lawfully obtained and analyzed. Ultimately, conclusions that are reached must be legally supportable.

The second tool used by these professionals is the interview, which is the process of obtaining relevant information about the matter in question 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 forensic accountants do not ask the questions, it is common for them to prepare questions for attorneys to ask, attend depositions of key financial personnel and those knowledgeable about the entity's finances, and provide the attorney with feedback and additional questions during the deposition of fact witnesses, who have financial knowledge related to the matters at hand.

FIGURE 1-22
Evidence-gathering order in fraud examinations

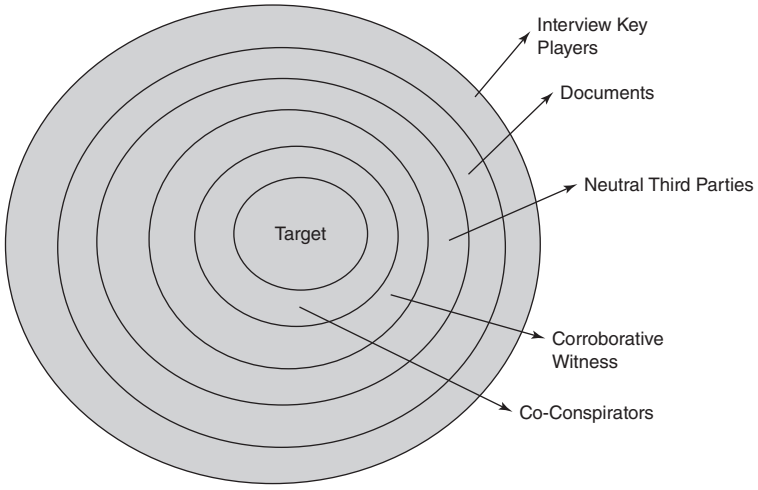


FIGURE 1-23
Fraud interview methodologies

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 1-22) and to taking witness statements (Figure 1-23). 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 for Fraudulent Financial Statements and Tax Returns

Interestingly, with fraudulent representations, such as materially misstated financial statements and false tax returns, the investigator may start 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 forensic accounting engagements is observation. Fraud examiners or forensic accountants 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 video surveillance if she discovers that Linda Reed Collins has a meeting scheduled

with a person suspected of making payoffs. In forensic litigation related to business losses, a 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 what is observed versus the payroll records will determine whether employees had been inappropriately reassigned. This methodology can be applied to virtually any type of fraud examination 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 case argued 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 all the purchases at retail. Reported sales were found to be approximately $500,000 less than the estimated sales calculated by the forensic professional.[19]

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 to estimate laundromat electricity usage, laundromat wash and dry cycle times, natural gas produced from gas wells, and tons of coal mined from underground. Nonfinancial data need not come from sources outside the company; they can be generated from internal operations and used by management. A patented data mining technique called NORA (nonobvious relationship awareness) was created to assist in determining the relationships between people.

Essentially, economists break the world into prices and quantities (p's and q's). Fraud examiners 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 if further investigation is needed. 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, the number of customer complaints, 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. 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 forensic accountants should consider this as a red flag. Finally, in most fraud examinations and forensic accounting engagements, professionals should seek out nonfinancial data to understand fully the information included in the accounting books and records.

Dates are also critical nonfinancial numbers. Allegations of fraud or a civil complaint will include a time period when the bad acts may have occurred. The fraud examiner and forensic accountant normally attempt to solicit data before, during, and after the timeframe of the alleged acts. It's critical to monitor this period around which the illegal acts are alleged to have occurred because they might offer relevant insight into the act, the concealment, and/or the conversion.

Graphical Tools

As noted in some of the critical thinking analyses, sometimes the only way to figure something out is to use graphic 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 graphic 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 needed 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. Graphic 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 forensic accounting 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. Graphic tools, such as link charts, flow charts, commodity and money flow diagrams, timelines, and other graphic 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. Software programs including PowerPoint, Excel, and Word offer tools that can be used to create graphic representations of linkages, flows, and timing. More sophisticated software such as Tableau, Visio, and I-2 can also create graphics; when used properly, these resources are able to present complicated material in an easily understandable presentation.

Big Data and Data Analytics

Almost all organizations have computer systems. These systems can capture large amounts of data, which is both a blessing and a curse. While data availability may help to further analysis and detection efforts, if it is not examined using a targeted approach, the professional might not know where to begin—everything looks anomalous or nothing looks anomalous. Data analytics and big data techniques can highlight anomalies—over time, by location, by employee—to detect fraud. Data analysis can point antifraud and forensic accounting professionals in the direction of those most likely to inform the examination. During the engagement, electronic evidence is isolated using big data and data analytics tools. Supplemental evidence gathered from a deeper examination of the details can be accumulated to conclusively prove whether the anomalies are explainable, based on the totality of the evidence.

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

To be successful, the investigator must be able to explain—to prosecutors, attorneys, juries, judges, and other participants in the investigative process—the outcome of the investigation: who, what, when, where and how. Investigations centered on the triangle of fraud action—aka the "elements of fraud" (the act, concealment, and conversion)—have the greatest chances of being successful, assuming that these investigative outcomes are grounded in the evidence.

Although fraud examiners and forensic accountants 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 these 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 communicate like a journalist telling a news story.

Teamwork and Leadership

Thinking like a fraudster may be challenging, so the use of investigative teams can be an effective tool. In cases involving large frauds, for example, investigators should use other professionals to brainstorm, interpret the significance of evidence, develop new fraud theories, and work to connect the dots. Even if the fraud professional is the only one "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 and kept "in the loop" with any new information.

Being a successful team player requires at least two attributes. First, each team member must be professionally competent at his or her assigned task. For your teammates to be able to rely on your work, they must believe that it will be completed to the highest standards. 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 an essential 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 also to individual team members. Thus, good teammates also demonstrate leadership when their unique abilities are needed by the team.

Module 7: Fraud Examination Methodology

Fraud examination is a methodology developed by the 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 that 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.[20]

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.[21]

Fraud deterrence refers to creating environments in which people are discouraged from committing fraud, although it is still possible. The 2021 *Federal Sentencing Guidelines 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.[22]

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.

This textbook provides eight types of assignments for instructors to choose from:

a. Critical Thinking
b. Review Questions
c. Multiple Choice Questions
d. Fraud Casebook
e. Brief Cases
f. Major Case Investigation (MCI)
g. IDEA Exercises
h. Tableau Exercises

CRITICAL THINKING

CT-1 **The Light Switch.** A man stands at one end of a 100-m curved hallway where he cannot see the end. Next to him are three light switches, and at the end of the hall is one incandescent light.

How many feet will the man have to walk to definitively say which light switch operates the light?

CT-2 **How Would You Prefer to Die?** A murderer is condemned to death. He has to choose between three rooms. The first is full of raging fires, the second is full of assassins with loaded guns, and the third is full of lions that haven't eaten in 3 years. Which room is safest for him?

REVIEW QUESTIONS

1. Define forensic accounting and describe two types of forensic accounting engagements.
2. Define nonfinancial data and how it's used in forensic accounting.
3. Define fraud and identify a potentially fraudulent situation.
4. Differentiate between fraud and abuse.
5. Describe the services that a forensic accountant might provide related to a marital dispute.
6. Explain the differences between an audit, fraud examination, and forensic accounting engagement.
7. Explain the triangle of fraud action (elements of fraud).
8. List the legal elements of fraud.
9. Identify common fraud schemes.
10. Give examples of nonfraud forensic and litigation advisory engagements.
11. Describe the fraud examiner/forensic accountant's approach to investigations.
12. Explain fraud examination methodology.

MULTIPLE CHOICE QUESTIONS

1. Select from the following situations the one that should ***not*** be defined as abuse:
   - **A.** A human resources employee surfs the Internet, including searching for college friends on social media during working hours.
   - **B.** A human resources employee calls in sick and then spends the day getting a car repaired, going to the DMV and shopping at a local retail outlet.
   - **C.** A human resources employee surfs the Internet, including social media during working hours for information about prospective employees.
   - **D.** A human resources employee takes their laptop home for the weekend to search for college friends on social media.
2. Given the elements of fraud in the triangle of fraud action, which element is most often associated with evidence of intent by the perpetrator?
   - **A.** The conversion
   - **B.** The concealment
   - **C.** The act
   - **D.** All three elements are indicative of intent
3. Which of the following is a true statement about fraud examination methodology?
   - **A.** Remediation requires a critical examination of internal control weaknesses.
   - **B.** Fraud can always be prevented.
   - **C.** Predication is almost always discovered near the end of the investigation.
   - **D.** Deterrence is most closely associated with making sure that perpetrators spend time in jail for their crimes.
4. Which scenario is an example of larceny?
   - **A.** Brook borrowed a company computer and didn't intend to return it.
   - **B.** Larry took cash from the register and replaced it with an IOU.
   - **C.** Mary used a company vehicle without her supervisor's permission.
   - **D.** Daniel accepted a new car from a vendor to influence his current company to purchase additional merchandise from this vendor.
5. The following evidence might be most helpful to antifraud professionals understand and possibly identify which of the following fraud perpetrators?
   - **A.** The perpetrator who has stolen from and been fired by two previous employers in the last 4 years.
   - **B.** Two perpetrators who collude to steal hundreds of thousands of dollars and split the stolen cash.
   - **C.** A financially well-off perpetrator who has been stealing from his House of Worship every week for the last 15 years.
   - **D.** The perpetrator whose spouse is diagnosed with a rare cancer that is not covered by the employee's health insurance but whose treatment will be very expensive and cost more than the employee earns and the employee was the only one with access to bank accounts and accounting records.
6. Which of the following is true with regard to the relative importance of interviewing?
   - **A.** Auditors never interview clients and interviewing plays little role in auditing.
   - **B.** In a civil litigation setting, very little interviewing is performed by attorneys through the deposition process.
   - **C.** Interviewing is an integral part of auditing, fraud examination, and forensic accounting and all such professionals should develop and refine interviewing skills.
   - **D.** In general, auditors are provided exceptional training in interviewing skills and techniques.
7. Which of the following is a true statement about fraud statistics?
   - **A.** Position tends to have only a minor impact on the frequency of fraud but higher level personnel (e.g., managers) tend to steal lower dollar amounts.
   - **B.** Men tend to steal more frequently than women.

C. Large corporations tend to be the biggest victims of fraudsters in terms of frequency and dollar losses.
D. Men and women tend to steal at the same frequency and at approximately the same dollar values.

8. Which of the following is ***not*** an essential element of fraud?
   A. A material false statement
   B. Knowledge that the statement was false when it was spoken
   C. Evidence that the statement was false
   D. Damages resulting from the victim's reliance on the false statement

9. Which of the following is a true statement about the detection of fraud?
   A. The combined frequency of tips and accidents in discovering fraud exceeds the combined frequency of internal and external audits.
   B. Law enforcement plays a significant role in the detection of white collar (economic) crimes.
   C. Internal controls when properly designed are almost bullet proof in terms of preventing fraud.
   D. For the purposes of understanding how fraud is discovered, whistleblower hotlines are the only method proven to detect fraud.

10. Which of the following would likely be characterized as a forensic accounting investigation rather than a fraud examination?
    A. An employee submits unsupported damage claims to his employer, provides false documents and statements, and deposits the insurance proceeds in his bank account.
    B. A husband submits altered bank account statements to his wife's attorney during their divorce case.
    C. A plaintiff claims that a breach of contract by a vendor resulted in a loss of business and ultimate bankruptcy.
    D. The state taxing agency has accused a state resident of filing a false tax return, claiming that income appears in their bank account but does not appear as income on their tax filings.

FRAUD CASEBOOK

Elizabeth Holmes

Read the following articles or other related articles regarding the Elizabeth Homes case and then answer the questions below.

Sources:

Carreyrou, John. "Hot Startup Theranos Has Struggled With Its Blood-Test Technology." *Wall Street Journal*. October 16, 2015.

Griffith, Erin and Erin Woo. "Elizabeth Holmes is found guilty of four counts of fraud." *The New York Times*, January 3, 2022.

Hartmans, Avery and Sarah Jackson. "The rise and fall of Elizabeth Holmes, the former Theranos CEO found guilty of wire fraud and conspiracy who is the subject of the new Hulu series 'The Dropout.'" *Insider*. March 3, 2022

Short Answer Questions

1. What type of fraud scheme did Elizabeth Holmes commit?
2. Was Theranos a public or private company?
3. What year did Elizabeth Holmes graduate from Stanford?
4. For which company (that was also infamous for its fraud) did Elizabeth Holmes' father work?
5. Which newspaper was credited with breaking the story related to Theranos and its fraudulent blood testing technology?
6. On how many criminal counts was Holmes convicted?

Discussion Questions

1. In general, would you define Theranos investors as sophisticated or naive? Why?
2. What character traits did Elizabeth Holmes display as a child and are those relevant to her ultimate conviction of committing investment fraud?
3. Fraud requires concealment. Discuss "concealment" or a similar attribute that is consistent with a fraudster covering up (concealing) their bad acts.

BRIEF CASES

1. Assume that an organization maintains and uses one checking account. Further assume that a representative of the bank where the checking account is located has alerted law enforcement that the checking account has deposit activity that has several cash deposits that are just below $10,000. As readers will learn in later chapters, the U.S. Treasury Department has reporting requirements for financial institutions that require that cash transactions of $10,000 or more be reported to the U.S. Federal Government on a Currency Transaction Report (CTR) form. CTRs are analyzed using big data and data analytics techniques to identify potential money launderers.

   Case discussion: Consider the following questions:
   a. If the deposits observed by the bank representative are less than $10,000, why is the bank representative concerned?
   b. Assuming that an examination of this issue is launched by law enforcement, what is the scope of the examination?
   c. Assuming that an examination of this issue is launched by law enforcement, should a forensic accountant or fraud examiner subpoena all bank and company records for the past five years? Why or why not?
   d. What would be the first step in an examination of this issue?

2. Assume that a company receives a tip that the company is being "ripped off." The tip alleges that a company employee with checking account and recordkeeping authority is accepting and paying invoices from a contractor for work that is not being performed and is not needed.

   Case discussion: Answer the following questions:

   a. What is the scope of work that a forensic accountant or fraud examiner would consider at this point in time? Why?
   b. How does this scope of work differ from an (i) audit of the victim company's financial statements or (ii) an engagement to complete the company's current year's tax return?
   c. Would the examination of the alleged "rip off" entail more or less work than an audit of the financial statements?

MAJOR CASE INVESTIGATION (MCI)—REAL ESTATE BROKERAGE, INC.

Real Estate Brokerage, Inc. is a major case investigation. Readers will complete one major case investigation (MCI) throughout this text; at the end of each chapter, relevant case evidence will be provided through the instructor and an assignment related to the case investigation will be described. Across the chapters of this text, assuming that one completes each chapter's assignment, the reader will complete the entire case investigation. Alternatively stated, a major case investigation and its relevant evidence has been broken into pieces and each piece or several pieces are examined at the end of each chapter; by the end of the text, the investigation will have been completed and a report written.

The purpose of the major case investigation is to provide the reader with experience in performing basic investigative tasks and analysis. The project will involve analyzing real-world, but simulated, case information, including business records to determine if fraud or a financial crime has occurred, and if so, who did it, what was done, how, when (during what date/time period), and where (e.g., what locations or organizations were involved). Students follow investigative processes used in real cases by conducting analytical reviews, soliciting information from clients, and reporting suspicious activity for a fictitious client company.

Chapter 1 MCI Introduction—Real Estate Brokerage, Inc.

Jennifer James is the broker and owner of Real Estate Brokerage, Inc., a real estate sales organization in Morgantown, West Virginia. Normally, James hires a local accounting firm on an annual basis to audit the organization's financial records. With the business in a state of rapid growth, James has been preoccupied and has forgone the audit for the last three years. Instead, her spouse, Ashford James, has exercised his somewhat rusty college accounting skills to pull the data needed for tax professionals to prepare the tax returns. In prior year, Mr. James observed no issues with the records.

During the current year's annual reconciliation of accounts, Ashford discovered discrepancies between the commission receipts from real estate closing records and the actual bank deposits. Ashford also noted that despite assurances from his wife that business has been good, the checking account balance has continued to decline and the company's bank account fell into the red (a negative number) in December, and the company bounced a few checks during the month. Ashford also noted some unusual expenditures (seemingly nonbusiness-related expenses) in the company accounts that he was not aware of; such expenditures were not observed in prior years.

Ashford James promptly but quietly filed a report with the local prosecutor, a long-time family friend and requested a thorough investigation. As a result, the prosecutor's office has contracted a regional accounting firm to perform the financial examination.

The assignment includes working with prosecutors, special agents, law enforcement, and the complainant (Ashford James). The accounting firm's managing partner has stressed the following points:

- The prosecutor's office has assigned special agents (SA) from the Task Force on White Collar Crime to conduct an investigation. Ashford James will pay all fees for this investigation. If criminal charges are found to be supported, the prosecutor's office will take the case forward.
- It is extremely difficult to schedule time with the James':
  - Jennifer James is politically well connected in the community and difficult to contact due to the nature of her business. Also, given her husband's concerns, she will not be contacted directly.
  - Ashford James is a practicing surgeon at a local hospital.
  - The couple has four children.
- Real Estate Brokerage, Inc. is a "small business" and does not employ staff accountants.
- Last month a fire at the real estate office destroyed the financial records, both paper and electronic.

In addition to compiling questions and information requests for the James' meeting, documentation of the team's working processes and discussions is to be prepared and maintained throughout the course of the case as working papers.

Assignment:
Develop a preliminary examination plan to investigate the issues described in the fact scenario:

a. Consider the various issues outlined above and think critically about how you might approach the examination.
b. Brainstorm the case issues identified and start to generate a series of questions that you, as the investigator, must answer to proceed with the investigation and "solve the case."
c. Rank order the issues and related questions.
d. Develop a data request that describes the evidentiary material required to proceed with the investigation. The data request lists physical and/or electronic evidence that might be helpful. Recall that as a forensic accountant and fraud examiner that "numbers" are your bailiwick. As such, evidence (data) could be physical or virtual, and examples might include financial numbers, financial documents, statements, invoices, cancelled checks, dates, times, contracts, databases, nonfinancial metrics, etc. Because of the fire at Real Estate Brokerage, Inc., where would you find these records? (Note: The prosecutor has subpoena power to solicit evidence from third party sources.)
e. What evidence is required to examine the issue or answer the question?
f. Submission to instructor: On 1-page, prioritize your list of issues/questions and associated data request. The submission should be in table format: column 1—issue/question, column 2—data request, column 3—time period, and column 4—purpose of data request. Each row of the table should be a separate issue/question.

Note: Academic cases are simulated and students may not receive all data requested.

IDEA EXERCISES

This assignment assumes that the instructor and students have downloaded and opened the student version of IDEA.

As of the time of this writing, you should search the following terms on the Internet: Caseware IDEA Academic Partnership. You should see this webpage.

Professors interested in incorporating IDEA into the classroom may locate this information from IDEA directly.

IDEA Case background. The overall objective of the following assignments is to complete a forensic accounting/fraud examination of the payroll records related to contractors for the period January 1, 2022 through June 30, 2023. Mon Company Legal Services provides "temporary labor" services to support in-house legal counsel. Lawyers, employed by Mon Company, are located in the United States, Canada, England and Germany. The company started in 2019.

Mon Company Legal Services has the following accounting and payroll personnel.

- The accounting controller is Jessica Gallow and she manages the payroll master file.
- The payroll manager is Alexa Benson.
- Ms. Benson gets payroll assistance from a general accounting clerk, Jenny Andrea. Ms. Andrea manages the general ledger and completes almost all reconciliations.
- The accounting department has another general accountant with no payroll duties, responsibilities, or authority, Melissa Revis. Ms. Revis is primarily in charge of accounts payable, including disbursements, and accounts receivable. Revis is also involved in the monthly general ledger closing and financial statement preparation.

Each week or upon completion of an assignment for a client, the contract laborers (attorneys) are paid; some payroll disbursements are made during weekdays other than Fridays. Legal service employees who claim 80 or more hours for a payroll period require the approval of the controller prior to payment. The attorneys are treated as employees and their payroll check can be cut on any day of the week, except Saturday and Sunday. To ensure adequate supervision, review and approval of payroll processing and disbursement, Mon Company strictly requires that payroll processing occur only on Monday–Friday. FICA (social security) and Medicare are withheld from employee paychecks. The company also enrolls all employees in a 401K retirement plan. Employees can contribute up to 6% of their salary. Since company inception, only one attorney has terminated, Terry Alinna. Ms. Alinna was one of Mon Company's first employees and a former long-time roommate of the payroll manager.

The company also incurs payroll related (company) expenses in terms of FICA (6.2%), Medicare (1.45%), and a 6% contribution to the 401K plan (whether the employee contributes or not).

Rates paid to attorney employees range from $165 per hour to a maximum of $312.50 per hour with pay rates of $165, $200, $250, or $312.50 per hour. Client mark-up is 127.3%, including employer benefit costs.

> ***As an example, a $165 hourly rate, plus employee expenses of 13.65 % for FICA—6.2%, Medicare—1.45%, and 401K—6% is a total cost to Mon Company of $187.52; the client is charged $375.05; thus, the mark-up on the base rate of $165 is 127.3% (375.05/165 = 2.273 minus 1 = 1.273 or 127.3%).***

The company runs two payrolls, one for attorney employees who provide labor services to clients. All administrative personnel, including accounting personnel are paid as part of the administrative payroll. When payroll is disbursed, each disbursement has an ordered unique identifier called "Record."

Known related parties: Alexa Benson has a sister who works for Mon Company as a contract lawyer, Evelynn Evans. Ms. Evans resides in Germany.

An examination of client profitability indicates that all clients have been billed with the appropriate mark-up. This analysis was completed on each client. Recently, two clients have complained that the costs of their services are over-budget: clients 10011 and 10080. These complaints are being handled by the sales manager and CEO and the clients seem to be very satisfied with the quality of services provided.

Assignment and Skill Summary

Number	Description	IDEA Skills
1	Importing data and ensuring that the file imports correctly	Creating a Project Import a File
2	Do any accounting or payroll personnel or related parties appear on the contractor payroll?	Summarizing Data Export a File
3	Is Mon Company in compliance with Federal withholding requirements for FICA and Medicare?	Extract: Direct Equation Editor Export a File
4	Is Mon Company in compliance with company policy that requires explicit approval of 80 hours or more?	Extract: Direct Equation Editor Sorting Data (column)
5	Does Mon Company have any duplicate payroll records?	Duplicate Key
6	Does Mon Company have any payroll processing on the weekends?	Field Statistics Using hyper-links
7	Does Mon Company have any contactor personnel whose are being paid but are not on the payroll master file?	Import a File Sorting Using Data-Sort Join
8	Does Mon Company have any contactor personnel whose have terminated but are being paid through payroll (e.g., ghost employee)?	Sorting Data (column) Extract: Key Value
9	Does Mon Company have any personnel whose last name is similar?	Summarization Fuzzy Match Using hyper-links
10	Is Mon Company in compliance with their payroll rates schedule: $165, $200, $250, and $312.50?	Summarization
11	Does the Mon Company payroll system's company expense file match to its payroll disbursements file?	Import a File Join
12	Does the payroll disbursements file being analyzed appear to have all of the payroll records disbursed during the period January 1, 2022 to June 30, 2023?	Gap Detection
13	The HR (human resources) department would like to identify all employees who are not withholding the maximum savings amount for the 401K retirement plan of 6%.	Virtual Data Equation Editor Extract: Direct Field Statistics
14	Do the payroll hours comply with Benford's Law?	Benford's Law
15	Summarize forensic accounting concerns that require follow-up examination.	n/a
16	Write a report.	n/a

IDEA—ASSIGNMENT CHAPTER 1

Student Material for step-by-step screenshots for completing the assignment are available from your instructor.

Creating a Project and Importing a File

1. The first step is to create a project.
2. The second step is to import data.

The file should have 986 records.

Student Material for step-by-step screenshots for completing the assignment are available from your instructor.

TABLEAU EXERCISES

This assignment assumes that the instructor and students have downloaded and opened the academic version of Tableau. As of the time of this writing, the web address of the Tableau Academic Programs is https:// www.tableau.com/academic

Professors interested in incorporating Tableau into the classroom may locate this information from Tableau directly.

Tableau Objective. The overall objective of the following assignments is to support, through communication and analysis, a forensic accounting/fraud examination of the payroll records related to contractors for the period January 1, 2022 through June 30, 2023.

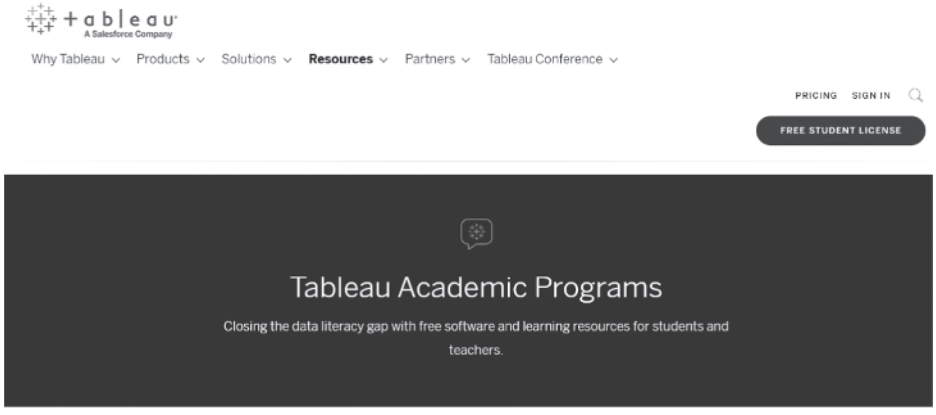


TABLEAU SOFTWARE, LLC / https://www.tableau.com/academic / last assceesd 14 April, 2023.

Tableau case background: See IDEA case background.

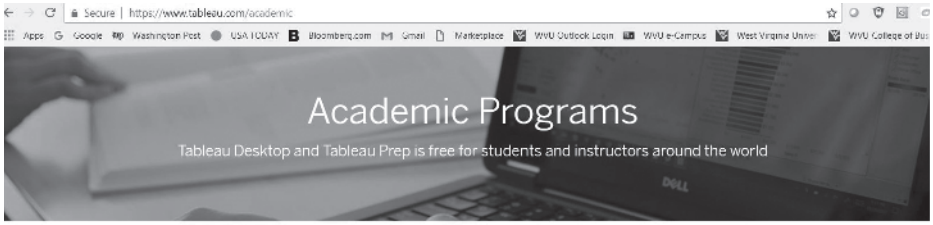


Tableau helps you see and understand your data

Whether you're a student creating scatter plots for a project or an educator instructing an economics course, Tableau will enhance learning and teaching with a fast, easy-to-use, visual analytics platform.

WATCH NOW

TABLEAU—ASSIGNMENT CHAPTER 1

Creating a Tableau Book and Connecting a File

1. The first step is to create a Tableau Book and Connect to the data.
2. The second step is to ensure that all data connected. The file should have 997 rows.

Student Material for step-by-step screenshots for completing the assignment are available from your instructor.

Endnotes

1. See Department of Justice, U.S. Attorney's Office, Northern District of Texas, "Fort Worth Man Arrested on $25 Million Health Care Fraud Scheme," October 13, 2017.
2. J. Bandler and A. Zimmerman, "A Wal-Mart Legend's Trail of Deceit," *Wall Street Journal*, April 8, 2005.
3. Henry Campbell Black, *Black's Law Dictionary*, 5th ed. (St. Paul, MN: West Publishing Co., 1979), p. 792.
4. 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.
5. Black, p. 300.
6. T. Fowler, "*Skilling Gets 24 Years in Prison for Enron Fraud*." Chron. com, October 23, 2006.
7. ACFE, "*Cooking the Books: What Every Accountant Should Know*," Austin, TX, 1993.
8. National Commission on Fraudulent Financial Reporting, "*Report to the National Commission on Fraudulent Financial Reporting*," NY, 1987.
9. 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.
10. Adapted from D. Larry Crumbley, Lester E. Heitger, and G. Stevenson Smith, *Forensic and Investigative Accounting*, 2005. See also: AICPA Business Valuation and Forensic & Litigation Services.
11. Source unknown.
12. 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.
13. Adapted from *Occupational Fraud and Abuse*, Joseph T. Wells (Obsidian Publishing Company,1997).
14. 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.
15. See http://www.answrs.com/red%20flag.
16. *ACFE's Fraud Examiners Manual*, Section 2.601.
17. 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.
18. The authors are grateful to West Virginia University Professor Jason Thomas who first shared this example with the forensic accounting and fraud examination students.
19. James DiGabriel (ed.), *Forensic Accounting in Matrimonial Divorce* (2005), pp. 51–52.
20. Adapted from *ACFE Fraud Examiners Manual*.
21. W. Steve Albrecht, *Fraud Examination*, 2003.
22. 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.

APPENDIX I

Careers in Fraud Examination and Financial Forensics

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

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

Background

Recent corporate accounting and financial scandals have led to increased legal and regulatory requirements, such as the Sarbanes–Oxley Act of 2002, the Emergency Economic Stabilization Act of 2008 (EESA), the Dodd–Frank Act, and the UK Bribery Act. These requirements address internal controls for detecting and deterring fraud and other economic crime. They also encourage financial statement auditors and organizational governance leaders to be more aggressive in searching for fraud and financial malfeasance, as well as challenging accountants, corporate governance, and other professionals to conduct risk assessments to mitigate the occurrence of fraud.

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

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

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

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

The demand for students who have specialized qualifications in fraud and financial forensics has grown significantly and is likely to continue to grow. The increasing demand is creating an unprecedented opportunity for those professionals who develop the knowledge, skills, and abilities associated with fraud examination and forensic accounting. For example, the Bureau of Labor Statistics (BLS) predicts 10% job growth for accountants and auditors from 2016 to 2026.[1] Moreover, each of the largest accounting firms is now recruiting accounting students with some exposure to forensic accounting, fraud examination, anticorruption and related knowledge, skills, and abilities. The need for competent staffing at the SEC, at PCAOB, and in private industry is outpacing the supply. It is hard to envision a more stable and in-demand career.

Places Where Fraud Examiners and Financial Forensic Specialists Work

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

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

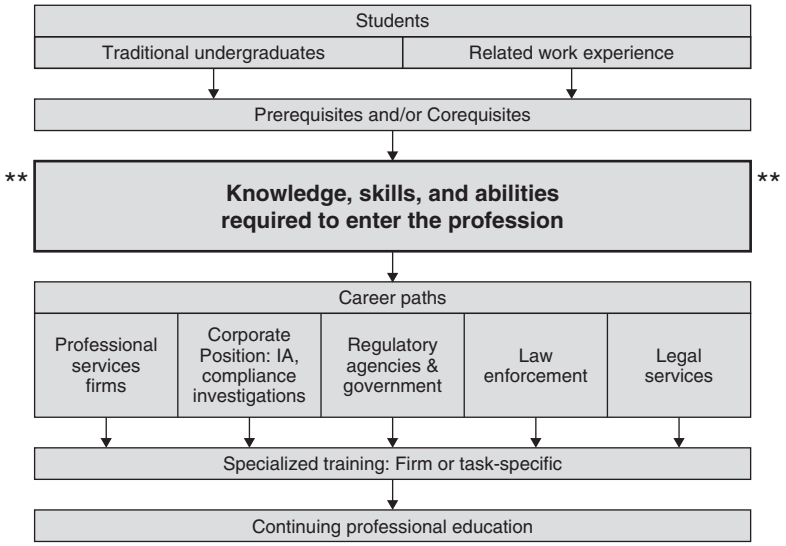


FIGURE 1A-1
Career paths

Professional Services Firms

Fraud examiners and financial forensic specialists work in accounting and professional service firms that provide fraud deterrence, detection, investigation, and remediation services to a variety of organizations. In addition, professional service firms, specialized service, and boutique services firms provide litigation advisory services to individuals, as well as to businesses and other entities. Fraud risk assessments, including consideration of financially motivated illegal acts, are now integral to organizational governance.

Public and Private Companies

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

According to the Association of Certified Fraud Examiners' 2018 "Report to the Nations," internal auditors discover a significantly greater percentage of fraud than external auditors do. Many internal audit departments employ certified fraud examiners (CFE) and forensic accountants.

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

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

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

Regulatory Agencies

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

Government and Nonprofits

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

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

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

Nonprofit entities may include public school systems, charities, hospitals, and other health-care facilities. According to the ACFE 2022

RTTN, nonprofit organizations were the most likely to modify their anti-fraud controls (87%), as compared to public and private companies (each 83%), or governmental agencies (74%). The challenges, related to fraud examination and forensic accounting, have bled over to the public sector, and many of these organizations are hiring professionals with expertise in these areas.

Law Enforcement Agencies

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

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

Law Firms

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

Related Professions

Law

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

Psychology

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

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

Sociology

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

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

Criminology

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

Intelligence

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

Information Systems and Computer Forensics

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

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

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

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

Information Systems Governance and Controls

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

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

Cyberforensics

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

Digital Evidence

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

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

Electronic Detection and Investigation

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

Cybercrime

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

Other Forensic Science Fields

Fraud examination and forensic accounting also utilize knowledge, skills, and abilities from other forensic sciences such as crime scene investigation, forensic chemistry, and biology. For example, in crime scene investigation, the investigator has three primary goals: protection of evidence (e.g., crime scene tape), preservation of evidence, and collection of evidence. Although an accounting department and the IT systems cannot be "roped off" with crime scene tape, it is important for the fraud examiner or forensic accountant to be thinking about three concepts: (1) protecting the evidence by using backup tapes of the computer system collected and

protected in such a way as to be admissible in court, (2) preserving the evidence by preventing physical and electronic corruption and destruction, and (3) collecting the evidence in sufficient amounts and in a manner that protects the chain of custody. These types of lessons are routinely available from our colleagues in other forensic fields.

Related Career Titles

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

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

Business Administration, Management, and Corporate Governance

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

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

The following outlines the basics of fraud risk management for those charged with corporate governance: the board of directors, the audit committee, management, internal auditors, and external auditors. "Managing the Business Risk of Fraud: A Practical Guide," developed by the IIA, AICPA, and ACFE, suggests that with regard to corporate malfeasance, fraud risk management needs to include five key features[3]:

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

Boards of Directors

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

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

Audit Committees

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

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

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

To be proactive, the audit committee should ensure that

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

Senior/Executive Management

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

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

Internal Audit

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

External (Independent) Audit

Financial statement fraud has been, and continues to be, the focus of the auditing profession. During the early 1900s, external auditors viewed the detection of fraud, particularly financial statement fraud, as the primary purpose of their financial audit. During the twentieth century, the auditing profession moved from acceptance of fraud detection as their primary responsibility to the mere expression of an opinion on the fair presentation of the financial statements. Recently, the accounting profession directly addressed the external auditor's responsibility to detect financial statement fraud in its AU 316, Statement on Auditing Standards (SAS) No. 99/113, titled "Consideration of Fraud in a Financial Statement Audit" SAS No. 99/113 requires independent auditors to obtain information to identify financial statement fraud risks, assess those risks while taking into account the entity's programs and controls, and respond to the results of this assessment by modifying their audit plans and programs.

Auditors in identifying and assessing the risks of material financial statement fraud should (1) make inquiries of the audit committee or other comparable committee of the board of directors, senior executives, legal counsel, chief internal auditors, and others charged with government governance within the client organization to gather sufficient information about the risk of the fraud, (2) communicate with the

audit committee, management, and legal counsel about the allegations of fraud and how they are addressed, (3) consider all evidence gathered through analytical procedures that is considered unusual, unexpected, or even suspiciously normal based on the financial condition and results of the business, and (4) consider evidence gathered through the audit of internal control of financial reporting that may suggest the existence of one or more fraud risk factors, and that adequate and effective internal controls did not address and account for the detected risk. Auditors should inquire of the audit committee, management, and others charged with government governance about the entity's antifraud policies and procedures and whether they are in writing, updated on a timely basis, implemented effectively, and enforced consistently.

Regulators and Governing Bodies

Regulatory reforms in the United States are aimed at improving the integrity, safety, and efficiency of the capital markets while maintaining their global competitiveness. Regulations should be perceived as being fair and in balance in order to inspire investor confidence. Regulations, including SOX, are aimed at protecting investors. The provisions of SOX- and SEC-related rules include strengthening the corporate board and external auditor independence, instituting executive certifications of both financial statements and internal controls, and creating the PCAOB to oversee the accounting profession. These provisions helped to rebuild investor confidence in public financial information.

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

Professional Organizations and their Related Certifications

Association of Certified Fraud Examiners (ACFE)

The ACFE is the world's premier provider of antifraud training and education. Together with its nearly 85,000 members, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity within the profession. The mission of the Association of Certified Fraud Examiners is to reduce the incidence of fraud and white-collar crime and to assist the membership in fraud detection and deterrence. To accomplish its mission, the ACFE

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

Certified Fraud Examiner (CFE)

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

American Institute of Certified Public Accountants (AICPA)

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

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

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

Accredited in Business Valuation (ABV)

The mission of the ABV credential program is to provide a community of business valuation experts with specialized access to information, education, tools, and support that enhance their ability to make a genuine difference for their clients and employers. The ABV credential program allows credential holders to brand or position themselves as CPAs or finance professionals, who are premier business valuation service providers. ABV credential holders differentiate themselves by going beyond the core service of reaching a conclusion of value to also create

value for clients through the strategic application of this analysis. The ABV credential program is designed to

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

Certified Information Technology Professional (CITP)

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

Certified in Financial Forensics (CFF)

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

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

ACAMS: Association of Certified Anti-Money Laundering Specialists

ACAMS is an international organization dedicated to advancing the professional knowledge, skills, and experience of those dedicated to the detection and prevention of money laundering around the world and to promote the development and implementation of sound anti-money laundering policies and procedures. ACAMS achieves its mission through

- promoting international standards for the detection and prevention of money laundering and terrorist financing;
- educating professionals in private and government organizations about these standards and the strategies and practices required to meet them;
- certifying the achievements of its members; and
- providing networking platforms through which AML/CFT professionals can collaborate with their peers throughout the world.

Certified Anti-Money Laundering Specialist (CAMS)

The CAMS credential is a gold standard in AML certifications and recognized internationally by financial institutions, governments, and regulators as a serious commitment to protecting the financial system against money laundering. The ACAMS organization also offers advanced certification programs in audit and financial crimes investigations.

Forensic CPA Society (FCPAS)

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

Forensic Certified Public Accountant (FCPA)

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

Information Systems Audit and Control Association (ISACA)

Since its inception, ISACA has become a pace-setting global organization for information governance, control, security, and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide. Its research pinpoints professional issues challenging its constituents, and its Certified Information Systems Auditor (CISA) certification is recognized globally. The Certified Information Security Manager (CISM) certification uniquely targets the information security management audience and has been earned by more

than thousands of professionals. The Certified in the Governance of Enterprise IT (CGEIT) designation promotes the advancement of professionals who wish to be recognized for their IT governance-related experience and knowledge. It publishes a leading technical journal in the information control field (the Information Systems Control Journal) and hosts a series of international conferences focusing on both technical and managerial topics pertinent to the IS assurance, control, security, and IT governance professions. Together, ISACA and its affiliated IT Governance Institute lead the information technology control community and serve its practitioners by providing the elements needed by IT professionals in an ever-changing worldwide environment.

Certified Information Systems Analyst (CISA)

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

Certified Information Security Manager (CISM)

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

Institute of Internal Auditors (IIA)

Established in 1941, the Institute of Internal Auditors (IIA) is an international professional association of more than 150,000 members with global headquarters in Altamonte Springs, Florida. Worldwide, the IIA is recognized as the internal audit profession's leader in certification, education, research, and technical guidance. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator. Members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security. The mission of the IIA is to provide dynamic leadership for the global profession of internal auditing. Although the institute does not have a designation directly associated with fraud examination and forensic accounting, its dedication to this area is demonstrated in its training programs, its work with the Institute for Fraud Prevention, and its leadership in developing (along with the ACFE and AICPA) "Managing the Risk of Fraud: A Practical Guide."

Certified Internal Auditor

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

National Association of Certified Valuators and Analysts (NACVA)

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

Certified Valuation Analyst (CVA)

NACVA trains and certifies CVAs to perform business valuations as a service to both the consulting community and the users of their services. Through training and examination requirements, including a valuation exercise, CVAs demonstrate qualifications to provide capable and professionally executed valuation services. NACVA recommends specific training as a prerequisite to certification to assure that practitioners have the knowledge and understanding necessary to perform competent services and to assure a level of consistency and continuity in their work product.

Master Analyst in Financial Forensics (MAFF)

The MAFF credential is designed to provide assurance to the legal and business communities—the primary users of financial litigation services—that the designee possesses a level of experience and knowledge deemed acceptable by the Association to provide competent and professional financial litigation support services. To earn the MAFF credential, candidates must attest to having met certain prerequisites and an experience requirement, plus pass a five-hour proctored exam that tests the NACVA's Financial Forensics Body of Knowledge (FFBOK). To prepare for the exam, NACVA sponsors and recommends a five-day course entitled, Financial Litigation Consulting Professionals Workshop (previously titled Foundations of Financial Forensics Workshop). To support the MAFF designees and the entire financial forensics discipline, NACVA offers intermediate to advanced training in eight areas of specialized focus (specialty areas).

Accredited in Business Appraisal Review (ABAR)

The ABAR designation certifies competence in the review of business appraisal reports. As such, the ABAR credential is specially designed for business valuators whose work involves the review of valuation reports and analysis performed by others, including managers, expert witnesses, attorneys, coaches, mentors, trainers, and government appraisers.

Society of Financial Examiners (SOFE)

The Society of Financial Examiners is a professional society for examiners of insurance companies, banks, savings and loans, and credit unions. The organization has a membership representing the fifty states, the District Education: Building Knowledge, Skills, and Abilities in

Fraud Examination and Financial Forensics of Columbia, Canada, Aruba, and the Netherlands Antilles. SOFE is the one organization in which financial examiners of insurance companies, banks, savings and loans, and credit unions come together for training and to share and exchange information on a formal and informal level. The society was established in 1973 to establish a strict code of professional standards for members engaged in the examination of financial institutions, to promote uniform ethical standards to engender employer and public confidence to the degree that those interested can identify professionally qualified practitioners, and to promote and enforce minimum requirements of conduct, training, and expertise for members engaged in financial examination. SOFE offers three professional designations, which may be earned by completing extensive requirements including the successful completion of a series of examinations administered by the society. The designations are Accredited Financial Examiner, Certified Financial Examiner, and Automated Examiner Specialist.

International Fraud Examination and Financial Forensics

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

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

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

Education: Building Knowledge, Skills, and Abilities in Fraud Examination and Financial Forensics

The progression of knowledge, skills, and abilities for fraud and forensic accounting for entry-level professionals is presented in Figure 1A-2 (from the DOJ's National Institute of Justice model curriculum project "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students"; available through the National Criminal Justice Reference Service at www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf). This section and Figure 1A-2 (NCJRS) were developed with the extensive use of the DOJ's project. This project was also highlighted in the November 2008 volume of Issues in Accounting Education.

As noted above, fraud examination and financial forensics embrace many more disciplines than simply accounting. Those disciplines and professions include law, psychology, sociology, criminology, intelligence, information systems, computer forensics, and the greater forensic science fields. One of the challenges for individuals with these backgrounds is that most fraud and financial forensics engagements require at least some knowledge of accounting, finance, and economics because of the nature of the work. Thus, the NCJRS addresses prerequisite accounting, auditing, and business law knowledge that is considered necessary for the fraud and financial forensics curriculum. Students with an accounting degree will have met these prerequisites as part of their degree requirements. Students who do not have an accounting degree will need to obtain the prerequisite knowledge and skills before embarking on the fraud examination and financial forensics curriculum. That prerequisite knowledge, skills, and abilities can be developed through experience, and many educational programs recognize past professional accomplishments.

Figure 1A-2 depicts the continuum of knowledge development, transfer (education), and use in practice.

Prerequisite Knowledge and Skills

The knowledge and skills students should obtain when they study fraud and financial forensics include the following[4]:

Basic Accounting Concepts

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

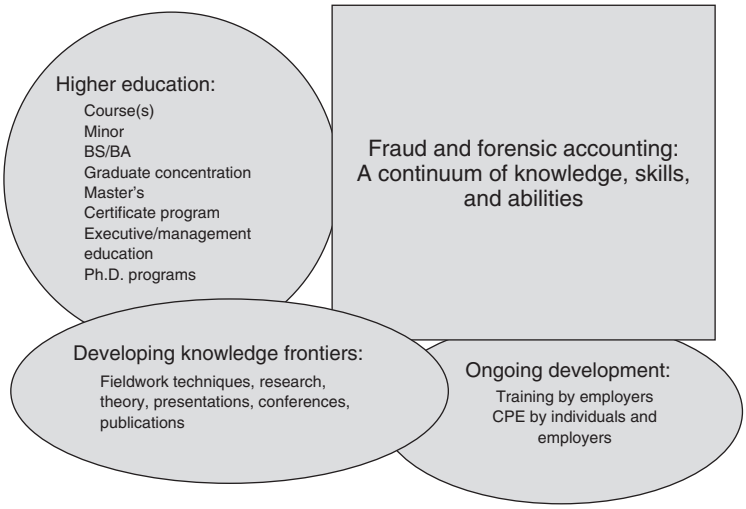


FIGURE 1A-2
Fraud examination and forensic accounting: A continuum of knowledge, skills, and abilities

Basic Auditing Concepts

- The basic elements of auditing, including professional skepticism in evaluating statements or representations made
- Different types and quality of audit evidentiary matter and how to evaluate types of evidence (definitive, circumstantial, direct, corroborative, and conflicting)
- Relevant current accounting and auditing standards and the roles and responsibilities of standard-setting, professional, and regulatory bodies
- Organization and development of working papers

Transaction Processing Cycles and Control Environment

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

Basic Finance and Economics

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

Business Law Concepts

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

General Business Communications Skills and Business Ethics

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

Basic Computer Skills

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

Exposure Material/Course

NCJRS shows the exposure to fraud and forensic accounting topics that may be covered in an undergraduate or graduate accounting curriculum. Colleges, universities, and other curriculum providers may use this outline of topical areas as a guide to provide exposure to students by incorporating coverage in current offerings or may add a single course/training module. Some of these topics are covered briefly—for example, as one chapter in the auditing text or one chapter in the accounting systems text. Because the coverage of these topics in traditional texts is relatively minimal, they should be reinforced and explored in greater depth as part of the fraud and forensic accounting curriculum.

In-Depth Course Material

NCJRS also provides an overview of the model curriculum areas required for in-depth study. Entry-level fraud and forensic accounting professionals should possess knowledge, skills, and abilities in the following areas:

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

The Role of Research in a Profession

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

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

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

Endnotes

1. www.bls.gov/ooh/business-and-financial/mobile/accountants-and-auditors.htm
2. Figure 1A-1 was developed as part of the DOJ's National Institute of Justice model curriculum project "Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty and Students," www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf.
3. "Managing the Business Risk of Fraud: A Practical Guide," The Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), and Association of Certified Fraud Examiners (ACFE), 2008, http://www.acfe.com/documents/managing businessrisk.pdf.
4. University students who develop an early interest in fraud and forensic accounting may also want to take criminology and risk management courses to the extent that such courses are available and fit into their course of study.