Professional Education Services, LP

Introduction to Forensic Accounting and Fraud Examination

#8315

COURSE MATERIAL

Professional Education Services, LP

The Professional's Choice for Quality CPE.

4208 Douglas Blvd. • Suite 50

Granite Bay, CA 95746 • www.mypescpe.com

1-800-998-5024 • Customer Service: 1-800-990-2731

Fax: 916-791-4099

TABLE OF CONTENTS

NOTICE

This course and test have been adapted from supplemental materials and uses partial text from the materials entitled *Forensic Accounting and Fraud Examination* by Mary-Jo Kranacher and Richard A. Riley, Jr. © 2020 by John Wiley & Sons, Inc. Displayed by permission of the publisher, John Wiley & Sons, Inc., Hoboken, New Jersey.

The views expressed in this text are those of the author(s) and do not necessarily reflect the views, opinions, or positions of Professional Education Services, LP, its employees, or owners.

Use of these materials or services provided by Professional Education Services, LP ("PES") is governed by the *Terms and Conditions* on PES' website (www.mypescpe.com). PES provides this course with the understanding that it is not providing any accounting, legal, or other professional advice and assumes no liability whatsoever in connection with its use. PES has used diligent efforts to provide quality information and material to its customers, but does not warrant or guarantee the accuracy, timeliness, completeness, or currency of the information contained herein. Ultimately, the responsibility to comply with applicable legal requirements falls solely on the individual licensee, not PES. PES encourages you to contact your state Board or licensing agency for the latest information and to confirm or clarify any questions or concerns you have regarding your duties or obligations as a licensed professional.

Program Publication Date 11/29/2023

This course is one of a series of courses for Fraud Examination that builds a comprehensive understanding of this important topic. They may be taken in order, taken individually or all together.

Course #8315 *Introduction to Forensic Accounting and Fraud Examination*

Course #8320 *Fraud Schemes*

Course #8325 *Detection and Investigative Tools and Techniques in Fraud Examination*

Course #8330 *Additional Topics in Forensic Accounting and Fraud Examination*

Course #8335 *Fraud Examination: Litigation Advisory Services and Remediation*

Please note: As this is a new series, some of the courses listed may still be in the development phase and not yet available. Please check our website at www.mypescpe.com for full course descriptions and availability.

CHAPTER 1: CORE FOUNDATION RELATED TO FORENSIC ACCOUNTING AND FRAUD EXAMINATION

Chapter Objective

After completing this chapter, you should be able to:

- Recall the three categories of organizational fraud that make up the occupational fraud and abuse classification system (fraud tree).

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% (4,200 of 6,000 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 extent of damage (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 is no longer alive.

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 with 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 relation to his fraudulent billing of United HealthCare Services, Inc., Aetna, Inc., and Cigna.*

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.

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 red flags.
- Module 7 provides an overview of the key elements of fraud examination. Fraud examination is more than just investigation of allegations and 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: Wal-Mart 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 Wal-Mart's Board of Directors. Mr. Coughlin, fifty-five years old at the time, periodically had subordinates create fake invoices to get the company to pay for his personal expenses. The questionable activity appeared to involve dozens of transactions over more than five years, including hunting vacations, custom-made alligator boots, and

an expensive dog pen for his family home. Wal-Mart indicated that it found questionable transactions totaling between $100,000 and $500,000. In his last year, Mr. Coughlin's compensation totaled more than $6 million. Interestingly, Mr. Coughlin was an outspoken critic of corporate chicanery. In 2002, he told the *Cleveland Plain Dealer*, "Anyone who is taking money from associates and shareholders ought to be shot."[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

2. J. Bandler and A. Zimmerman, "A Wal-Mart Legend's Trail of Deceit," Wall Street Journal, April 8, 2005.

owner thereof."[3] In order to prove that a person has committed larceny, we would need to prove the following four elements:

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

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

The employee might also be accused of having committed a tort known as conversion.[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." In order for an embezzlement to occur, the person who stole the property must have been entitled to possession of the property at the time of the theft. Remember, possession is not the same as ownership. In our example, the employee might be entitled to possess the company's computer chips (to assemble them, pack them, store them, etc.), but clearly the chips belong to the employer, not the employee. When the employee steals the chips, he has committed embezzlement.

We might also observe that some employees have a recognized fiduciary relationship with their employers under the law. The term fiduciary, according to *Black's Law Dictionary*, 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.

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.

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.

6. T. Fowler, "Skilling Gets 24 Years in Prison for Enron Fraud." Chron.com, October 23, 2006.

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 2016 Report to the Nations on Occupational Fraud and Abuse noted that financial fraud tends to be the least frequent of all frauds, accounting for only about 10%. However, the median loss for financial statement fraud is approximately $1 million, more than eight times larger than the typical asset misappropriation and approximately four times larger than the typical corruption scheme. In addition, when financial statement fraud has been identified, in 80% of the cases, other types of fraud are also being perpetrated.

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.

Common Fraud Schemes

Table 1-1 depicts the most common fraud schemes.

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

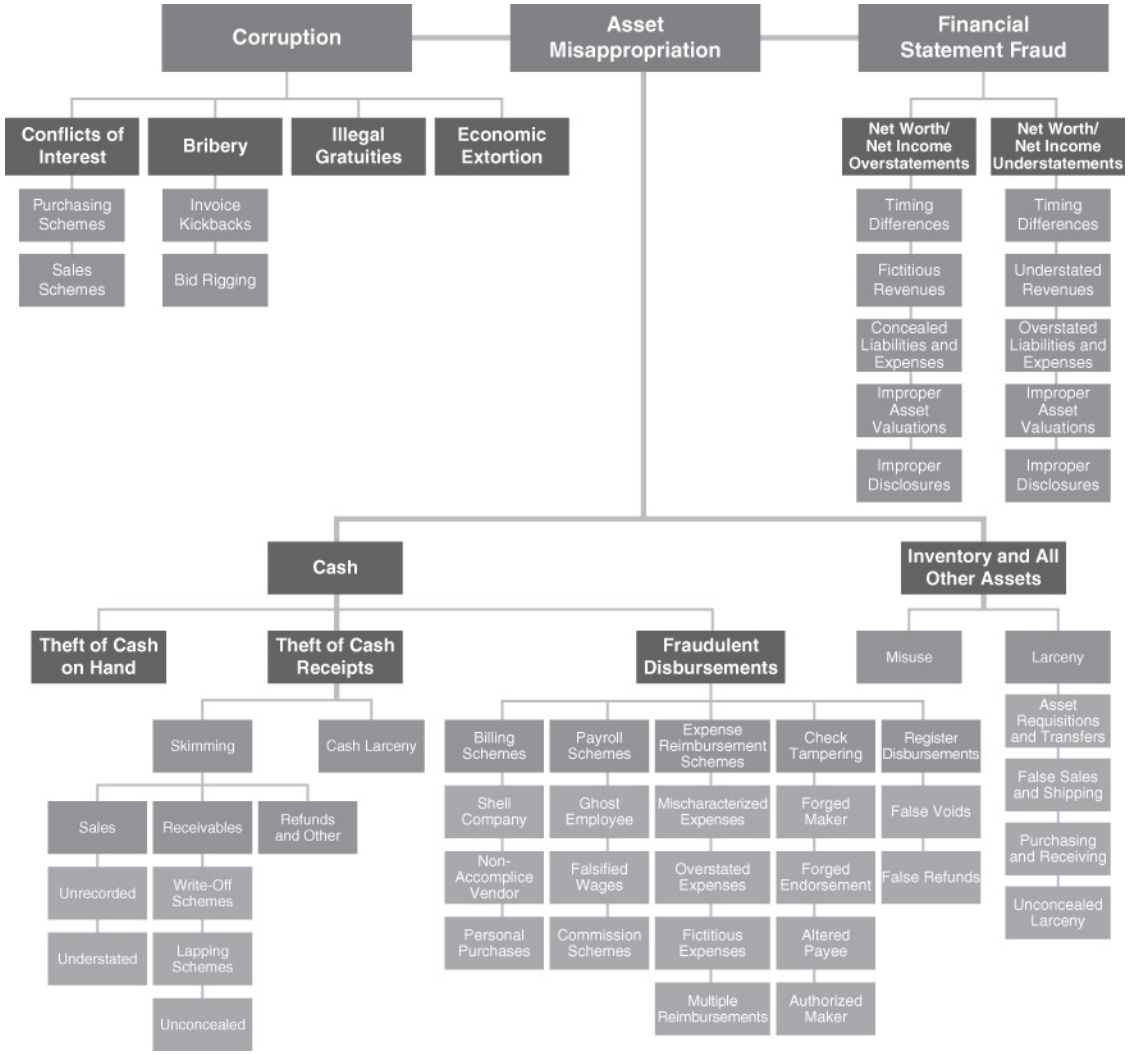
Noteworthy Industry-Specific Fraud

- Financial Institutions
- Insurance Fraud
- Health-Care Fraud
- Securities Fraud
- Public Sector Fraud

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.

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 (assets 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.

FIGURE 1-1 OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM (FRAUD TREE)



What Is the Difference Between Fraud and Abuse?

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

- Use equipment belonging to the organization
- Surf the Internet while at work
- Attend to personal business during working hours
- Take a long lunch, or a break, without approval
- Come to work late, or leave early
- Use sick leave when not sick
- Do slow or sloppy work
- Use employee discounts to purchase goods for friends and relatives
- Work under the influence of alcohol or drugs

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

Given the commonality of the language describing both fraud and abuse, what are the key differences? 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 Web site by Sam E. Antar at http:www.whitecollarfraud.com

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

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

The Four Phases of the Crazy Eddie Frauds

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

From the Fraudster's Perspective

Sam E. Antar was a CPA and the CFO of the Crazy Eddie electronics chain in the 1980s when that securities fraud scandal hit. The fraud cost investors and creditors hundreds of millions of dollars, and it cost others their careers. In addition to securities fraud, investigators later learned that the Crazy Eddie business was also involved in various other types of fraud, including skimming, money laundering, fictitious revenue, fraudulent asset valuations, and concealed liabilities and expenses, to name a few. Since then, Sam has shared his views—on white-collar crime, the accounting profession, internal controls, the Sarbanes–Oxley Act, and other related topics—with audiences around the country.

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

The Crazy Eddie Case (continued)

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 makes 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

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.

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.

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.

11. Source unknown.

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.

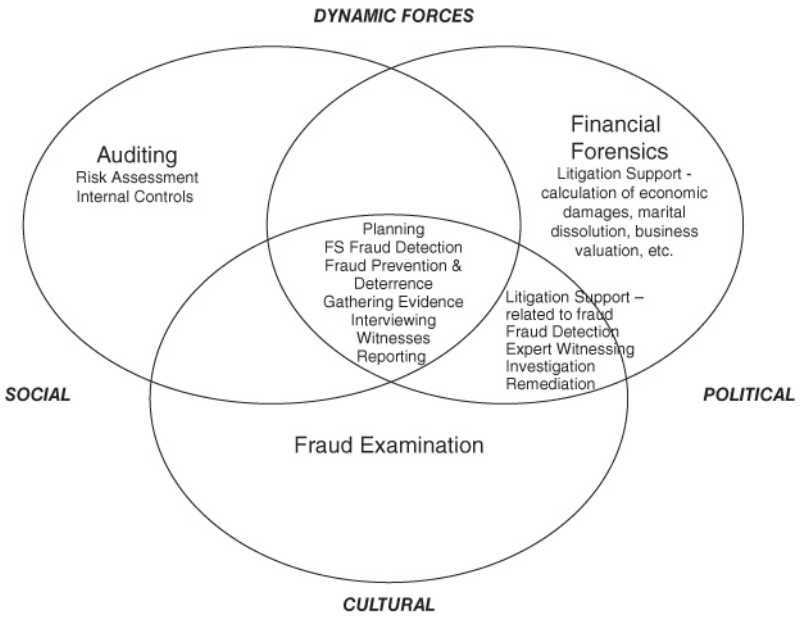
However, each discipline also encompasses separate and unique functional aspects. For example, fraud examiners are generally called in after there is reason to believe that fraud has occurred or is occurring, and often assist in fraud prevention and deterrence efforts that do not involve the audit of 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.

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.

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.

FIGURE 1-2 AUDITING, FRAUD EXAMINATION, AND FORENSIC ACCOUNTING



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 differences.

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.

(Continued)

Relationship	**Nonadversarial but skeptical**	**Adversarial**	**Independent**
	Historically, the audit process was nonadversarial. Since SOX and SAS 99, auditors use professional skepticism as a guide.	Fraud examinations, because they involve efforts to affix blame, are adversarial in nature.	A forensic accounting professional calculates financial impact based on formulaic assumptions.
Methodology	**Audit techniques**	**Fraud examination techniques**	**Forensic accounting techniques**
	Audits are conducted primarily by examining financial data using GAAS.	Gathering the required financial and nonfinancial evidence to affix culpability.	Gathering the required financial and nonfinancial evidence to examine the allegations independently and determine their financial impact.
Presumption	**Professional Skepticism**	**Proof**	**Proof**
	Auditors are required to approach audits with professional skepticism, as outlined in GAAS.	Fraud examiners approach the resolution of a fraud by attempting to gather sufficient evidence to support or refute an allegation of fraud.	Forensic accounting professionals will attempt to gather sufficient evidence to support or refute the allegation and related damages.

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 canceled 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 world GDP, in 2014, the ACFE estimated that the cost of fraud may be as high as $3.7 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 $1,000 (a computer, for example), the company would need to sell an additional 5,000 units of product.

Organizations incur costs to produce and sell their products or services. These costs run the gamut: labor, taxes, advertising, occupancy, raw materials, research and development—and, yes, fraud and litigation. The cost of fraud and litigation, however, are fundamentally different from the other costs—the true 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 2016 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 2016 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

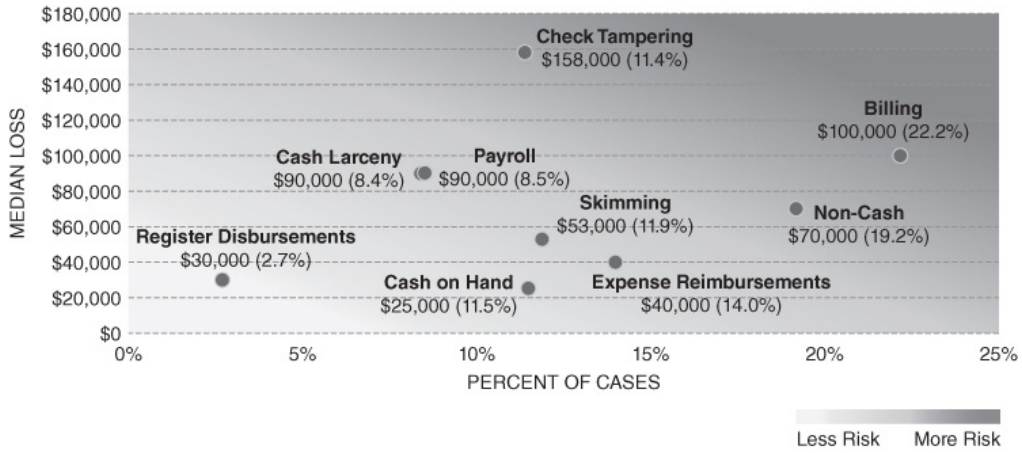
The ACFE highlights three major types of occupational fraud and abuse: asset misappropriation, corruption, and financial reporting fraud. The relative frequency and losses associated with each are as follows:

Fraud Scheme Category	Percentage	Median Losses
Asset Misappropriation	85	$130,000
Corruption	37	$200,00
Financial Reporting Fraud	9	$1,000,000

13. Adapted from Occupational Fraud and Abuse, Joseph T. Wells (Obsidian Publishing Company,1997).

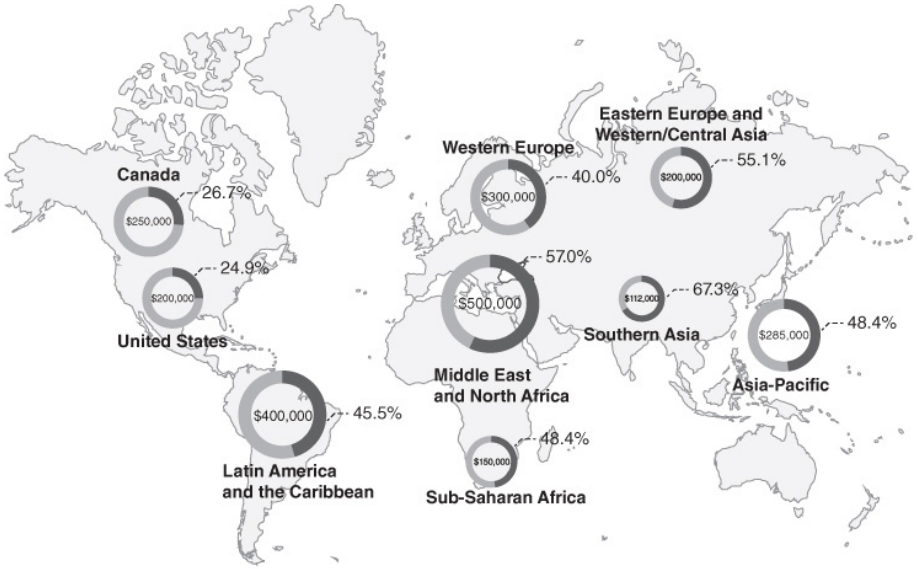
These percentages do not add up to 100% because many frauds involve multiple schemes. Within asset misappropriation, which has the most diversity, the heat map of frequency and loss (Figure 1-3) provides a broader view of the risk to victims.

FIGURE 1-3 FREQUENCY AND MEDIAN LOSS OF ASSET MISAPPROPRIATION SUBSCHEMES



Corruption is sometimes hypothesized to be especially common in cultures where “gratuities” are part of the business climate. As such, Figure 1-4 offers insight into corruption by regions of the world.

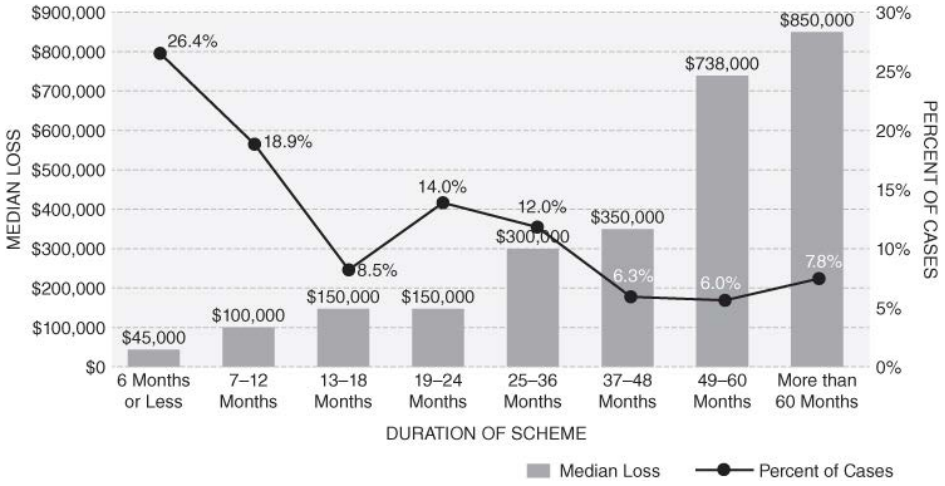
FIGURE 1-4 FREQUENCY AND MEDIAN LOSS OF CORRUPTION CASES BY REGION



*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.

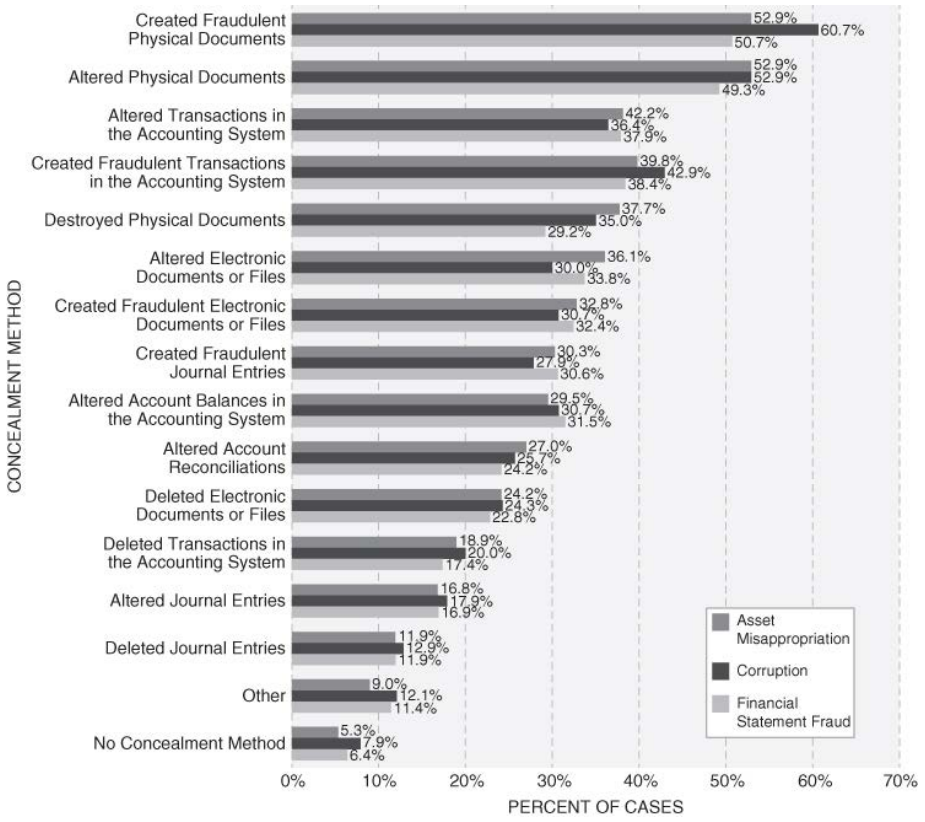
As the duration of the fraud lengthens, the cost of fraud increases. As noted in Figure 1-5, organizational efforts to detect fraud earlier should result in less impact. The median fraud lasts about eighteen months, according to the ACFE.

FIGURE 1-5 FREQUENCY AND MEDIAN LOSS BASED ON DURATION OF FRAUD



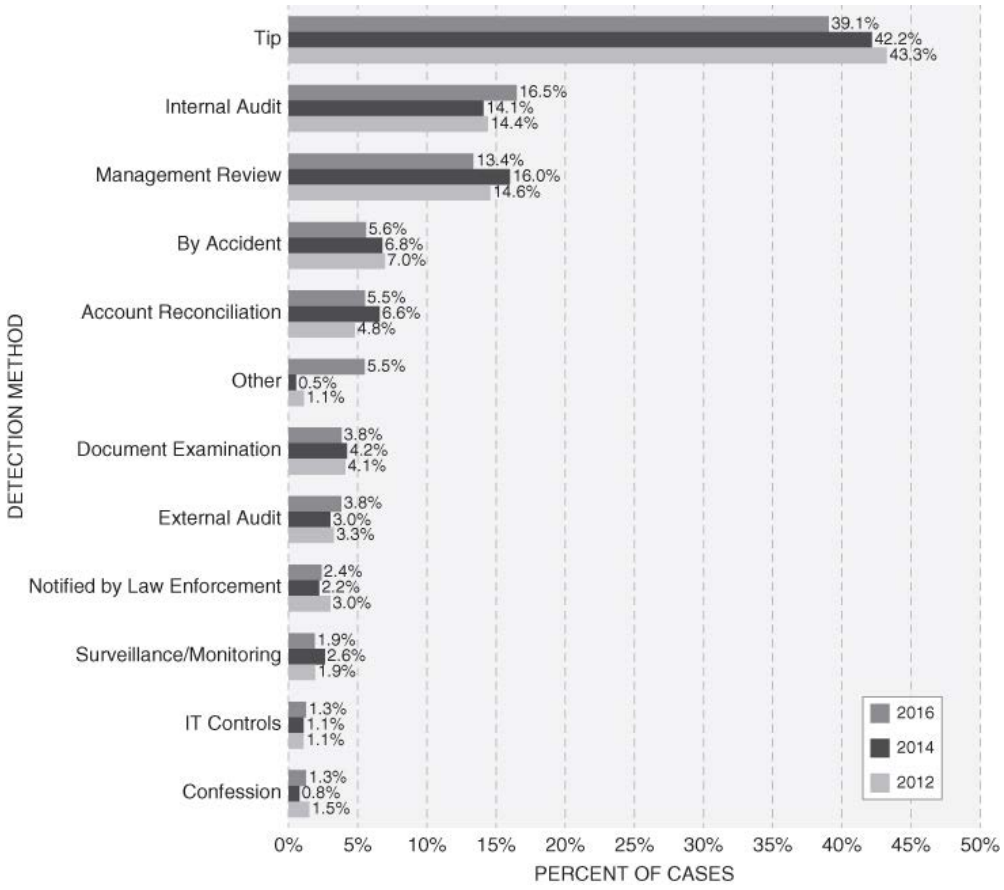
For the first time in the history of the Report to the Nations, the 2016 survey queried CFEs on the most common tactics to conceal fraud schemes. As the graphic in Figure 1-6 notes, the most common concealment schemes are "old fashioned" document-based efforts. Across time, antifraud professionals might 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.

FIGURE 1-6 CONCEALMENT METHOD BY SCHEME TYPE



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 2016 data, internal audit (16.5%) edged out management review (13.4%) as the second-most common detection method. Historically, external audits detected only about 3% 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 85%, 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.

FIGURE 1-7 INITIAL DETECTION OF OCCUPATIONAL FRAUDS



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

Source of the Tip	Percentage
Employee	51.5
Customer	17.8
Anonymous	14.0
Other	12.6
Vendor	9.9
Shareholder/Owner	2.7
Competitor	1.6

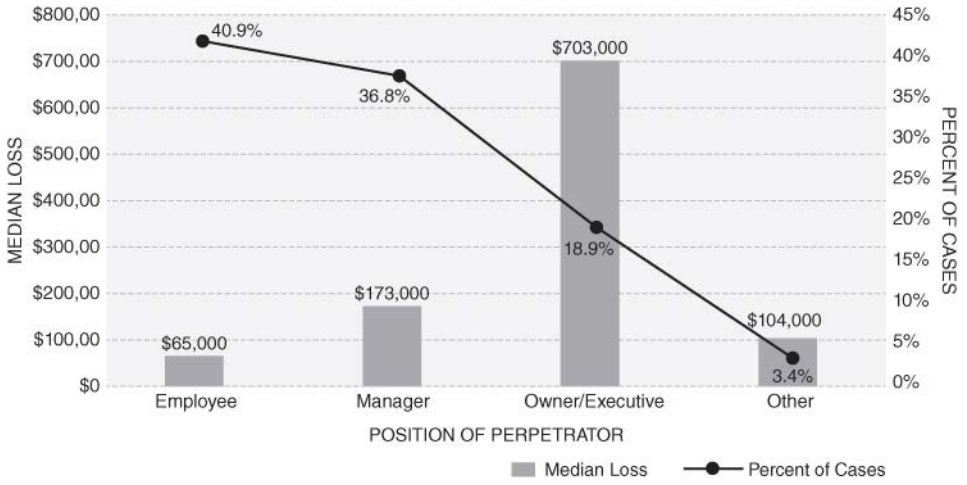
The Perpetrators of Fraud

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 2016 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.

FIGURE 1-8 POSITION OF PERPETRATOR—FREQUENCY AND MEDIAN LOSS

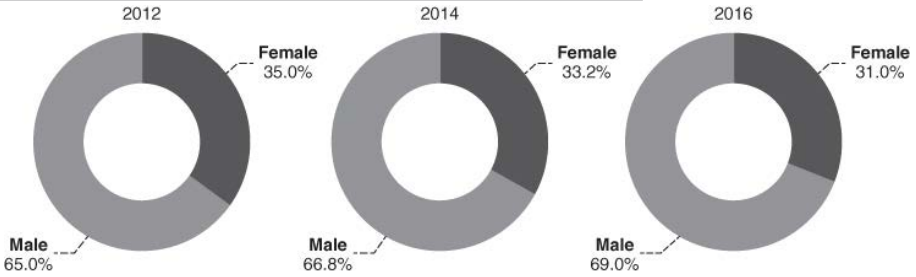


The lowest median loss of $65,000 was found in frauds committed by employees. Although the median loss in schemes committed by managers reached $173,000, the median loss skyrocketed to $703,000 for executives/owners. Approximately 18.9% of the schemes are committed by executives/owners.

The Effect of Gender on Median Loss

The 2016 ACFE Report to the Nation showed that male employees caused median losses that were more than twice as large as those of female employees; the median loss in a scheme caused by a male employee was $187,000, whereas the median loss caused by a female employee was $100,000. 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 69.0% of the cases, as Figure 1-9 shows.

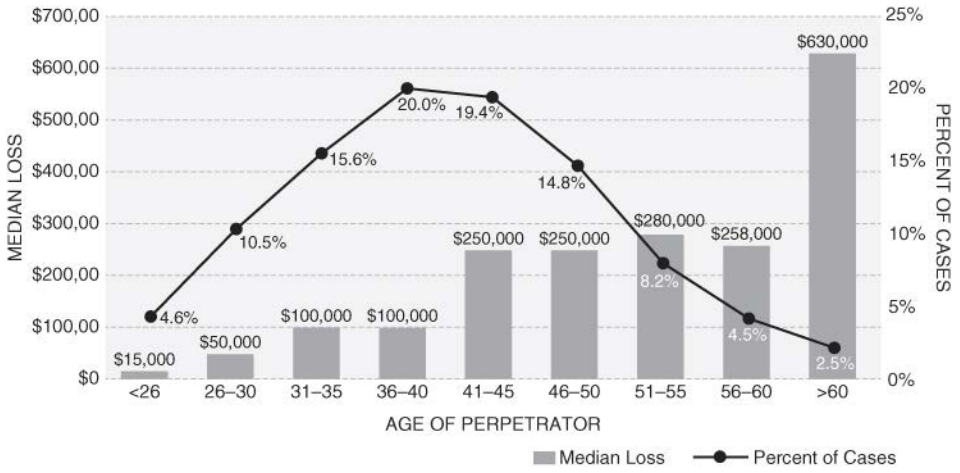
FIGURE 1-9 GENDER OF PERPETRATOR—FREQUENCY



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 (2.5%), the median loss in those schemes was $630,000. By comparison, the median loss in frauds committed by those twenty-five or younger was $15,000. 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.

FIGURE 1-10 AGE OF PERPETRATOR—FREQUENCY AND MEDIAN LOSS

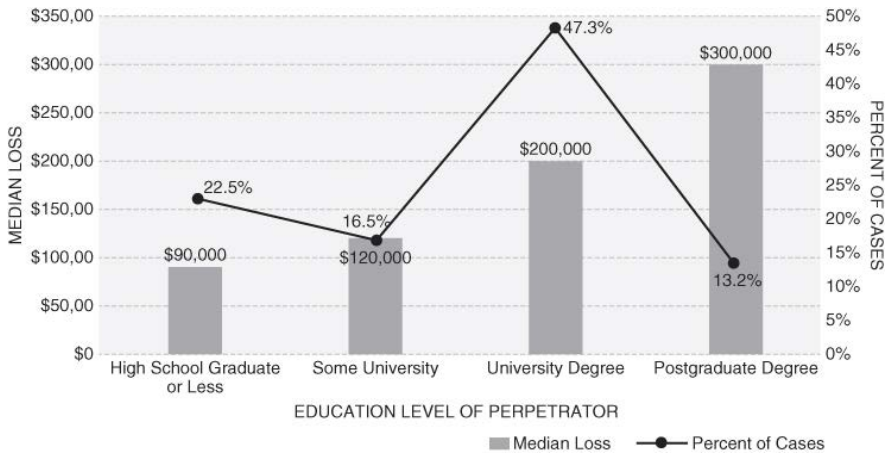


Although frauds committed by those in the older age groups were the most costly on average, almost two-thirds of the frauds reported were committed by employees 31−50 years old. The median age among perpetrators was 40.

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 $90,000, whereas the median loss caused by employees with a postgraduate education was $300,000. This trend was to be expected, given that those with higher education levels tend to occupy positions with higher levels of authority.

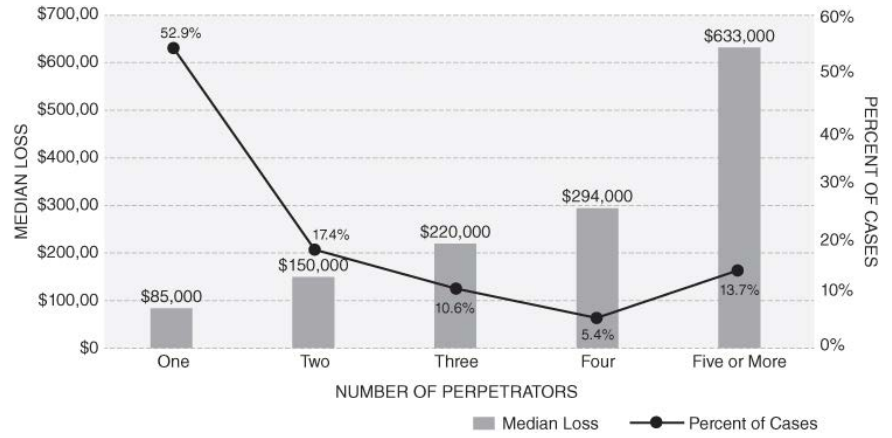
FIGURE 1-11 EDUCATION LEVEL OF PERPETRATOR—FREQUENCY AND MEDIAN LOSS



The Effect of Collusion on Median Loss

It was not surprising to see that in cases involving more than one perpetrator, fraud losses rose substantially. The majority of 2016 survey cases (52.9%) only involved a single perpetrator, but when two or more persons conspired, the median loss was more than seven times higher (see Figure 1-12).

FIGURE 1-12 NUMBER OF PERPETRATORS—FREQUENCY AND MEDIAN LOSS

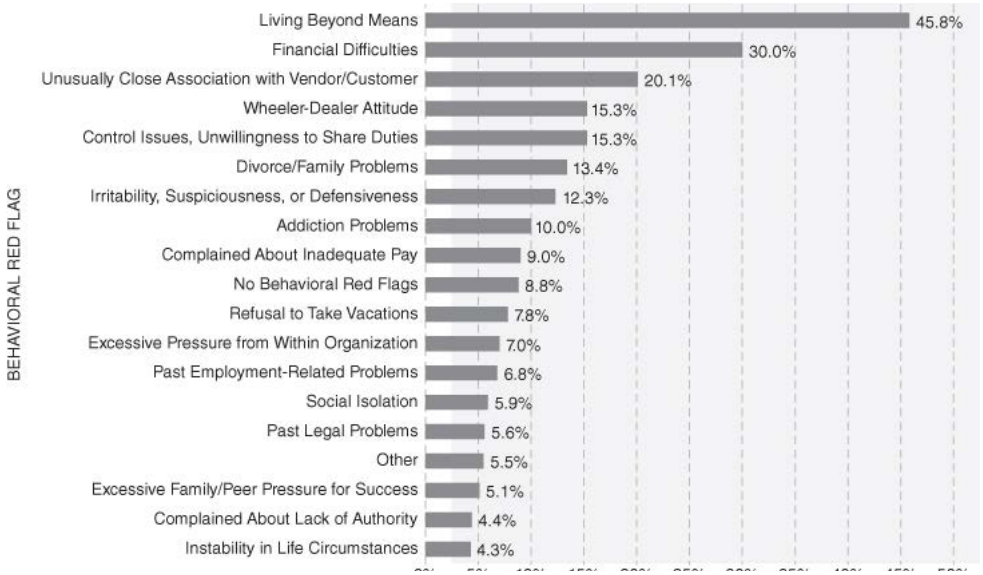


Criminal History of the Perpetrators

Most people who commit occupational fraud are first-time offenders. Only 5.2% of the perpetrators identified in the 2016 study were known to have been convicted of a previous fraud-related offense. Another 5.5% 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 8.3% 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 91% of cases, at least one behavioral red flag was identified prior to detection, and in 57% of cases two or more red flags were seen. The behavioral red flags and their frequency are presented in Figure 1-13.

FIGURE 1-13 BEHAVIORAL RED FLAGS DISPLAYED BY PERPETRATORS



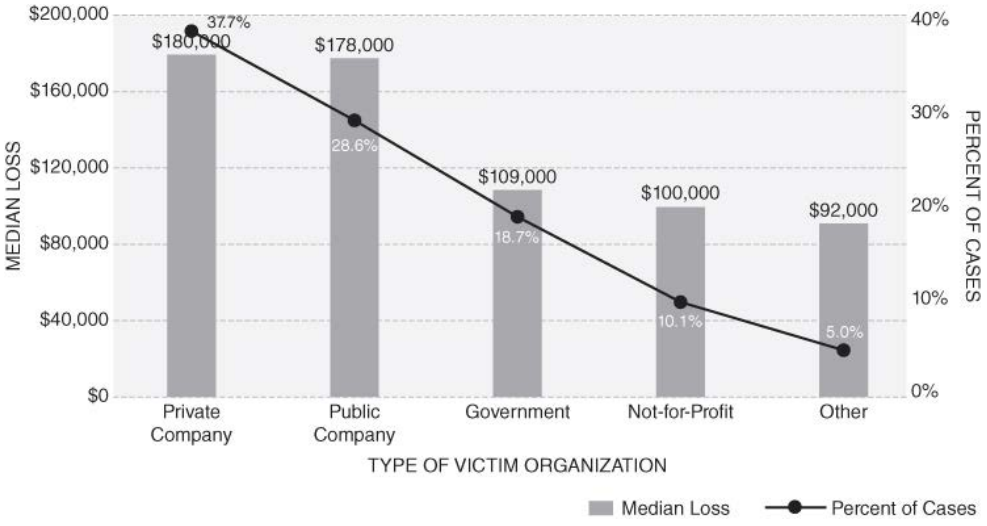
The Victims

The victims of occupational fraud are organizations that are defrauded by those they employ. The ACFE's 2016 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 $180,000, similar to that of public companies ($178,000). This exceeded the median loss for cases in other organization types: government, not-for-profit and other (Figure 1-14).

FIGURE 1-14 TYPE OF VICTIM ORGANIZATION—FREQUENCY AND MEDIAN LOSS



Median Loss Based on Size of the Organization

Small businesses (those with fewer than 100 employees) tend to suffer a disproportionately large number of fraud incidents and fraud losses, similar to findings in prior reports. 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 (see Figures 1-15 and 1-16).

FIGURE 1-15 SIZE OF VICTIM ORGANIZATION—FREQUENCY

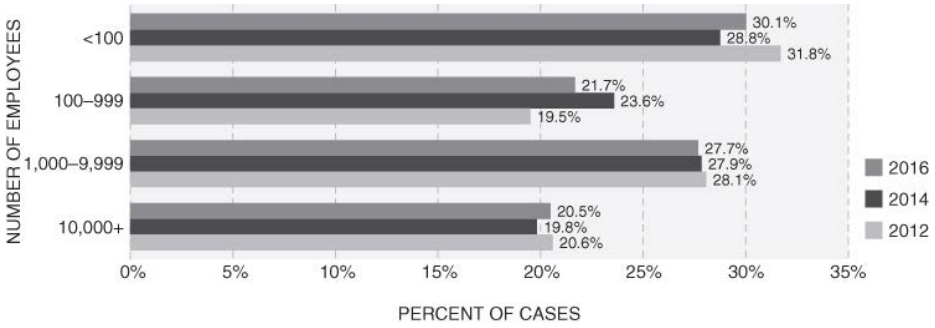


FIGURE 1-16 SIZE OF VICTIM ORGANIZATION—MEDIAN LOSS

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.

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 antifraud measure was in place or not (excluding other factors).

The most common antifraud measure was the external audit of financial statements, utilized by approximately 81.7% of the victims, followed by a formal code of conduct, which was implemented by 81.1% of victim organizations (Figure 1-17). Organizations that implemented these controls noted median losses that were 14.3% and 40% lower, respectively, than those of organizations lacking these controls. Interestingly, the three controls associated with the largest reduction in median losses—proactive data monitoring/analysis (big data and data analytics), management review, and hotlines—were not among the most commonly implemented antifraud controls.

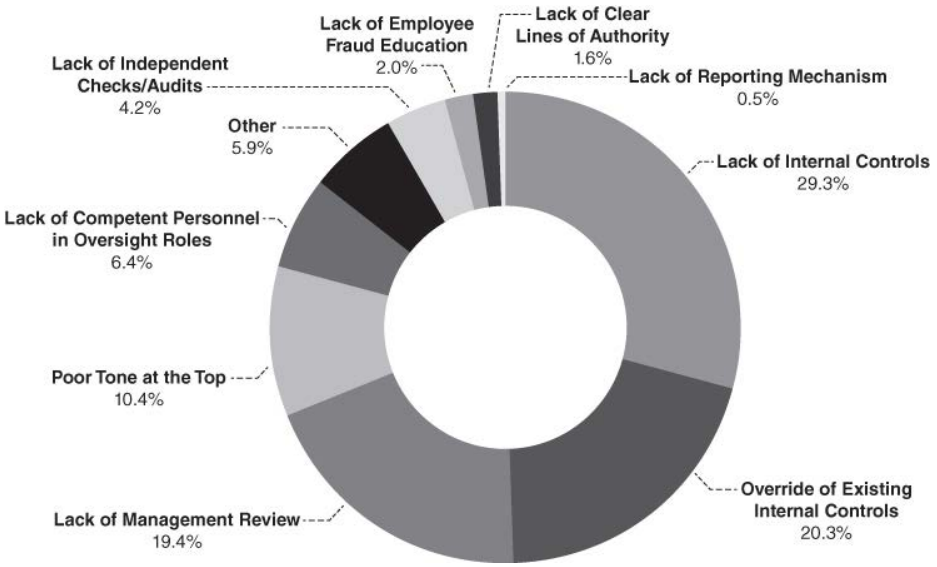
FIGURE 1-17 EFFECTIVENESS OF CONTROLS

Control	Percent of Cases	Control in Place	Control Not in Place	Percent Reduction
Proactive Data Monitoring/Analysis	36.7%	$92,000	$200,000	54.0%
Management Review	64.7%	$100,000	$200,000	50.0%
Hotline	60.1%	$100,000	$200,000	50.0%
Management Certification of Financial Statements	71.9%	$104,000	$205,000	49.3%
Surprise Audits	37.8%	$100,000	$195,000	48.7%
Dedicated Fraud Department, Function, or Team	41.2%	$100,000	$192,000	47.9%
Job Rotation/Mandatory Vacation	19.4%	$89,000	$170,000	47.6%
External Audit of Internal Controls over Financial Reporting	67.6%	$105,000	$200,000	47.5%
Fraud Training for Managers/Executives	51.3%	$100,000	$190,000	47.4%
Fraud Training for Employees	51.6%	$100,000	$188,000	46.8%
Formal Fraud Risk Assessments	39.3%	$100,000	$187,000	46.5%
Employee Support Programs	56.1%	$100,000	$183,000	45.4%
Anti-fraud Policy	49.6%	$100,000	$175,000	42.9%
Internal Audit Department	73.7%	$123,000	$215,000	42.8%
Code of Conduct	81.1%	$120,000	$200,000	40.0%
Rewards for Whistleblowers	12.1%	$100,000	$163,000	38.7%
Independent Audit Committee	62.5%	$114,000	$180,000	36.7%
External Audit of Financial Statements	81.7%	$150,000	$175,000	14.3%

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 29.3%, with another 20.3% stating that internal controls were present but had been overridden by the perpetrator (see Figure 1-18).

FIGURE 1-18 PRIMARY INTERNAL CONTROL WEAKNESS OBSERVED BY CFE



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 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.

Criminal Prosecutions and Their Outcome

In 59.3% of the cases, the victim organization referred the case to law enforcement authorities.

For cases that were referred to law enforcement authorities, a large number of those cases were still pending at the time of the survey as shown in Figure 1-19. However, 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 dropped from 19.2% in 2012 to 13.3% in

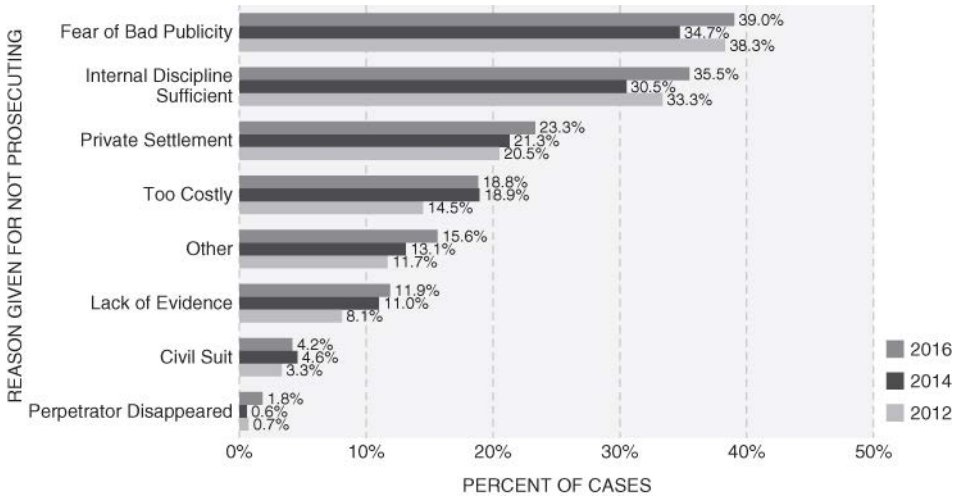
2016. Combining guilty pleas and convictions at trial, 76.4% of cases submitted for prosecution resulted in a finding of guilt in 2016, while 2.3% of such prosecutions ended in acquittal. Although the percentage of cases referred to prosecution decreased gradually from the 2012 to the 2016 reports, the percentage of cases that prosecutors successfully pursued increased.[14]

FIGURE 1-19 RESULTS OF CASES REFERRED TO LAW ENFORCEMENT

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. Fear of bad publicity (39.0%) was the most commonly cited reason, followed by internal discipline was sufficient (35.5%) and a private settlement being reached (23.3%).

FIGURE 1-20 REASON(S) CASES NOT REFERRED TO LAW ENFORCEMENT



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?

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.

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 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

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.

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.

15. See http://www.answrs.com/red%20flag.
16. ACFE's Fraud Examiners Manual, Section 2.601.

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.

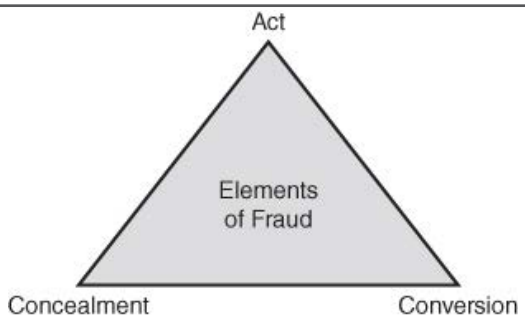
Whether the engagement is based on allegations associated with a civil litigation claim or a tip about a fraud act, the forensic accountant or fraud examiner needs to ensure that they have a clear understanding of the concerns. These allegations or concerns define the initial scope of the engagement. 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 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).

FIGURE 1-21 THE TRIANGLE OF FRAUD ACTION: ELEMENTS OF FRAUD



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.

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.

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:

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.

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

Saddam Hussein's public statements of intent not to retaliate.	**H1**	**H2**	**H3**
Absence of terrorist offensive during the 1991 Gulf War.	0	0	0
Assumption: Iraq does not want to provoke another US war.	+	0	−
Increase in frequency/length of monitoring by Iraqi agents of regional radio and TV broadcasts.	+	+	−
Iraqi embassies instructed to take increased security precautions.	0	+	+
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—i.e., a bribery or kickback scheme, embezzlement, conflict of interest, or financial statement fraud—in which evidence indicates that the hypothesis is a reasonable possibility.

Testing the Hypotheses

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

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

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

Refining and Amending the Hypotheses

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

Methodologies Used in Fraud 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. In many cases, these provide the indicia of fraud and/or the motivations of the parties under review. Related to such evidence, the fraud examiner must also 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.

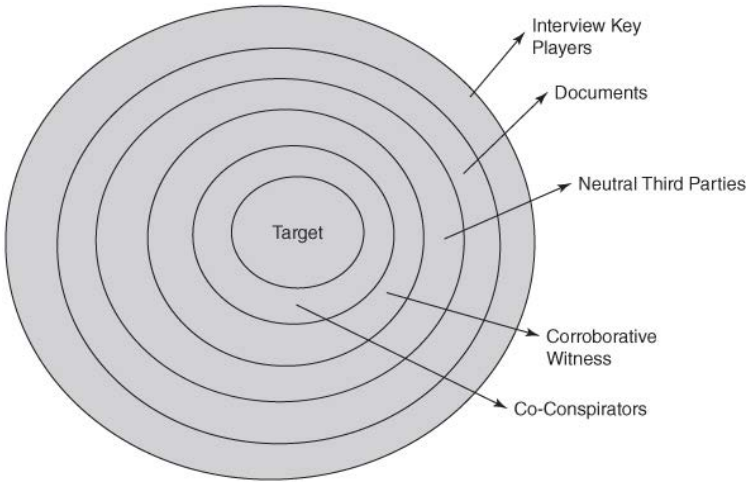
The second tool used by these professionals is the interview, which is the process of obtaining relevant information about the matter in question from those with knowledge of it. For example, in developing information about Linda Reed Collins, it might be necessary to interview her co-workers, superiors, 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.

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.

FIGURE 1-22 EVIDENCE-GATHERING ORDER IN FRAUD EXAMINATIONS

FIGURE 1-23 FRAUD INTERVIEW METHODOLOGIES



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]

19. James DiGabriel (ed.), Forensic Accounting in Matrimonial Divorce (2005), pp. 51–52.

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 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 graphical tools—such as, who knows who (linkages), who is connected with what business, how the scheme works (flow diagram), who must be involved (links and flows), what the important events

are (timelines). During the investigation, these graphical representations, even handwritten ones, can provide important clues and enhance the investigator's understanding of fact and events, interpret evidence, and otherwise draw meaning from seemingly disparate pieces of data. They can also show weaknesses in the case—places where additional evidence is required to provide a complete evidence trail.

Although completed during the investigation as a work-in-progress tool, the same graphics are often reused during the formal communication process at or near the conclusion of an investigation. Graphical representations can let nonprofessionals and those with less time on the investigation know what happened. Even though catching the bad guy or reconstructing what happened is the primary role of the fraud examiner or 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. Graphical tools, such as link charts, flow charts, commodity and money flow diagrams, timelines, and other graphical representations, are both important investigative tools and excellent communication tools. 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 graphical 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, graphical representation.

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. Once suspected, 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/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 2016 *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

20. Adapted from ACFE Fraud Examiners Manual.
21. W. Steve Albrecht, Fraud Examination, 2003.

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.

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.

THIS PAGE INTENTIONALLY
LEFT BLANK.

CHAPTER 1: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

1.	**Which of the following is <u>not</u> one of the four essential elements of fraud under common law?** **A.** a material false statement **B.** reliance on the false statement by the victim **C.** knowledge that the statement was false when it was spoken **D.** use of email, wire, or telephone with a criminal intent to deceive
2.	**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 is the definition of which of the following:** **A.** collusion **B.** concealment **C.** capital misappropriation **D.** conversion
3.	**Which of the following are the essential characteristics of financial statement fraud:** **A.** the misstatement is material and intentional and the users of the financial statements have been misled **B.** the misstatement is material and intentional and the users of the financial statements are investors in publicly traded companies **C.** the misstatement is material and intentional and the preparers of the financial statements have a fiduciary obligation to the organization **D.** the misstatement is material and intentional and the preparers of the financial statements fail to report the misstatement to the SEC or other applicable authority

4.	**Forensic accounting is the application of financial principles and theories to facts or hypotheses in a legal dispute and consists of which of the following primary functions:** **A.** litigation advisory services and investigative services **B.** expressing an opinion of guilt or innocence in court regarding audit results and documenting the steps taken to reach that opinion **C.** subjecting accounting data to a Benford Analysis and explaining the results to a judge or jury **D.** providing courtroom testimony and administrative technical guidance to attorneys
5.	**Which of the following is correct regarding auditor responsibilities under current auditing standards:** **A.** auditors must undertake a fraud-risk assessment and are responsible for planning and performing auditing procedures to detect immaterial misstatements **B.** auditors must undertake a fraud-risk assessment, but they are not responsible for planning and performing audit procedures to detect immaterial misstatements **C.** auditors must undertake a fraud-risk assessment, but they are not responsible for planning and performing audit procedures to detect immaterial misstatements unless such misstatements are caused by fraud (rather than error) **D.** auditors must undertake a fraud-risk assessment and are responsible for planning and performing auditing procedures to detect immaterial misstatements, whether caused by fraud or error
6.	**According to the ACFE's *2016 Report to the Nations on Occupational Fraud and Abuse*, what kind of fraud scheme resulted in the greatest percentage of cases:** **A.** billing **B.** check tampering **C.** expense reimbursements **D.** skimming

7.	**When it comes to fraud loss amounts in organizations, the ACFE's data shows that there is a direct correlation between _____ loss and _____.** **A.** average; perpetrator's intelligence **B.** average; perpetrator's position **C.** median; perpetrator's intelligence **D.** median; perpetrator's position
8.	**Among those who investigate fraud, which of the following is a common complaint regarding organizations and law enforcement:** **A.** they fail to understand the many ways in which fraud and other white-collar crime can be perpetrated **B.** they do not keep pace with the growing sophistication of fraud and other white-collar offenses **C.** they do not do enough to punish fraud and other white-collar offenses **D.** they are overwhelmed with other concerns to the extent that fraud and other white-collar offenses are regarded as inconsequential in the grand scheme of things
9.	**The authors believe that which of the following is the most effective way to catch a fraudster:** **A.** setting aside professional skepticism **B.** relying on one's own value system **C.** thinking like one **D.** accepting evidence without being critical of it
10.	**Which of the following is cited by the authors as one of the best ways to ruin an investigation, fail to gain a conviction, or lose a civil case:** **A.** take disparate pieces of financial and non-financial data to tell a story of who, what, when, where, how, and why **B.** base investigative conclusions on logic and arguments that the defendant is a "bad person" **C.** connect the dots in a case consistent with the investigator's interpretation of the evidence **D.** excessively rely on evidence, especially when the plaintiff has a clear track record of ethical conduct or is an upstanding community leader

11.	**The triangle of fraud action is composed of which three elements:** **A.** incentive, opportunity, rationalization **B.** surveillance, invigilation, documentation **C.** devising a scheme, executing the scheme, laundering the proceeds **D.** act, concealment, conversion

CHAPTER 1: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

1.

A. Incorrect. The existence of a material false statement is an essential element of fraud under common law.

B. Incorrect. One of the four essential elements of fraud is that a reliance on the false statement by the victim exists.

C. Incorrect. Under common law, knowledge that the statement was false when it was spoken is an essential element of fraud.

D. **CORRECT**. Under common law, fraud includes four essential elements. A material false statement must exist, the fraudster must have knowledge that the statement was false when it was spoken, the victim relied on the false statement, and damages resulted from the victim's reliance on the statement.

(See page 4 of the course material.)

2.

A. Incorrect. Collusion is defined as a secret or illegal cooperation or conspiracy, especially in order to cheat or deceive others.

B. Incorrect. Concealment is defined as hiding a fraudulent act or masking it to look like something different.

C. Incorrect. Capital misappropriation involves the theft or misuse of an organization's capital.

D. **CORRECT**. Conversion, in the legal sense, is "an unauthorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition or the exclusion of the owner's rights." A person commits a conversion when they take possession of property that does not belong to them and, thereby, deprives the true owner of the property for any length of time.

(See page 5 of the course material.)

3.

A. **CORRECT**. The essential characteristics of financial statement fraud are that a misstatement is material and intentional and that the users of the financial statements have been misled.

B. Incorrect. The investors relying on the fraudulent financial statements do not have to be investors in publicly traded companies for the fraud to exist.

C. Incorrect. Financial statement fraud is not determined by whether or not the preparers of the financial statements have a fiduciary obligation to the organization.

D. Incorrect. The essential characteristics of financial statement fraud do not include failing to report a misstatement to the SEC or other applicable authority.

(See page 8 of the course material.)

4.	**A.** **CORRECT**. 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: litigation advisory services, which recognizes the role of the forensic accounting professional as an expert or consultant, and investigative services, which makes use of the forensic accounting professional's skills and may or may not lead to courtroom testimony. **B.** Incorrect. Testifying in court as to whether or not an individual is guilty of fraud is not a primary function of forensic accounting. **C.** Incorrect. Benford Analysis is not the only analytical tool available to the forensic accountant. **D.** Incorrect. The primary functions of forensic accounting are litigation advisory services and investigative services, not providing courtroom testimony and administrative technical guidance to attorneys. *(See page 14 of the course material.)*
5.	**A.** Incorrect. Under generally accepted auditing standards (GAAS), auditors are not currently responsible for planning and performing auditing procedures to detect immaterial misstatements. **B.** **CORRECT**. 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. **C.** Incorrect. 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. **D.** Incorrect. Under current auditing standards, auditors are not responsible for planning and performing auditing procedures to detect immaterial misstatements, whether caused by fraud or error. *(See page 16 of the course material.)*
6.	**A.** **CORRECT**. Billing fraud schemes were the most frequently reported, accounting for 22.2 percent of the total fraud schemes. **B.** Incorrect. The median loss was highest for check tampering schemes, but they did not account for the highest percentage of cases. **C.** Incorrect. Expense reimbursement schemes were the third-most frequently perpetrated fraud schemes reported by the ACFE. **D.** Incorrect. Skimming fraud schemes made up 11.9 percent of all fraud schemes, which was substantially less than the number of billing schemes reported by the ACFE. *(See page 20 of the course material.)*

7.	**A.** Incorrect. The ACFE did not find a correlation between the average of the loss and the perpetrator's intelligence. **B.** Incorrect. The correlation was not between average loss and the perpetrator's position. **C.** Incorrect. A correlation was not found between the median fraud loss and the perpetrator's intelligence. **D.** **CORRECT**. Fraud losses tend to rise based on the perpetrator's level of authority within an organization. Generally, employees with the highest levels of authority are the highest paid as well. Therefore, it was not a surprise to find a positive correlation between the perpetrator's position and the size of fraud losses. *(See page 23 of the course material.)*
8.	**A.** Incorrect. Fraud investigators do not frequently report that organizations and law enforcement fail to understand the many ways in which fraud and other white-collar crime can be perpetrated. **B.** Incorrect. Organizations and law enforcement are not frequently cited as not keeping pace with the growing sophistication of fraud and other white-collar offenses. **C.** **CORRECT**. 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 nonexistent sanctions faced by those caught committing fraud. **D.** Incorrect. Being overwhelmed with other concerns to the extent that fraud and other white-collar offenses are regarded as inconsequential in the grand scheme of things is not a common critique of organizations and law enforcement by fraud investigators. *(See page 29 of the course material.)*
9.	**A.** Incorrect. Setting aside professional skepticism is not a good practice. **B.** Incorrect. A reliance on one's own value system is not the best way to catch the perpetrators of occupational fraud. **C.** **CORRECT**. It can be challenging to conduct a forensic accounting engagement or fraud examination unless the investigator is prepared to look beyond their value system. In short, the most effective way to catch a fraudster, is to think like one. **D.** Incorrect. It is important to be critical of any evidence you are relying on. *(See page 31 of the course material.)*

10.	**A.** Incorrect. Taking disparate pieces of financial and non-financial data to tell a story of who, what, when, where, how, and why is the key to evidence-based decision making. This will help win cases, not lose them. **B.** **CORRECT**. According to the authors, one of the best ways to ruin an investigation, 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" 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. **C.** Incorrect. A fraud examiner is supposed to connect the dots in a case consistent with the investigator's interpretation of the evidence. **D.** Incorrect. Successful investigators base their conclusions, and the results of their investigations, on evidence. This is true regardless of the plaintiff's standing in the community. *(See pages 32 to 33 of the course material.)*
11.	**A.** Incorrect. The fraud triangle theory, not the triangle of fraud action, consists of incentive, opportunity, and rationalization. **B.** Incorrect. Surveillance, invigilation, and documentation are ways to gather evidence of fraud, not the elements of the fraud action triangle. **C.** Incorrect. The fraud action triangle does not consist of devising a scheme, executing the scheme, and laundering the proceeds. **D.** **CORRECT**. The elements of the fraud action triangle 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). *(See page 34 of the course material.)*

CHAPTER 2: WHO COMMITS FRAUD AND WHY: THE PROFILE AND PSYCHOLOGY OF THE FRAUDSTER

Chapter Objective

After completing this chapter, you should be able to:

- Recognize the elements of the fraud triangle.

According to a 2012 FBI Pittsburgh Division press release, Patricia K. Smith, 57 at the time and the former controller at Baierl Acura, plead guilty in federal court. The Pittsburgh Post-Gazette alleges that Ms. Smith fraudulently transferred $10.3 million from Baierl Acura's accounts to her own, using the money to finance a spree of frivolity and generosity. Ms. Smith was a one-time trusted employee who worked at the car dealership beginning in 1993, serving as the financial controller and working at the dealership for 11 years before embarking on her bad acts.

According to these sources, from late 2004 through mid-2011, Ms. Smith padded her $53,000-a-year salary with upward of $25,000 a week that she embezzled. What did she do with this extra money: She spent "$43,000 for a hotel in Paris, France, $1.8 million billed to her American Express account for private jet fare … $62,500 for six club-level Super Bowl tickets, and it goes on and on and on." Apparently a religious woman, she splurged on "The Vatican Package," ($5,000) which included Mass in Papal Audience with VIP seating, airfare for four, VIP tour of the Vatican Museum with a private tour guide, and a private tour of the Sistine Chapel with family before it is open to the public.

Ms. Smith told U.S. District Judge Gustave Diamond at her sentencing hearing that she spent the money on friends and family, saying "I wanted to earn their love, and I wanted to see what happiness really looked like."[1]

What causes a seemingly "good person" (at least before the revelation of their crimes) to commit bad acts? In this chapter, we examine "who commits fraud" and offer some insight into "why."

The authors examine this topic across several modules. Those modules, along with the learning objectives, include the following:

- Module 1 examines criminology, the study of crime and criminals, and its interface with fraud, financial crimes, and forensic accounting issues. The objective is for the reader to be able to describe occupational fraud and abuse as well as the role of civil litigation in forensic accounting and fraud examination issues.
- Module 2 develops a profile of the garden variety fraudster using one of the most recognized tools in the antifraud community, the fraud triangle. The goal in this module

1. See FBI Press Release, "Former Baierl Acura Controller Admits Embezzling $10.2 Million," January 10, 2012; Rich Lord, "Baierl Acura Controller Who Embezzled $10.2 Million Sentenced," Pittsburgh Post-Gazette.

is for the reader to apply the elements of the fraud triangle: nonshareable pressure, perceived opportunity, and rationalization to specific cases.

- Module 3 takes a look at some of the early efforts to fine-tune and improve the fraud triangle, adding the roles of personal integrity, capability, gender, and the influence of the organization. The goal here is for the reader to be able to describe the reasoning behind perpetrator decisions to commit bad acts.
- Module 4 reviews more recent findings from research that considers fraudsters whose profile is inconsistent with the fraud triangle: M.I.C.E., predatory (repeat) fraudsters, and collusive groups. The take-away from this module will be the ability to adjust the assessment of case issues, given the possibility of repeater offenders or collusive fraud teams. When complexity increases, particularly the ability to conceal bad acts, frauds become more difficult to detect and investigate.
- Module 5 offers a cautionary tale for practicing forensic accountants and fraud examiners related to courtroom testimony grounded in the fraud triangle. It offers a meta-model for moving from a focus on the perpetrator to an investigation grounded in evidence by using the triangle of fraud action (the "elements of fraud"). The important goal here is for the reader to recognize that while the fraud triangle and its improvements across time help us understand who commits fraud and why, when we conduct fraud and forensic examinations, gathering persuasive evidence is the key to success.

MODULE 1: CRIMINOLOGY, FRAUD, AND FORENSIC ACCOUNTING

Bethany holds the position of office manager at a small commercial real-estate company. Jackson Stetson, the owner, conducts numerous entertainment events each month to interact with, and locate, new clients. In addition, Mr. Stetson prides himself on his support of charitable organizations. In his capacity as a leader, organizer, and board member of several high-profile charities, Jackson has additional charity events each month.

Bethany is a trusted assistant to Mr. Stetson, runs many aspects of the company and organizes and hosts many of the social events for Mr. Stetson. Bethany has been with the company for many years and has a company credit card to pay for social events and incidentals associated with these events. The company pays the monthly credit card balance; and Bethany is supposed to save receipts and match those receipts to her company credit cards before seeking Mr. Stetson's approval for company payment.

Initially, Bethany lost a few receipts, and Mr. Stetson waived the requirement that she provide all receipts. As the business grew, Bethany's schedule became "crazy," and she had less time for administrative responsibilities. Mr. Stetson was so happy with her work on his social events that he was willing to overlook her lack of attention to administrative details. The problem was that, over time, Bethany started to charge personal expenses on the company-paid credit card. Not only was the company paying Bethany's salary, they also paid her grocery bills and household expenses at retailers where she shopped for social event incidentals. Over a twenty-four-month period, Bethany was able to double her $80,000 annual take-home pay, and the additional income was tax-free! Eventually, Bethany was

caught, convicted, and received a bill from the Internal Revenue Service for back taxes, interest, and penalties.

Criminology

Criminology is the sociological study of crime and criminals. Understanding the nature, dynamics, and scope of fraud and financial crimes is an important aspect of an entry-level professional's knowledge base. Fraudsters often look exactly like us, and many are first-time offenders. As such, to understand the causes of white-collar crime, we focus on perpetrators of fraud.[2]

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

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

Most civilized societies are dependent upon people doing the right thing. Despite rewards, punishment, and deterrence, the resources required to fully enforce all laws against every violation would be prohibitively expensive. Prevention is impossible, and even deterrence is costly to implement and does not guarantee an adequate level of compliance. The bottom line is that, in general, a person's normative values of right and wrong dictate their behavior and determine compliance or noncompliance with the law.[3] In other words, in most cases, people choose to follow the law because it is the right thing to do. Further, people usually follow laws with which they agree. For example, if the speed limit on a highway is 50 miles per hour, it is likely that some drivers will exceed that limit unless they understand and agree with the reason for it.

Occupational Fraud and Abuse

Occupational fraud and abuse is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."[4] By the breadth of this definition, occupational fraud and abuse involves a wide variety of conduct by executives, employees, managers, and principals of organizations, ranging from sophisticated investment swindles to petty theft. Common violations include asset misappropriation, fraudulent statements, corruption, pilferage, petty theft, false overtime, using company property for personal benefit, fictitious payroll, and sick time abuses, to name just a few.

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

---

2. See Albrecht's Fraud Examination and the ACFE's Fraud Examiners Manual. Fraud statistics can be found in the ACFE's 2004 Report to the Nation.

3. Adapted from the ACFE's Fraud Examiners Manual, Section 1.21.

4. The Association of Certified Fraud Examiners, The Report to the Nation on Occupational Fraud and Abuse (Austin, TX: ACFE, 2008).

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

White-Collar Crime

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

Organizational Crime

Organizational crime occurs when entities, companies, corporations, not-for-profits, nonprofits, and government bodies, otherwise legitimate and law-abiding organizations, are involved in a criminal offense. In addition, individual organizations can be trust violators when the illegal activities of the organization are reviewed and approved by persons with high standing in an organization, such as board members, executives, and managers. Federal law allows organizations to be prosecuted in a manner similar to individuals.[5] For example, although professional services firm Arthur Andersen's 2002 conviction of obstruction of justice associated with the Enron fraud was later overturned by the U.S. Supreme Court, the conviction, a felony offense, prevented it from auditing public companies. Corporate violations may include administrative breaches, such as noncompliance with agency, regulatory, and court requirements; environmental infringements; fraud and financial crimes, such as financial reporting fraud, bribery, and illegal kickbacks; labor abuses; manufacturing infractions related to public safety and health; and unfair trade practices.

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

---

5. "Thompson Memo," U.S. Department of Justice Memorandum, January 20, 2003: "Principles of Federal Prosecution of Business Organizations."

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

Organized Crime

These crimes are often complex, involving many individuals, organizations, and shell companies, and often cross jurisdictional borders. In this context, fraud examiners and financial forensic professionals often think of terrorist financing, the mob, international hacking, cyber-crime, and drug trafficking. Some of the crimes typically associated with organized crime include money laundering, mail and wire fraud, conspiracy, and racketeering.

Money laundering addresses the means by which organized criminals take money from illegal sources and process it so that it appears "as if" it came from legitimate business sources.

Mail and wire fraud involves schemes that use the postal service or interstate wires, such as telephone calls, email, or other electronic communications, to execute the fraud. The crimes of mail and wire fraud are often used by prosecutors to charge bad actors when other criminal charges are difficult to prove.

Criminal conspiracy occurs when two or more people intend to commit an illegal act and take some steps toward its implementation. A charge of conspiracy is often used as a means of prosecuting individuals involved in illegal organized activity. For example, if Alan, Bob, and Chad plan to rob a bank, and then research the bank's security system, and purchase a gun to implement their plan, they could be charged with criminal conspiracy to commit robbery, even if they don't go through with their plan.

RICO (Racketeering Influence and Corrupt Organizations Act) addresses organizations involved in criminal activity. For example, portions of the RICO Act

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

Torts, Breach of Duty, and Civil Litigation

Black's Law Dictionary defines "tort" as "a private or civil wrong or injury, other than breach of contract, for which the law will provide a remedy in the form of an action for damages." When a tort is committed, the party who was injured is entitled to collect compensation for damages from the wrongdoer for that

private wrong.[6] The tort of contract interference or tortuous interference with contracts occurs when parties are not allowed the freedom to contract without interference from third parties. While the elements of tortuous interference are complex, a basic definition is that the law affords a remedy when someone intentionally persuades another to break a contract already in existence with a third party.[7]

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

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

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

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

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

e. Damages—the plaintiff must establish that damages resulted from the defendant's breach of duty. In order to win an award for damages, the injured party must generally prove two points:

    - The other party was liable for all or part of the damages claimed
    - The injured party suffered damages as the result of the actions, or lack thereof, of the offending party

Furthermore, the amount of damages must be proven with a reasonable degree of certainty as to the amount claimed, and that the defendant could reasonably foresee the likelihood of damages if they failed to meet their obligations. The focus on monetary damages often creates professional opportunities for forensic accountants to work for plaintiffs or defendants. Generally speaking, the threshold is fairly low for a person or organization to sue another in civil court for a tort, breach of contract, or negligence. While judges have the ability to issue summary judgments and dismiss frivolous lawsuits, most judges are more inclined to let the parties negotiate a settlement or let a jury decide the case based on the merits of the arguments and evidence put forth by the plaintiff and the defense. A critical aspect of civil litigation for the forensic accountant and fraud examiner is the understanding that both sides (plaintiff and defendant) are expected to tell their "story." The professional's role is to examine those competing and conflicting stories to see which one, or which elements of each side's story, is consistent with the story being told by the other relevant evidence. It also requires a thorough examination of monetary damage claims, in light of the evidence, particularly how those damage amount(s) relate to the various stories presented by the opposing sides in civil litigation.

6. Marriane M. Jennings, Business: Its Legal, Ethical and Global Environment (Mason, OH: Thomson West, 2006), 367.
7. Ibid., 377.
8. Ibid., 383.

MODULE 2: WHO COMMITS FRAUD AND WHY: THE FRAUD TRIANGLE

Fraudsters, by their very nature, are trust violators. Perpetrators, generally, have achieved a position of trust within an organization and have chosen to violate that trust. According to the ACFE, owners and executives are involved in only about one quarter of all occupational frauds but, when involved, steal significantly larger amounts than lower-level employees. Managers are the second most frequent perpetrators. Finally, line employees are the principal perpetrators in the majority of occupational fraud schemes, yielding average losses to the company of less than $100,000. Research suggests that although males are most frequently the perpetrators, women are the principal perpetrators in approximately 30%–35% of all cases. Fraudsters are found in all age categories and educational achievement levels, but victim losses rise with both the age and education of the principal perpetrator. In the majority of cases, a perpetrator acts alone; however, when fraudsters collude, the losses to the victim organization increase more than fourfold. The following profile summarizes the characteristics of the typical fraud perpetrator.

Fraud perpetrator profile

Male[9]	Well educated
Middle aged to retired	Accountant, upper management, or executive
With the company for five or more years	Acts alone
Never charged or convicted of a criminal offense	

Regardless of whether fraud perpetrators are male or female, the fraudster's profile tends to look like those of average persons. Perhaps the most interesting of all the characteristics listed is that fraudsters typically do not have a criminal background.[10] Furthermore, it is not uncommon for a fraud perpetrator to be a respected member of the community, attend church services, and have a family.

Interestingly, in over 90 percent of the fraud cases examined by the ACFE, the perpetrator had been with the victim organization for more than one year. Dr. W. Steve Albrecht, a pioneer researcher, notes: "Just because someone has been honest for 10 years doesn't mean that they will always be honest." Not surprisingly, the longer the tenure, the larger the average loss. In less than 15% of fraud cases examined did the perpetrator have any prior criminal history. In fact, the typical fraudster is not a pathological criminal, but rather, a seemingly "good person" who has achieved a position of trust. So the critical question remains: what causes good people to make bad choices?

Edwin H. Sutherland

Much of the early literature regarding who commits fraud and why is based upon the works of Edwin H. Sutherland (1883–1950), a criminologist. For those new to the antifraud profession, Sutherland is to the world of white-collar crime, what Freud is to psychology. Indeed, it was Sutherland who coined the term *white-collar crime* in 1939. He intended the definition to mean criminal acts of corporations and individuals acting in their professional capacity. Since that time, however, the term has come to mean almost any financial or economic crime, from the mailroom to the boardroom.

Sutherland was particularly interested in fraud committed by the elite upper-world business executive, either against shareholders or the public. As Gilbert Geis noted, Sutherland said, "General Motors does

9. Donald R. Cressey, Other People's Money (Montclair, NJ: Patterson Smith, 1973), 35.
10. Ibid., 36.

not have an inferiority complex, United States Steel does not suffer from an unresolved Oedipus problem, and the DuPonts do not desire to return to the womb. The assumption that an offender may have such pathological distortions of the intellect or the emotions seems to me absurd, and if it is absurd regarding the crimes of businessmen, it is equally absurd regarding the crimes of persons in the economic lower classes."[11]

Many criminologists believe that Sutherland's most important contribution to criminal literature was elsewhere. Later in his career, he developed the theory of differential association, which is now the most widely accepted theory of criminal behavior in the twentieth century. Until Sutherland's landmark work in the 1930s, most criminologists and sociologists held the view that crime was genetically based, that criminals beget criminal offspring. Sutherland was able to explain crime's environmental considerations through the theory of differential association. The theory's basic tenet is that crime is learned, much like we learn math, English, or guitar playing.[12]

Sutherland believed this learning of criminal behavior occurred with other persons in a process of communication. Therefore, he reasoned, criminality cannot occur without the assistance of other people. Sutherland further theorized that the learning of criminal activity usually occurred within intimate personal groups. This explains, in his view, how a dysfunctional parent is more likely to produce dysfunctional offspring. Sutherland believed that the learning process involved two specific areas: the techniques to commit the crime; and the attitudes, drives, rationalizations, and motives of the criminal mind. You can see how Sutherland's differential association theory fits with occupational offenders. Organizations that have dishonest employees will eventually infect a portion of honest ones. It also goes the other way: honest employees will eventually have an influence on some of those who are dishonest.

Donald R. Cressey and the Fraud Triangle

One of Sutherland's brightest students during the 1940s was Donald R. Cressey (1919–1987). Although much of Sutherland's research concentrated on upper-world criminality, Cressey took his own studies in a different direction. Working on his Ph.D. in criminology, he decided his dissertation would concentrate on embezzlers. To serve as a basis for his research, Cressey interviewed about 200 incarcerated inmates at prisons in the Midwest.

Cressey's Hypothesis

Embezzlers, whom he called "trust violators," intrigued Cressey. He was especially interested in the circumstances that led them to be overcome by temptation. For that reason, he excluded from his research those employees who took their jobs for the purpose of stealing—a relatively minor number of offenders at that time. Upon completion of his interviews, he developed what still remains as the classic model for the occupational offender. His research was published in *Other People's Money: A Study in the Social Psychology of Embezzlement*.

Cressey's final hypothesis read as follows:

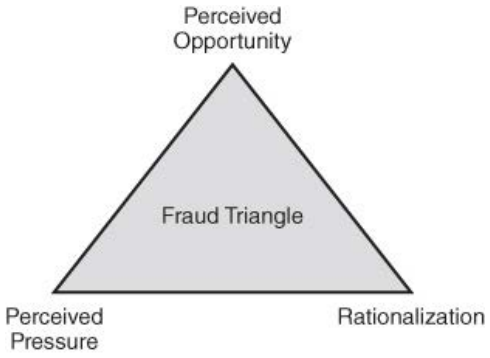
> *Trusted persons become trust violators when they conceive of themselves as having a financial problem that is nonshareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in*

11. Gilbert Geis, On White Collar Crime (Lexington, KY: Lexington Books, 1982).
12. Larry J. Siegel, Criminology, 3rd ed. (New York: West Publishing Company, 1989), 193.

that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.[13]

In a 1991 article penned by Dr. Steve Albrecht, he organized Cressey's three conditions into a tool that has become known as the "fraud triangle" (Figure 2-1).[14] One leg of the triangle represents perceived pressure. The second leg is perceived opportunity, and the final leg denotes rationalization.

FIGURE 2-1 FRAUD TRIANGLE



Nonshareable Financial Pressures

The role of perceived nonshareable financial pressures is important. Cressey reported that when the trust violators were asked to explain why they refrained from violation of other positions of trust they might have held at previous times, or why they had not violated the subject position at an earlier time, those who had an opinion expressed the equivalent of one or more of the following quotations: (a) "There was no need for it like there was this time." (b) "The idea never entered my head." (c) "I thought it was dishonest then, but this time it did not seem dishonest at first."[15] "In all cases of trust violation encountered, the violator considered that a financial problem which confronted him could not be shared with persons who, from a more objective point of view, probably could have aided in the solution of the problem."[16]

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

Thus a man could lose considerable money at the racetrack daily, but the loss, even if it construed a problem for the individual, might not constitute a nonshareable problem for him. Another man might define the problem as one that must be kept secret and private. Similarly, a failing bank or business might be considered by one person as presenting problems which must be shared with business associates and members of the community, while another person might conceive these problems as nonshareable.[17]

13. Donald R. Cressey, Other People's Money (Montclair, NJ: Patterson Smith, 1973), 30.
14. Albrecht W. Steve. 1991. "Fraud in Government Entities: The Perpetrators and the Types of Fraud," Government Finance Review, December, pp. 27–30.
15. Ibid., 33.
16. Ibid., 34.
17. Ibid., 34.

In addition to being nonshareable, the problem that drives the fraudster is described as "financial" because these are the types of problems that can generally be solved by the theft of cash or other assets. A person with large gambling debts, for instance, would need cash to pay those debts. Cressey noted, however, that there are some nonfinancial problems that could be solved by misappropriating funds through a violation of trust. For example, a person who embezzles in order to get revenge on her employer for perceived "unfair" treatment uses financial means to solve what is essentially a nonfinancial problem.[18]

Through his research, Cressey also found that the nonshareable problems encountered by the people he interviewed arose from situations that could be divided into six basic categories:

- Violation of ascribed obligations
- Problems resulting from personal failure
- Business reversals
- Physical isolation
- Status gaining
- Employer–employee relations

All these situations dealt in some way with status-seeking or status-maintaining activities by the subjects.[19] In other words, the nonshareable problems threatened the status of the subjects, or threatened to prevent them from achieving a higher status than the one they occupied at the time of their violation.

Violations of Ascribed Obligations

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

> *Financial problems incurred through nonfinancial violations of positions of trust often are considered as nonshareable by trusted persons since they represent a threat to the status which holding the position entails. Most individuals in positions of financial trust, and most employers of such individuals, consider that incumbency in such a position necessarily implies that, in addition to being honest, they should behave in certain ways and should refrain from participation in some other kinds of behavior.*[20]

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

When these persons then fall into debt or incur large financial obligations as a result of conduct that is "beneath" them, they feel unable to share the problem with their peers because this would require admitting that they have engaged in the dishonorable conduct that lies at the heart of their financial

18. Ibid., 35.
19. Ibid., 36.
20. Ibid., 36.

difficulties. Basically, by admitting that they had lost money through some disreputable act, they would be admitting—at least in their own minds—that they are unworthy to hold their trusted positions.

Problems Resulting from Personal Failure Problems resulting from personal failures, Cressey writes, are those that the trusted person feels he caused through bad judgment and therefore feels personally responsible for. Cressey cites one case in which an attorney lost his life's savings in a secret business venture. The business had been set up to compete with some of the attorney's clients, and though he thought his clients probably would have offered him help if they had known what dire straits he was in, he could not bring himself to tell them that he had secretly tried to compete with them. He also was unable to tell his wife that he'd squandered their savings. Instead, he sought to alleviate the problem by embezzling funds to cover his losses.[21]

> *While some pressing financial problems may be considered as having resulted from "economic conditions," "fate," or some other impersonal force, others are considered to have been created by the misguided or poorly planned activities of the individual trusted person. Because he fears a loss of status, the individual is afraid to admit to anyone who could alleviate the situation the fact that he has a problem which is a consequence of his "own bad judgment" or "own fault" or "own stupidity."[22] In short, pride goeth before the fall.[23] If the potential offender has a choice between covering his poor investment choices through a violation of trust and admitting that he is an unsophisticated investor, it is easy to see how some prideful people's judgment could be clouded.*

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

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

> *Case 36. There are very few people who are able to walk away from a failing business. When the bridge is falling, almost everyone will run for a piece of timber. In business there is this eternal optimism that things will get better tomorrow. We get to working on the business, keeping it going, and we get almost mesmerized by it … Most of us don't know when to quit, when to say, 'This one has me licked. Here's one for the opposition.'[24]*

It is interesting to note that even in situations where the problem is perceived to be out of the trusted person's control, the issue of status still plays a big role in that person's decision to keep the problem a secret. The subject of Case 36 continued, "If I'd have walked away and let them all say, 'Well, he wasn't a success as a manager, he was a failure,' and took a job as a bookkeeper, or gone on the farm, I would have been all right. But I didn't want to do that."[25] The desire to maintain the appearance of success was a common theme in the cases involving business reversals.

---

21. Ibid., 41.
22. Ibid., 42.
23. Proverbs 16:18.
24. Cressey, 47.
25. Ibid., 48.

Physical Isolation The fourth category Cressey identified consisted of problems resulting from physical isolation. In these situations, the trusted person simply has no one to turn to. It's not that he is afraid to share his problem; it's that he has no one to share the problem with. He is in a situation where he does not have access to trusted friends or associates who would otherwise be able to help him. Cressey cited the subject of Case 106 in his study, a man who found himself in financial trouble after his wife had died. In her absence, he had no one to go to for help and he wound up trying to solve his problem through an embezzlement scheme.[26]

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

> *The structuring of status ambitions as being nonshareable is not uncommon in our culture, and it again must be emphasized that the structuring of a situation as nonshareable is not alone the cause of trust violation. More specifically, in this type of case a problem appears when the individual realizes that he does not have the financial means necessary for continued association with persons on a desired status level, and this problem becomes nonshareable when he feels that he can neither renounce his aspirations for membership in the desired group nor obtain prestige symbols necessary to such membership.*[27]

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

Employer–Employee Relations Finally, Cressey described problems resulting from employer–employee relationships. The most common, he stated, was an employed person who resents his status within the organization in which he is trusted and at the same time feels he has no choice but to continue working for the organization. The resentment can come from perceived economic inequities, such as pay, or from the feeling of being overworked or underappreciated. Cressey said this problem becomes nonshareable when the individual believes that making suggestions to alleviate his perceived maltreatment will possibly threaten his status in the organization.[28] There is also a strong motivator for the perceived employee to want to "get even" when he feels ill-treated.

The Importance of Solving the Problem in Secret

Given that Cressey's study was done in the early 1950s, the workforce was obviously different from today. But the employee faced with an immediate, nonshareable financial need hasn't changed much over the years. That employee is still placed in the position of having to find a way to relieve the pressure

26. Ibid., 52-53.
27. Ibid., 54.
28. Ibid., 57.

that bears down upon him. Simply stealing money, however, is not enough; Cressey found it was crucial that the employee be able to resolve the financial problem in *secret*. As we have seen, the nonshareable financial problems identified by Cressey all dealt in some way with questions of status; the trust violators were afraid of losing the approval of those around them and so were unable to tell others about the financial problems they encountered. If they could not share the fact that they were under financial pressure, it follows that they would not be able to share the fact that they were resorting to illegal means to relieve that pressure. To do so would be to admit the problems existed in the first place.

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

> *In all cases [in the study] there was a distinct feeling that, because of activity prior to the defalcation, the approval of groups important to the trusted person had been lost, or a distinct feeling that present group approval would be lost if certain activity were revealed [the nonshareable financial problem], with the result that the trusted person was effectively isolated from persons who could assist him in solving problems arising from that activity*[29] *(emphasis added).*

Perceived Pressure

Many people inside any organizational structure have at least some access to cash, checks, or other assets. However, according to Cressey's hypothesis, it is a perceived pressure that causes individuals to seriously consider availing themselves of the opportunity presented by, for example, an internal control weakness. In today's terms, fraud pressures can arise from financial problems, such as living beyond one's means, greed, high debt, poor credit, family medical bills, investment losses, or children's educational expenses. Pressures may also arise from vices, such as gambling, drugs, or an extramarital affair.

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

Even in civil litigation, pressure can cause one organization to violate the terms and conditions of a contract. For example, a company may not be able to complete a construction project on time. As such, they may take "shortcuts" in violation of contract terms due to the pressure of an impending deadline. In other cases, an organization is attempting to raise investment capital; so, company leadership might "juice" (increase) the valuation for which they claim the business is worth.

Unanticipated pressures from a variety of sources may sometimes cause a person to act in inappropriate ways. It is also inherent upon the professional to realize that the majority of persons facing these same pressures do not commit fraud or financial crimes, but rather find some alternative, nonnefarious means of relieving the pressure.

---

29. Ibid., 66.

Perceived Opportunity

According to the fraud triangle model, the presence of a nonshareable financial problem by itself will not lead an employee to commit fraud. The key to understanding Cressey's theory is to remember that all three elements must be present for a trust violation to occur. The nonshareable financial problem creates the motive for the crime to be committed, but the employee must also ***perceive*** that he has an opportunity to commit the crime without being caught. This *perceived opportunity* constitutes the second element.

In Cressey's view, there were two components of the perceived opportunity to commit a trust violation: general information and technical skill. *General information* is simply the knowledge that the employee's position of trust could be violated. This knowledge might come from hearing of other embezzlements, from seeing dishonest behavior by other employees, or just from generally being aware of the fact that the employee is in a position where he could take advantage of his employer's faith in him. *Technical skill* refers to the abilities needed to commit the violation. These are usually the same abilities that the employee needs to have to obtain and keep his position in the first place. Cressey noted that most embezzlers adhere to their occupational routines (and their job skills) in order to perpetrate their crimes.[30]

In essence, the perpetrator's job will tend to define the type of fraud he has the opportunity to commit. "Accountants use checks which they have been entrusted to dispose of, sales clerks withhold receipts, bankers manipulate seldom-used accounts or withhold deposits, real estate fraudsters use deposits entrusted to them, and so on."[31] Obviously, the general information and technical skill that Cressey identified are not unique to occupational offenders; most, if not all, employees have these same characteristics. But because trusted persons possess this information and skill, when they face a nonshareable financial problem they see it as something that they have the power to correct. They apply their understanding of the possibility for trust violation to the specific crises they are faced with.

Cressey observed, "It is the next step which is significant to violation: the application of the general information to the specific situation, and conjointly, the perception of the fact that in addition to having general possibilities for violation, a specific position of trust can be used for the specific purpose of solving a nonshareable problem."[32]

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

30. Ibid., 84.
31. Ibid., 84.
32. Ibid., 84.

Fraud deterrence begins in the employee's mind. Employees who perceive that they will be caught are less likely to engage in fraudulent conduct. The logic is hard to dispute. Exactly how much deterrent effect this concept provides depends on a number of factors, both internal and external. But internal controls can have a deterrent effect only when the employee perceives that such a control exists in both design and operation, and the controls are likely to uncover the potential fraud. This is referred to as the "perception of detection," and it is a critical aspect of antifraud efforts. Alternatively stated, "hidden" controls have little deterrent effect. Conversely, controls that are not even in place—but are perceived to be—may have deterrent value.

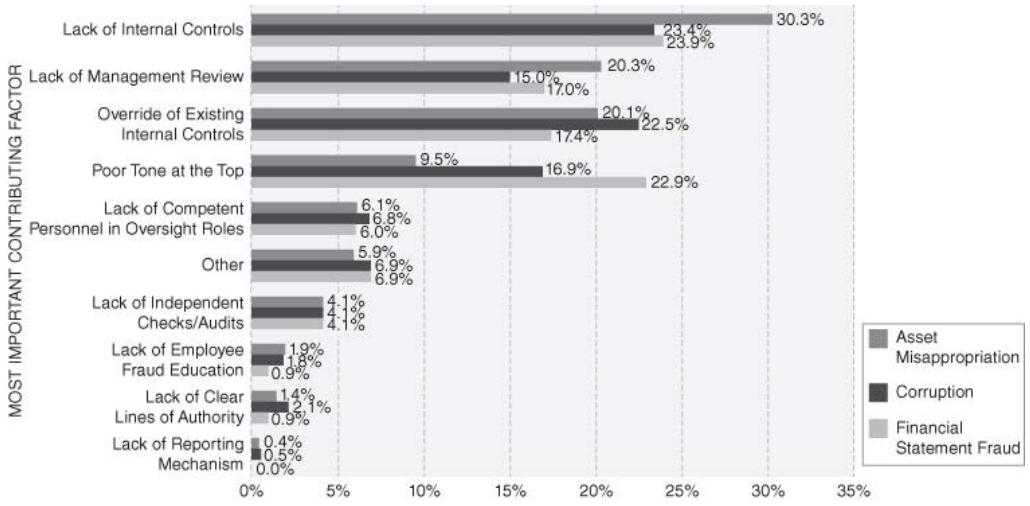
According to the 2016 ACFE Report to the Nations (see Figure 2-2), the general implementation rates of antifraud controls have remained notably consistent throughout their studies, although the ACFE has seen a slight uptick in the prevalence of each control over the last six years. The most notable changes have been in the implementation rates of hotlines and fraud training for employees, which have increased approximately 9% and 8%, respectively, since 2010. On the other end of the spectrum, the percentage of organizations that undergo external audits of their financial statements has remained relatively flat, with less than a 1% increase over the same period.

FIGURE 2-2 TRENDS IN THE IMPLEMENTATION OF ANTIFRAUD CONTROL

Control	2010 Implementation rate	2016 Implementation rate	Change from 2010–2016
Hotline	51.2%	60.1%	8.9%
Fraud Training for Employees	44.0%	51.6%	7.6%
Anti-fraud Policy	42.8%	49.6%	6.8%
Code of Conduct	74.8%	81.1%	6.3%
Management Review	58.8%	64.7%	5.9%
Surprise Audits	32.3%	37.8%	5.6%
Fraud Training for Managers/ Executives	46.2%	51.3%	5.2%
Independent Audit Committee	58.4%	62.5%	4.1%
Management Certification of Financial Statements	67.9%	71.9%	4.0%
Rewards for Whistleblowers	8.6%	12.1%	3.5%
Job Rotation/Mandatory Vacation	16.6%	19.4%	2.8%
External Audit of Internal Controls over Financial Reporting	65.4%	67.6%	2.2%
Employee Support Programs	54.6%	56.1%	1.5%
External Audit of Financial Statements	80.9%	81.7%	0.8%

In Figure 2-3, the ACFE examined the impact of internal control weaknesses by the type of fraud scheme perpetrated: asset misappropriation, corruption, and financial statement fraud. The findings suggest that organizations that lacked internal controls were more susceptible to asset misappropriation schemes, while corruption schemes, more often, involved an override of existing controls. Further, poor "tone at the top" was much more likely to contribute to financial statement fraud than either of the other two categories of occupational fraud.

FIGURE 2-3 INTERNAL CONTROL WEAKNESSES THAT CONTRIBUTED TO FRAUD



Rationalizations

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

Cressey pointed out that rationalization is not an *ex post facto* means of justifying a theft that has already occurred. Significantly, rationalization is a necessary component of the crime before it takes place; in fact, it is a part of the motivation for the crime.[33]Because the embezzler does not view himself as a criminal, he must justify his misdeeds before he ever commits them. Rationalization is necessary so that the perpetrator can make his illegal behavior acceptable to him and maintain his concept of himself as a trusted person.[34] After the criminal act has taken place, the rationalization will often be abandoned. This reflects the nature of us all: the first time we do something contrary to our morals, it bothers us. As we repeat the act, it becomes easier. One hallmark of occupational fraud and abuse offenders is that once the line is crossed, the illegal acts become more or less continuous. So an occupational fraudster might begin stealing with the thought that "I'll pay the money back," but after the initial theft is successful, he will usually continue to steal past the point where there is any realistic possibility of repaying the stolen funds.

Cressey found that the embezzlers he studied, generally, rationalized their crimes by viewing them (1) as essentially noncriminal, (2) as justified, or (3) as part of a general irresponsibility for which they were

33. Note: In criminology research, rationalization is the moral justification after the bad act and the closely related construct of neutralization is the moral justification before the bad act.
34. Cressey, 94-95.

not completely accountable.[35] He also found that the rationalizations used by trust violators tended to be linked to their positions and to the manner in which they committed their violations. He examined this by dividing the subjects of his study into three categories: *independent businessmen*, *long-term violators*, and *absconders*. He discovered that each group had its own type of rationalization.

Independent Businessmen The *independent businessmen* in Cressey's study were persons who were in business for themselves and who converted deposits that had been entrusted to them.[36] Perpetrators in this category tended to use one of two common excuses: (1) they were "borrowing" the money they converted or (2) the funds entrusted to them were really theirs—you can't steal from yourself. Cressey found the "borrowing" rationalization was the most frequently used. These perpetrators also tended to espouse the idea that "everyone" in business misdirects deposits in some way, which therefore made their own misconduct less wrong than stealing.[37] Also, the independent businessmen almost universally felt their illegal actions were predicated by an "unusual situation," which Cressey perceived to be in reality a nonshareable financial problem.

Long-Term Violators Cressey defined long-term violators as individuals who converted their employer's funds, or funds belonging to their employer's clients, by taking relatively small amounts over a period of time.[38] Similar to independent businessmen, the long-term violators also generally preferred the "borrowing" rationalization. Other rationalizations of long-term violators were noted, too, but they almost always were used in connection with the "borrowing" theme: (1) they were embezzling to keep their families from shame, disgrace, or poverty; (2) theirs was a case of "necessity"; their employers were cheating them financially; or (3) their employers were dishonest toward others and deserved to be fleeced. Some even pointed out that it was more difficult to return the funds than to steal them in the first place and claimed they did not pay back their "borrowings" because they feared that would lead to detection of their thefts. A few in the study actually kept track of their thefts but most only did so at first. Later, as the embezzlements escalated, it is assumed that the offender would rather not know the extent of his "borrowings."

All of the long-term violators in the study expressed a feeling that they would like to eventually "clean the slate" and repay their debt. This feeling usually arose even before the perpetrators perceived that they might be caught. Cressey pointed out that at this point, whatever fear the perpetrators felt in relation to their crimes was related to losing their social position by the exposure of their nonshareable problem, not the exposure of the theft itself or the possibility of punishment or imprisonment. This is because their rationalization still prevented them from perceiving their misconduct as criminal. "The trust violator cannot fear the treatment usually accorded criminals until he comes to look upon himself as a criminal."[39]

Eventually, most of the long-term violators finally realized they were "in too deep." It is at this point that the embezzler faces a crisis. While maintaining the borrowing rationalization (or other rationalizations, for that matter), the trust violator is able to maintain his self-image as a law-abiding citizen; but when the level of theft escalates to a certain point, the perpetrator is confronted with the idea that he is behaving in

35. Ibid., 93.
36. Ibid., 101-102.
37. Ibid., 102.
38. Ibid., 102.
39. Ibid., 120-121.

a criminal manner. This is contrary to his personal values and the values of the social groups to which he belongs. This conflict creates a great deal of anxiety for the perpetrator. A number of offenders described themselves as extremely nervous and upset, tense, and unhappy.[40]

Without the rationalization that they are borrowing, long-term offenders in the study found it difficult to reconcile converting money, at the same time seeing themselves as honest and trustworthy. In this situation, they have two options: (1) they can readopt the attitudes of the (law-abiding) social group that they identified with before the thefts began or (2) they can adopt the attitudes of the new category of persons (criminals) with whom they now identify.[41] From his study, Cressey was able to cite examples of each type of behavior. Those who sought to readopt the attitudes of their law-abiding social groups "may report their behavior to the police or to their employer, quit taking funds or resolve to quit taking funds, speculate or gamble wildly in order to regain the amounts taken, or 'leave the field' by absconding or committing suicide."[42] On the other hand, those who adopt the attitudes of the group of criminals to which they now belong "may become reckless in their defalcations, taking larger amounts than formerly with fewer attempts to avoid detection and with no notion of repayment."[43]

Absconders The third group of offenders Cressey discussed was absconders—people who take the money and run. Cressey found that the nonshareable problems for absconders usually resulted from physical isolation. He observed that these people "usually are unmarried or separated from their spouses, live in hotels or rooming houses, have few primary group associations of any sort, and own little property. Only one of the absconders interviewed had held a higher status position of trust, such as an accountant, business executive, or bookkeeper."[44] Cressey also found that the absconders tended to have lower occupational and socioeconomic status than the members of the other two categories.

Because absconders tended to lack strong social ties, Cressey found that almost any financial problem could be defined as nonshareable for these persons, and also that rationalizations were easily adopted because the persons only had to sever a minimum of social ties when they absconded.[45] The absconders rationalized their conduct by noting that their attempts to live honest lives had been futile (hence their low status). They also adopted an attitude of not caring what happened to themselves and a belief that they could not help themselves because they were predisposed to criminal behavior. The latter two rationalizations, which were adopted by absconders in Cressey's study, allowed them to remove almost all personal accountability from their conduct.[46]

In the 1950s, when Cressey gathered this data, embezzlers were considered persons of higher socioeconomic status who took funds over a limited period of time because of some personal problem such as drinking or gambling, while "thieves" were considered persons of lower status who took whatever funds were at hand. Cressey noted,

---

40. Ibid., 121.
41. Ibid., 122.
42. Ibid., 121.
43. Ibid., 122.
44. Ibid., 128.
45. Ibid., 129.
46. Ibid., 128-129.

> *Since most absconders identify with the lower status group, they look upon themselves as belonging to a special class of thieves rather than trust violators. Just as long-term violators and independent businessmen do not at first consider the possibility of absconding with the funds, absconders do not consider the possibility of taking relatively small amounts of money over a period of time.*[47]

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

Conjuncture of Events

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

> *[a] trust violation takes place when the position of trust is viewed by the trusted person according to culturally provided knowledge about and rationalizations for using the entrusted funds for solving a non- shareable problem, and that the absence of any of these events will preclude violation. The three events make up the conditions under which trust violation occurs and the term "cause" may be applied to their conjecture since trust violation is dependent on that conjuncture. Whenever the conjuncture of events occurs, trust violation results, and if the conjuncture does not take place there is no trust violation.*[48]

Cressey's Conclusion

Cressey's classic fraud triangle helps explain the nature of many—but not all—occupational offenders. For example, although academicians have tested his model, it has still not fully found its way into practice in terms of developing fraud prevention programs. Our sense tells us that one model—even Cressey's—will not fit all situations. Plus, the study is nearly half a century old. There has been considerable social change in the interim. And now, many antifraud professionals believe there is a new breed of occupational offender—those who simply lack a conscience sufficient to overcome temptation. Even Cressey saw the trend later in his life.

After doing this landmark study in embezzlement, Cressey went on to a distinguished academic career, eventually authoring 13 books and nearly 300 articles on criminology. He rose to the position of Professor Emeritus in Criminology at the University of California, Santa Barbara.

---

47. Ibid., 133.
48. Ibid., 139.

Joe Wells, Founder and Chairman of the Association of Certified Fraud Examiners Remembers Donald Cressey

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

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

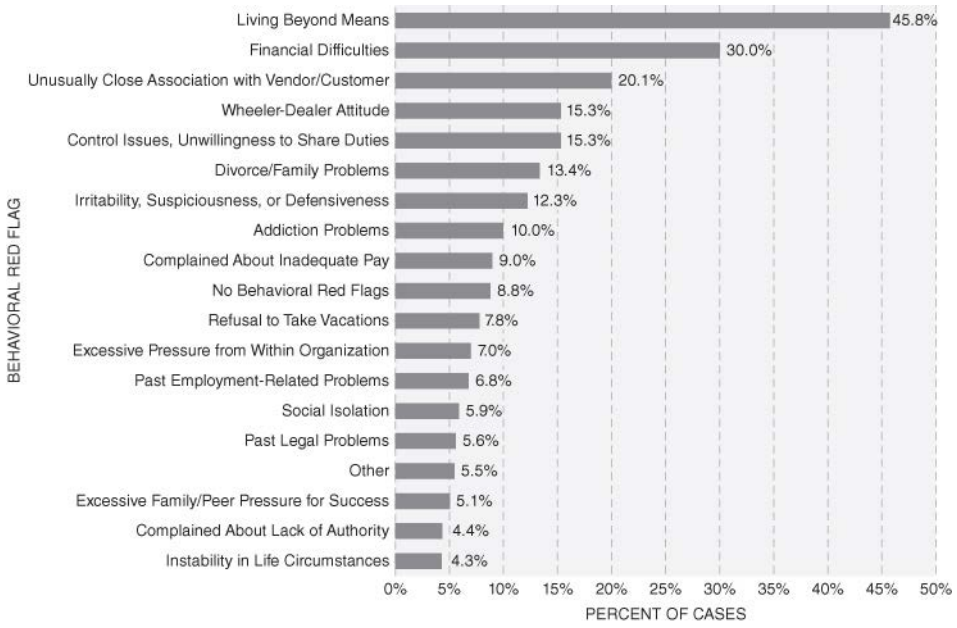
From there, the vice president succumbed to full kickbacks. By the time the dust settled, he had secretly pocketed about $3.5 million. After completing the internal investigation for the company, assembling the documentation and interviews, I worked with prosecutors at the company's request to put the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

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

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

In Figure 2-4 from the ACFE's 2016 Report to the Nations, survey respondents provided their observations with regard to which, if any, warning signs had been displayed by the perpetrator before the fraud was detected. These warning signs are consistent with various attributes of the fraud triangle: pressure, opportunity, and rationalization. In more than 91% of cases, at least one behavioral red flag was observed prior to detection, and in 57% of cases two or more red flags were seen. As Figure 2-4 illustrates, the six most common behavioral red flags are as follows: (1) living beyond means; (2) financial difficulties; (3) unusually close association with a vendor or customer; (4) a "wheeler-dealer" attitude involving shrewd or unscrupulous behavior; (5) excessive control issues or unwillingness to share duties; and (6) recent divorce or family problems. Approximately 79% of the perpetrators in the ACFE study displayed at least one of these six red flags during their schemes. What is even more notable is how consistent the distribution of red flags has been over time. The six most common red flags shown in Figure 2-4 have also been the six most common red flags in every report since 2008, when the ACFE first began tracking this data.

FIGURE 2-4 BEHAVIORAL RED FLAGS DISPLAYED BY PERPETRATORS



MODULE 3: THE ROLE OF PERSONAL INTEGRITY, CAPABILITY, GENDER, AND THE INFLUENCE OF THE ORGANIZATION

According to the Intelligencer/Wheeling News Register, law enforcement officials believe Shelly Lough took in excess of $1 million from Bethany College in an effort to keep another woman, Rachelle Weese, quiet about an alleged affair.

According to William J. Ihlenfeld II, U.S. attorney for the Northern District of West Virginia, the charge alleges Weese used violence or fear to extort money from Lough, who is the former manager of the cashier's office at Bethany College. Over a 16-month period, Lough stole the money while she cashed payroll and personal checks from staff and students and altered records to hide the thefts.

The criminal complaint against Weese alleges that she threatened to reveal to Lough's husband that Lough was in a relationship outside her marriage if she did not pay money. Although the exact amount Weese was paid in the alleged extortion attempt is not known, Ihlenfeld said the FBI has accounted for various sums adding up to a "substantial" amount. So far, the agency has identified from business records and other means some of Weese's assets, including paying $35,000 cash for a new SUV and some "very expensive" jewelry totaling more than $25,000. A search warrant executed at Weese's home also turned up $262,000 in cash.

Lough received probation and an order of restitution, while Jason Kirkland Weese, 31 at the time, who along with his wife Rachelle extorted more than $1 million will serve 63 months in prison for his role in the crime. Rachelle Weese's sentence is not available.[49]

The challenge to the fraud triangle is that while it explains many garden variety frauds, oftentimes, the fraudster's decision-making process, the facts and circumstances surrounding the bad act are complex. In this module, we offer research findings that supplement the early works of Sutherland and Cressey.

The Fraud Scale

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

Albrecht's research contributions in fraud have been enormous. In the early 1980s, he and two of his colleagues, Keith Howe and Marshall Romney, conducted an analysis of 212 frauds, leading to their book entitled *Deterring Fraud: The Internal Auditor's Perspective*.[50] The participants in the survey were internal auditors of companies that had been victims of fraud.

Albrecht and his colleagues believed that, taken as a group, occupational fraud perpetrators are hard to profile and that fraud is difficult to predict. His research included an effort to assemble a complete list of pressure, opportunity, and integrity variables, resulting in a list of fifty possible red flags or indicators of occupational fraud and abuse. These variables fell into two principal categories: perpetrator characteristics and organizational environment. Table 2-1 shows the complete list of occupational fraud red flags that Albrecht identified.[51]

49. See J. Bobby-Gilbert, "Bethany Case Goes to $1 Million," Intelligencer/Wheeling News Register, February 18, 2104; "Weese Sentenced in Lough Extortion," Intelligencer/Wheeling News Register, November 14, 2014.
50. W. Steve Albrecht, Keith R. Howe, and Marshall B. Romney, Deterring Fraud: The Internal Auditor's Perspective (Altamonte Springs, FL: The Institute of Internal Auditor's Research Foundation, 1984).
51. Ibid., 13-14.

TABLE 2-1 OCCUPATIONAL FRAUD RED FLAGS

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

The researchers gave participants both sets of twenty-five motivating factors and asked which factors were present in the frauds they had dealt with. Participants were asked to rank these factors on a seven-point scale indicating the degree to which each factor existed in their specific frauds. The ten most highly ranked factors from the list of personal characteristics, based on this study, are as follows[52]:

1. Living beyond their means
2. An overwhelming desire for personal gain
3. High personal debts
4. A close association with customers
5. Feeling pay was not commensurate with responsibility
6. A wheeler-dealer attitude
7. Strong challenge to beat the system
8. Excessive gambling habits
9. Undue family or peer pressure
10. No recognition for job performance

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

The ten most highly ranked factors from the list dealing with organizational environment are as follows[53]:

1. Placing too much trust in key employees
2. Lack of proper procedures for authorization of transactions
3. Inadequate disclosures of personal investments and incomes
4. No separation of authorization of transactions from the custody of related assets
5. Lack of independent checks on performance
6. Inadequate attention to details
7. No separation of custody of assets from the accounting for those assets
8. No separation of duties between accounting function
9. Lack of clear lines of authority and responsibility
10. Department that is not frequently reviewed by internal auditors

Readers are likely to notice that Dr. Albrecht explicitly introduced the role of the organization into the actions of the fraudsters. This role was inherent in Cressey's efforts but Albrecht brought these issues to the forefront.

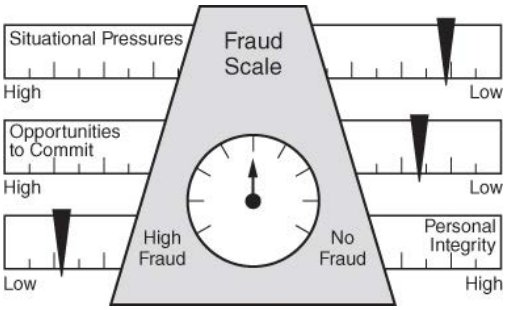
52. Ibid., 32.
53. Ibid., 39.

Most of the factors on this list affect employees' opportunity to commit fraud without being caught. Opportunity, as you will recall, was the second factor identified in Cressey's fraud triangle. In many ways, the study by Albrecht et al. supported Cressey's model. Like Cressey's study, the Albrecht study suggests that there are three factors involved in occupational frauds:

> *… it appears that three elements must be present for a fraud to be committed: a situational pressure (nonshareable financial pressure), a perceived opportunity to commit and conceal the dishonest act (a way to secretly resolve the dishonest act or the lack of deterrence by management), and some way to rationalize (verbalize) the act as either being inconsistent with one's personal level of integrity or justifiable.*[54]

Armed with these research findings, Albrecht substituted personal integrity for rationalization and developed the "Fraud Scale" (Figure 2-5), which included the components of *situational pressures, perceived opportunities*, and *personal integrity*.[55] When situational pressures and perceived opportunities are high and personal integrity is low, occupational fraud is much more likely to occur than when the opposite is true.[56]

FIGURE 2-5 THE FRAUD SCALE



Albrecht described situational pressures as "the immediate problems individuals experience within their environments, the most overwhelming of which are probably high personal debts or financial losses."[57] Opportunities to commit fraud, Albrecht says, may be created by individuals or by deficient or missing internal controls. Personal integrity "refers to the personal code of ethical behavior each person adopts. While this factor appears to be a straightforward determination of whether the person is honest or dishonest, moral development research indicates that the issue is more complex."[58]

In addition to its findings on motivating factors of occupational fraud, the Albrecht study also disclosed several interesting relationships between the perpetrators and the frauds they committed. For example, perpetrators of large frauds used the proceeds to purchase new homes and expensive automobiles, recreation property, and expensive vacations; support extramarital relationships; and make speculative investments. Those committing small frauds did not.[59]

---

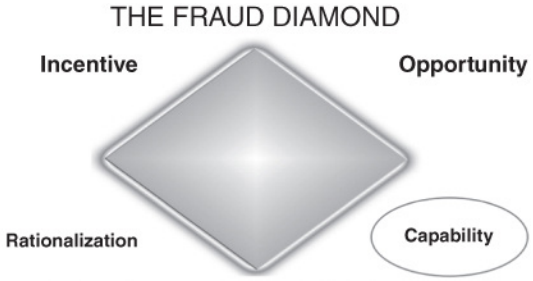
54. Ibid., 5.
55. Ibid., 6.
56. Ibid., 5.
57. Ibid., 5.
58. Ibid., 6.
59. Ibid., 42.

There were other observations: perpetrators who were interested primarily in "beating the system" committed larger frauds. However, perpetrators who believed their pay was not adequate committed primarily small frauds. Lack of segregation of responsibilities, placing undeserved trust in key employees, imposing unrealistic goals, and operating on a crisis basis were all pressures or weaknesses associated with large frauds. College graduates were less likely to spend the proceeds of their loot to take extravagant vacations, purchase recreational property, support extramarital relationships, and buy expensive automobiles. Finally, those with lower salaries were more likely to have a prior criminal record.[60]

Capability and Arrogance

In a 2004 CPA Journal article, Wolfe and Hermanson[61] argue that the fraud triangle could be enhanced to improve both fraud prevention and detection by considering a fourth element, capability. The authors altered the fraud triangle by presenting a four-sided fraud diamond (Figure 2-6). The fourth side adds an individual's capability, which is tied to an individual's personal traits and abilities. The authors suggest that capability plays an important role in whether fraud may actually occur.

FIGURE 2-6 THE FRAUD DIAMOND



Source: Wolfe and Hermanson, December 2004/The CPA Journal.

Examining evidence associated with multibillion-dollar fraud, Wolfe and Hermanson suggest that many of these large-dollar frauds would not have occurred without the perpetrator(s) having the right capabilities. As described by the authors, opportunity opens the door to fraud, incentive and rationalization draw the fraudster closer to the door, but the fraudster must have the capability to recognize the opportunity to walk through that door to commit the fraudulent act and conceal it.

Essential traits thought necessary for committing fraud, especially for large sums over long periods of time, include a combination of intelligence, position, ego, and the ability to deal well with stress. The person's position or function within the organization may furnish the ability to create or exploit an opportunity for fraud. Additionally, the potential perpetrator must have sufficient knowledge to understand and exploit internal control weaknesses and to use position, function, or authorized access to his or her advantage. The largest frauds are committed by intelligent, experienced, and creative people with a solid grasp of company controls and vulnerabilities. This knowledge is used to leverage the person's responsibility over, or authorized access to, personnel, systems, or assets. This type of person has a

60. Ibid., 15.
61. See David T. Wolfe and Dana Hermanson, "The Fraud Diamond: Considering the Four Elements of Fraud," The CPA Journal (December 2004); Jonathan Marks, "Playing Offense in a High-risk Environment"; Crowe Horwath (2010); J. Dorminey, S. Fleming, M.-J. Kranacher, and R. Riley, "The Evolution of Fraud Theory," Issues in Accounting Education 27, no. 2 (2012): 555–79.

strong ego and great confidence that he will not be detected, or he believes that he could easily talk himself out of trouble, if caught.

Further, as noted by Pavlo and Weinburg, committing and managing a fraud over a long period of time can be extremely stressful.[62] Therefore, in addition to being knowledgeable and confident, a successful fraudster also deals well with the stress of committing and concealing the fraud.

In 2010, Jonathan Marks argued for examination of the role of arrogance in fraud. Arrogance, or lack of conscience, is an attitude of superiority and entitlement or greed on the part of a person who believes that corporate policies and procedures simply do not apply to him. This person, perhaps fueled by today's compensation structures, has disregard for the consequences bestowed upon his victims. Competence and arrogance play a major role in determining whether an employee today has what it takes to perpetrate a fraud (Figure 2-7).

FIGURE 2-7 CROWE'S FRAUD PENTAGON™

The Role of the Organization

Ramamoorti, Morrison, Koletar, and Pope in their 2013 book, *A.B.C.'s of Behavioral Forensics: Applying Psychology to Financial fraud Prevention and Detection*, offer three levels of the fraud paradigm: bad apples (i.e., individuals such as employees) can collude into bad bushels (i.e., groups of employees), which may cause the whole crop (i.e., organization) to be ruined.[63]While providing insight into fraud acts, these authors are not the first to suggest that the organization plays a role in fraud.

In 1983, Richard C. Hollinger and John P. Clark published federally funded research involving surveys of nearly 10,000 American workers. In their book, *Theft by Employees*, the two researchers reached a different conclusion from Cressey. They found that employees steal primarily as a result of workplace conditions. They also concluded that the true costs of employee theft are vastly understated: "In sum, when we take into consideration the incalculable social costs … the grand total paid for theft in the workplace is no doubt grossly underestimated by the available financial estimates."[64] Following is a summary of the Hollinger and Clark research with respect to production deviance.[65]

62. See Pavlo, Jr., Walter and Neil Weinberg, Stolen Without a Gun: Confessions from Inside History's Biggest Accounting Fraud—The Collapse of MCI Worldcom (Tampa, FL: Etika Books Ltd, 2007).
63. S. Ramamoorti, D. Morrison, J. W. Koletar, and K. R. Pope, The A.B.C.'s of Behavioral Forensics: Applying Psychology to Financial Fraud Prevention and Detection (Hoboken, NJ: John Wiley & Sons, 2013).
64. Richard C. Hollinger and John P. Clark, Theft by Employees (Lexington, KY: Lexington Books, 1983), 6.
65. Hollinger and Clark, p. 57.

Employee Deviance

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

TABLE 2-2 COMBINED PHASE I AND PHASE II PRODUCTION-DEVIANCE ITEMS AND PERCENTAGE OF REPORTED INVOLVEMENT, BY SECTOR

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

Items	Involvement				
	Almost daily	About once a week	Four to twelve times a year	One to three times a year	Total
Retail Sector (N = 3, 567)					
Take a long lunch or break without approval	6.9	13.3	15.5	20.3	56.0
Come to work late or leave early	0.9	3.4	10.8	17.2	32.3
Use sick leave when not sick	0.1	0.1	3.5	13.4	17.1
Do slow or sloppy work	0.3	1.5	4.1	9.8	15.7
Work under the influence of alcohol or drugs	0.5	0.8	1.6	4.6	7.5
Total involved in production deviance					65.4
Hospital Sector (N = 4, 111)					
Take a long lunch or break without approval	8.5	13.5	17.4	17.8	57.2
Come to work late or leave early	1.0	3.5	9.6	14.9	29.0
Use sick leave when not sick	0.0	0.2	5.7	26.9	32.8
Do slow or sloppy work	0.2	0.8	4.1	5.9	11.0
Work under the influence of alcohol or drugs	0.1	0.3	0.6	2.2	3.2
Total involved in production deviance					69.2
Manufacturing Sector (N = 1, 497)					
Take a long lunch or break without approval	18	23.5	22.0	8.5	72.0
Come to work late or leave early	1.9	9.0	19.4	13.8	44.1
Use sick leave when not sick	0.0	0.2	9.6	28.6	38.4
Do slow or sloppy work	0.5	1.3	5.7	5.0	12.5
Work under the influence of alcohol or drugs	1.1	1.3	3.1	7.3	12.8
Total involved in production deviance					82.2

Job Satisfaction and Deviance

The research of Hollinger and Clark strongly suggests that employees who are dissatisfied with their jobs—across all age groups, but especially younger workers—are the most likely to seek redress through counterproductive or illegal behavior in order to right the perceived inequity. Other writers, notably anthropologist Gerald Mars and researcher David Altheide, have commented on this connection. Mars observed that among both hotel dining room employees and dock workers it was believed that pilferage was not theft, but was "seen as a morally justified addition to wages; indeed, as an entitlement due from exploiting employers."[66] Altheide also documented that theft is often perceived by employees as a "way of getting back at the boss or supervisor."[67] Jason Ditton documented a pattern in U.S. industries called "wages in kind," in which employees "situated in structurally disadvantaged parts [of the organization] receive large segments of their wages invisibly."[68]

Organizational Controls and Deviance

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

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

Hollinger and Clark interviewed numerous employees in an attempt to determine their attitudes toward control. With respect to policy, they concluded, "the issue of theft by employees is a sensitive one in organizations and must be handled with some discretion. A concern for theft must be expressed without creating an atmosphere of distrust and paranoia. If an organization places too much stress on the topic, honest employees may feel unfairly suspected, resulting in lowered morale and higher turnover."[69]

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

---

66. Ibid., 86.
67. Ibid.
68. Ibid.
69. Ibid., 106.

Hollinger and Clark concluded that formal organizational controls provide both good and bad news. "The good news is that employee theft does seem to be susceptible to control efforts … . Our data also indicate, however, that the impact of organizational controls is neither uniform nor very strong. In sum, formal organizational controls do negatively influence theft prevalence, but these effects must be understood in combination with the other factors influencing this phenomenon."[70]

Employee Perception of Control

The researchers also examined the perception—not necessarily the reality—of employees believing they would be caught if they committed theft. "We find that perceived certainty of detection is inversely related to employee theft for respondents in all three industry sectors—that is, the stronger the perception that theft would be detected, the less the likelihood that the employee would engage in deviant behavior."[71]

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

Control in the workplace, according to Hollinger and Clark, consists of both formal and informal social controls. Formal controls can be described as external pressures that are applied through both positive and negative sanctions; informal controls consist of the internalization by the employee of the group norms of the organization. These researchers, along with a host of others, have concluded that—as a general proposition—informal social controls provide the best deterrent. "These data clearly indicate that the loss of respect among one's acquaintances was the single most effective variable in predicting future deviant involvement." Furthermore, "in general, the probability of suffering informal sanction is far more important than fear of formal sanctions in deterring deviant activity."[72] Again, this supports the notion that the greatest deterrent to the fraudster is the idea that he will be caught, not the threat of punishment by his employer.

Other Hollinger and Clark Conclusions

Hollinger and Clark reached several other conclusions based on their work. First, they found that "substantially increasing the internal security presence does not seem to be appropriate, given the prevalence of the problem. In fact, doing so may make things worse."[73]

70. Ibid., 117.
71. Ibid., 120.
72. Ibid., 121.
73. Ibid., 144.

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

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

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

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

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

The researchers summed up their observations by saying,

> *perhaps the most important overall policy implication that can be drawn … is that theft and workplace deviance are in large part a reflection of how management at all levels of the organization is perceived by the employee. Specifically, if the employee is permitted to conclude that his or her contribution to the workplace is not appreciated or that the organization does not seem to care about the theft of its property, we expect to find greater involvement. In conclusion, a lowered prevalence of employee theft may be one valuable consequence of a management team that is responsive to the current perceptions and attitudes of its workforce.*[74]

MODULE 4: THE PSYCHOLOGY OF THE FRAUDSTER, A DEEPER LOOK: M.I.C.E., PREDATORS, AND COLLUSION

Consider these headlines and related news stories…

- "Judge Sentences Woman Who Faked Cancer." According to the USA Today, Lori Stilley received nearly $12,000 in donations from more than 300 people in 20 states by pretending to have cancer, scamming relatives, neighbors, and strangers including her 13-year-old daughter and 8-year-old son.[75]

74. Ibid., 146.
75. Natalie DiBasso, USA Today, 2013.

- "Canadian Charged with Fraud After Faking Cancer." Ontario man Christopher Gordon organized a fundraiser and collected $2,900 in donations, alleging terminal brain cancer to friends and family.[76]
- "Woman Accused of Faking Cancer Pleads Guilty." In this case, according to news reports, Ashley Kirilow had a benign lump removed from her breast in 2009 but pretended to have a more serious form of cancer to make her estranged parents feel bad. When word spread through the community, Ms. Kirilow shaved her head and eyebrows and plucked her eyelashes to make it look as if she had been through chemotherapy. She also started a Facebook page call "Change for a Cure," collecting money from donors who believed they were paying for her treatment and giving to charity. The total amount of the fraud appeared to be less than $10,000.[77]
- "Second Ontario Woman Admits to Cancer Fraud."[78]

In these cases, three women and one man are accused of faking cancer. While all involve some monetary gain to the perpetrator, the amounts are relatively small, especially in light of the emotional pain to friends, relatives, and the victims in their communities documented in these news articles.

Consider further the example of Thomas Coughlin, former Wal-Mart Vice Chairman of the board.

When trying to provide an understanding of fraudsters, this example from the Wall Street Journal is a gem (Figure 2-8). Although the article appeared in 2005, the lessons learned are timeless. As outlined by the Wall Street Journal, Thomas Coughlin was accused by Wal-Mart of having the company reimburse him for personal expenditures including alligator boots, a dog pen, and hunting vacations, among other things. Before his alleged fraud came to light, Mr. Coughlin was the vice chairman of Wal-Mart, essentially, the second-in-command at the retail giant.

FIGURE 2-8 A WAL-MART LEGEND'S TRAIL OF DECEIT

FRIDAY, APRIL 8, 2005 · VOL. CCXLV NO. 69 ~ ★★★ $1.00

A Wal-Mart Legend's Trail of Deceit

Mr. Coughlin Told Others Bogus Expenses Hid Plot Against Unions

Retailer Disputes His Claim

By James Bandler And Ann Zimmerman

BENTONVILLE, Ark. - Last November, Thomas M. Coughlin, Wal-Mart Stores Inc.'s vice chairman, approached a lieutenant with an unusual request. He wanted Jared Bowen to approve around $1,000 in expense payments without any receipts. Mr. Bowen, then a 31-year-old vice president, recalls that Mr. Coughlin, briefly mentioned the money had been used for a

Exit Route Thomas Coughlin's career with Wal-Mart

1976: Hired as director of loss prevention.

1982: Named head of human resources.

1999: Named president of the Wal-Mart Stores division.

April 2003: Elected to Wal-Mart's board.

October 2003: Collapses while exercising and is treated for a coronary blockage.

Jan. 24, 2005: Retires as an executive with Wal-Mart.

March 25, 2005: Forced to resign from Wal-Mart's board.

Source: the company

Was it appropriate to ask Wal-Mart to pay for these personal items? As fraud examiners and forensic accountants, we need to be careful about drawing conclusions without evidence. Depending on Mr. Coughlin's terms of employment (contract), Wal-Mart travel and entertainment policies, etc., it is possible that he was entitled to some reimbursement for these expenditures. However, the Wall Street Journal article suggests that the reimbursements were not in compliance with Wal-Mart polices because Mr.

76. The Associated Press, November 19, 2010.
77. CityNews, November 2, 2010.
78. YahooNews Canada, November 9, 2010.

Coughlin used false documentation and fake invoices, so the expenses would qualify. The Wall Street Journal estimates suggest that Mr. Coughlin may have defrauded Wal-Mart by as much as $500,000 over three years.

The twist: in the single year before he resigned in disgrace and was tried in court for his acts, Mr. Coughlin earned approximately $6,000,000. It appears that Mr. Coughlin was willing to sacrifice everything—his income, his employment, and his reputation for an extra $150–$175K per year.

Finally, consider financial statement fraud. As documented by Rezaee and Riley in "Financial Statement Fraud: Prevention and Detection," the authors argued that Phar-Mor committed financial statement fraud, at least in the early periods, so that management could "buy time" to turn the company's fortunes around. SAS No. 99, AU316, offers a variety of nonmonetary motivations for financial reporting fraud, such as meeting analysts' earnings estimates for public companies.

Each of these examples—fake cancer, Mr. Coughlin's actions, and nonfinancial motivations for financial statement fraud—suggests that the fraud triangle provides an incomplete explanation for many frauds. As such, additional models and tools were offered to supplement the psychology of the fraudster: who commits fraud and why.

M.I.C.E

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

Money
Ideology
Coercion
Ego/Entitlement

Money and ego are the two most commonly observed motivations. Enron, WorldCom, Adelphia, Phar-Mor, and ZZZ Best provide good examples of cases in which the convicted perpetrators seemed to be motivated by greed (money) and power (ego/entitlement). Ego and entitlement might offer insights into Mr. Coughlin's actions. Less frequently, individuals may be unwillingly pulled into a fraud scheme (coercion). These lower-level individuals are often used to provide insight and testimony against the ringleaders and, as such, sometimes receive more lenient sentences or no sentence at all. Ideology is probably the least frequent motivation for white-collar crime, but society has seen this occur in the case of terrorist financing. Another ideological explanation might be associated with some tax frauds where persons do not believe in taxation, or they only want to pay what they believe is their fair share (even if that amount defies tax laws and regulation). With ideology, the end justifies the means, and perpetrators steal money to achieve some perceived greater good that furthers their cause. Although the M.I.C.E. heuristic oversimplifies fraudulent motivations, and some motivations fit multiple categories, it is easily remembered and provides investigators with a framework to evaluate motive.

While the fraud triangle was developed to explain fraud perpetrators, the same motivations can be used to understand other financial disputes that are the subject of forensic accounting examinations. For example, consider the contract dispute in which company A claims that company B has not fulfilled its

contractual obligations. Company B clearly recognizes that its personnel “walked off the job” before meeting the contract specifications. Assuming that companies A and B negotiated a fair, arms-length transaction, something must explain the, otherwise, unusual action of company B.

In contractual matters, the alleged wrongdoer clearly has the opportunity to violate the terms of the contract: that company can simply not perform on their end of the contract. Possible pressure- and rationalization-related explanations might include: company B had old equipment, a labor shortage, or a lack of technical expertise to perform under the contract, or they are unable to operate profitably. These circumstances may have created pressure on company B and pushed them to consider not delivering the product to company A.

Assume further that company A and company B have been working together for many years. How does company B rationalize its behavior? Perhaps company B’s management focuses on contractual ambiguities that were resolved unfavorably, from its perspective, and then uses that as a basis for the unfulfilled obligation.

Consider a divorce situation, where the husband thinks that his former spouse is asking for a more generous settlement than he thinks is appropriate. The fact that his wife is asking for a settlement that is unreasonable (in his mind) may create pressure on him to rationalize that he is doing the right thing by hiding assets. Furthermore, he may use the size of the settlement request as rationalization for arguing with her over the children. When money is involved, we may see individuals, companies, or organizations behave in ways that are out of character. In those situations, we may often be able to explain their actions in terms of the fraud triangle: pressure, opportunity, and rationalization.

Predatory versus Situational Fraudsters

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

Notwithstanding the fraud act, the situational fraudster is generally considered to be a law-abiding person, who under normal circumstances would never consider theft, break important laws, or harm others. When discovered, family members, fellow employees, and other persons in the community are often surprised or even shocked by the alleged behavior of the situational perpetrator, because many of these perpetrators are in positions of trust (which creates opportunity), well educated, and have leadership-level employment. The ACFE finds that only about 5% of fraudsters had previously been convicted of a fraud-related offense. Thus, the vast majority of occupational fraudsters have no history of fraud convictions or prior fraud acts.

The fraud triangle most closely aligns with the situational fraudster. The notion of perceived pressure, opportunity, and the development of a rationalization for the crime provides a profile, not only to help understand the typical fraudster but also to help identify meaningful, nonfinancial, sociological, and psychological red flags that can be used as part of the investigatory process to determine who perpetrated the identified occupational fraud or abuse.

On the other hand, what if the person has committed an act of fraud at a prior organization? Franco Frande, former ATF Financial Investigations Chief, often tells the story of ten-year-old Christopher Woods, who was killed by his father for life insurance money. His father strangled and tossed him onto the side of the road near a lake. The father then started a fire in his home, but when inquiries were made by investigators and the TV news media, he blamed Christopher for accidentally starting the fire. He stated that his son had run away after starting the fire, and Mr. Woods tearfully pleaded to the TV audience for his son's safe return home. At the time, no one except the father knew that Christopher was dead. Mr. Woods set up the crime by talking with others about the "problem" he was having with his son playing with matches. He also placed matches under the couch seat cushion where Christopher's mother would discover them during routine cleaning. The fire allowed the father to collect additional insurance proceeds related to the home structure and contents. All of this was done to repay his most recent former employer for a fraud that Mr. Woods had been perpetrating, so that the employer wouldn't press criminal charges against him.

Mr. Woods' employer had agreed not to file charges against him or make any public disclosures of the fraud incident, provided that Mr. Woods reimbursed the company for the missing funds. What the employer did not know is that he was fraud victim #4; Mr. Woods had perpetrated fraud on three of his former employers. In the prior three incidents, upon discovery, the previous employers chose not to press charges and instead had quietly terminated Mr. Woods. It's possible that Christopher Woods might be alive today if any of the prior employers had prosecuted Mr. Woods. The choice made by each of his former employers allowed him to quietly move on to his next victim.

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

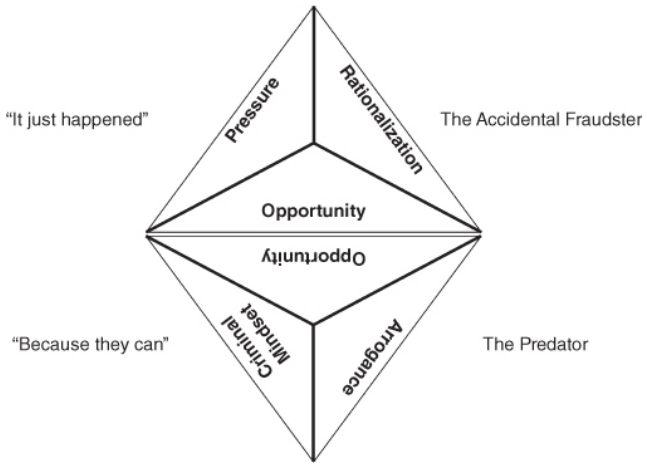
Beyond the predator-type person, often a repeat offender, who seeks to deliberately defraud organizations with seemingly little remorse, we also find individuals and organizations that have operational modus operandi, where a complex fraud or financial crime is inherently part of their goals and objectives. Organizational crimes occur when public and private companies, nonprofits, and government entities, otherwise legitimate and law-abiding organizations are involved in a pattern of criminal activity. Corporate violations include administrative violations that involve noncompliance with agency, regulatory, and legal requirements. In other cases, organizations are deliberately established with at least some nefarious purposes in mind. We often think about organized crimes, drug trafficking, and terrorist financing for the more complex frauds and financial crimes. Organized criminal activities frequently involve many individuals, organizations, shell companies, and cross-jurisdictional borders. Some of the crimes that are

typically observed include conspiracy and RICO (Racketeer Influenced and Corrupt Organizations) Act violations, money laundering, and mail and wire fraud. With terrorist financing, illegal acts derived from the USA Patriot Act come into play.

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

With regard to the fraud triangle and predators, pressure and rationalization play little or no role because the predator needs only opportunity. Instead, arrogance and a criminal mindset replace the original fraud triangle's antecedents of pressure and rationalization and we are left with the elements as they pertain to the predator. See the New fraud diamond in Figure 2-9.

FIGURE 2-9 NEW FRAUD DIAMOND EMERGES WITH A COMMON ELEMENT



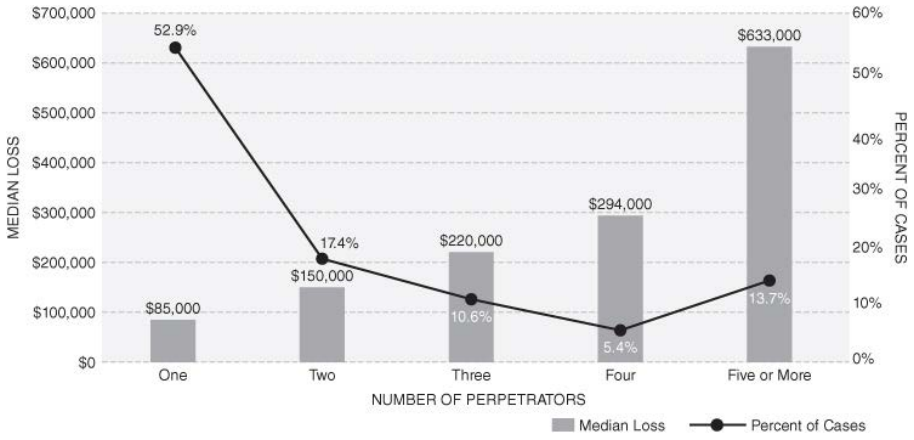
Predators may be individuals or organizations. Some organizations—drug traffickers, organized criminals, terrorist financers—are deliberately established for a nefarious purpose and use complex frauds and financial crimes, such as money laundering, to conceal their criminal activity. These activities often involve many individuals, organizations, or shell companies and span multiple jurisdictional boundaries.

Collusion and Collusive Groups

In 2005, the AICPA identified collusion, along with management override, as the Achilles Heel of antifraud efforts. The ACFE's 2016 Report to the Nations and the 2010 COSO report by Beasley et al. on financial statement fraud, both found that collusive fraud occurs with high frequency.

As noted in Figure 2-10 from the ACFE 2016 Report, nearly half of the cases involved multiple perpetrators colluding with one another to commit fraud. The second important finding is that the greater the number of fraudsters involved, the higher the losses to the victim company.

FIGURE 2-10 THE IMPACT OF COLLUSION



By way of explanation, the ACFE suggests that one possible reason for the increase in losses associated with multiple perpetrators is that many antifraud controls work on the basis of separation of duties and independent checks. When multiple fraudsters work together, they are able to undermine the independent verification of transactions or other mechanisms designed to uncover fraud. Another explanation for the larger losses in schemes with multiple perpetrators could simply be that with more fraudsters involved, the perpetrators needed to steal more because their proceeds needed to be split among more individuals. In other words, with more perpetrators expecting a payout, the conspirators needed to steal more to satisfy everyone involved in the crime.

With regard to the fraud triangle, Bishop et al. suggest the following:

- Pressure, motive or incentive, generally, is experienced by the leader (instigator) or recruiter who lacks opportunity.
- Opportunity is enhanced in the collusive group setting, particularly with regard to capability and concealment.
- Rationalization is more easily accomplished in a collusive environment where, at least, some of the blame can be emotionally/psychologically shifted to others.

Researchers have recently started to give the issue of collusion more attention. Free and Murphy (2015) find that three categories of social ties emerged from interviews with 37 convicted fraudulent co-offenders. The first category—individual-serving functional bonds—was identified in 21 of the 37 participants (57%). The primary beneficiary of the fraud was an individual, and the co-offending groups were formed to maximize their opportunity (access) to commit fraud. In most cases (17 of 21), an instigator led the fraud by recruiting followers to create the necessary means to commit and conceal the fraud act. In the remaining four cases, the collusive fraud participants were members of pre-existing groups that collaborated to identify or respond to opportunities. The co-offending groups were bound by trust relationships based on "mutual dependence and negative reciprocity."[79]

As noted above, collusive frauds may be initiated by a leader, but that leader lacks some aspect of opportunity. Opportunity is the perception that (1) a control weakness is present and, importantly, (2) the likelihood of being caught is remote.

In a collusive environment, co-offenders are likely purposefully selected for their skill set or access, especially those that create or facilitate opportunity whether to commit or conceal the fraud. If an instigator does not possess the required resources to commit the crime, and he can find or recruit someone who does, collusive fraud results. Wolfe and Hermanson suggest modifying the fraud triangle to incorporate capability—the fraudster's capability to take advantage of an opportunity to commit and conceal fraud using his personal traits and abilities. In their framework, traits and abilities include intelligence, ego, position or function in the organization, knowledge of internal control weaknesses, authorized access, confidence, and ability to handle stress associated with deception. In the context of Wolfe and Hermanson, co-offenders may provide the needed capabilities across the group. Free and Murphy suggest that for many fraudsters the co-offending network "offers a structure that provides, or enhances, opportunities for fraud."

Bishop, Hermanson, and Riley find a number of key differences between collusive frauds and solo frauds.[80]

With respect to leader characteristics:

- Collusive fraudsters are younger
- More likely to be male
- Less likely to have college degrees than solo offenders
- Less likely to exhibit addiction problems or excessive control issues
- More likely to have unusually close associations with vendors or customers and to have a wheeler-dealer attitude

79. C. P. Free and P. R. Murphy, "The Ties That Bind: The Decision to Co-offend in Fraud," Contemporary Accounting Research 32, no. 1 (2015): 18–54.
80. C. Bishop, D. Hermanson, and R. Riley Collusion: Leader, Fraud and Organizational Attributes, ed., C. Bailey (FL: Journal of Forensic Accounting Research, 2017).

Regarding incident characteristics, collusive frauds are as follows:

- More likely to involve financial statement fraud
- Larger in terms of dollar amount
- Shorter duration
- More likely to be discovered by tip or complaint, internal audit, law enforcement, or by accident
- Less likely in U.S. organizations than in non-U.S. organizations

The results highlight the importance of considering a potential fraudster's ability to build a fraud team to commit large, intense frauds. The findings suggest that a typical profile for such a team leader is a younger male with close ties to customers or vendors and a wheeler-dealer attitude. This profile contrasts with the typical notion of the white-collar criminal as older and possibly facing personal problems, such as financial problems, addiction, or demonstrating control issues.

For some time, the fraud triangle has been recognized for best fitting the situational fraudster acting alone. The recognition that fraudsters often operate in groups allows for a more informed approach to detection and investigation as well as the ability to enhance fraud deterrence and prevention efforts. Importantly, collusion creates incremental opportunity, and therefore, supervisory and managerial review becomes increasingly important.

MODULE 5: THE FRAUD TRIANGLE IN COURT AND THE META-MODEL

John Gill, ACFE Vice President of Education, wrote an article for Fraud Magazine[81] in which he examined several U.S. court opinions that refer to the fraud triangle. He stated that he was initially surprised to learn that the cases denied the admission of expert testimony about the triangle because they deemed it "unreliable." The following is Gill's summary of three cases:

- The first case was Haupt v. Heaps, 131 P.3d 252 (2005). The dispute involved a developer, who claimed the CEO of the company that hired him as a contractor defrauded him into relinquishing stock back to the company at an artificially low price because of representations made about the imminent financial collapse of the company. The developer lost at trial. One of his asserted points on appeal was that the trial court improperly excluded the testimony of his expert about the fraud triangle. The developer wanted to introduce testimony that the conduct of the defendant was consistent with the three elements of the fraud triangle. The appellate court agreed with the trial court's conclusion that "[r]esearch into case law … failed to locate even a single case in which the 'fraud triangles' [sic] theory has been adopted as a reliable scientific method in any court of law." The evidence was rejected for that reason and because the court felt the testimony was more prejudicial than probative.

81. "The Fraud Triangle on Trial," Fraud Magazine, September/October 2017.

- The second case Gill reviewed was Travis v. State Farm Fire & Cas. Co., 2005 U.S. Dist. LEXIS 49957. Linda Travis sued State Farm Insurance because it denied her claim for losses she sustained in a fire. State Farm claimed she committed fraud by concealing or misrepresenting material facts regarding her claim. State Farm sought to admit the testimony of an expert that her financial position created "a significant incentive or pressure for her to commit fraud, and that she possesses 'attitudes, characteristics, or ethical values that could allow an individual to rationalize committing a fraudulent act.'" The trial judge excluded the testimony. In his opinion, the judge notes that applying the triangle relies more on professional judgment than "hard science." The judge writes, "it is also unlikely that there is a known rate of error or specific objective controls associated with the application of the fraud triangle. The court stated: "The fact that the fraud triangle appears in the Fraud Examiner's Manual and in SAS 99 indicates that the concept is widely accepted among professional fraud examiners and is relevant to various types of fraud detection. But that does not mean that it is, or was ever, intended to be anything more than a general conceptual underpinning of fraud detection theory… . The flexibility of the triangle and its adaptability to different contexts suggest that it might have been intended to be more of a theoretical concept than a set of measurable standards or a specific, practical methodology."
- In the third case, Gill highlights the problem of allowing testimony that speculates on someone's mental state. The most recent case, Kremsky v. Kremsky, 2017 U.S. Dist. LEXIS 22794, discusses this problem. The case involved an uncle who sued his nephew and claimed the nephew breached fiduciary duties and committed fraud against the uncle. The uncle sought to admit the testimony of a financial expert. The expert, in addition to his testimony about financial books and records, was slated to testify that the nephew met the elements of the fraud triangle and, therefore, had a motive to commit the fraud. The court denied the request. In its opinion, the court notes that an expert witness can't speak to the subjective belief of a party because it would basically amount to unsupported speculation. The court writes, "Uncle does not cite a case where an expert touting this 'fraud triangle' has been permitted to opine as to motive." It further stated, "An expert cannot speak as to the subjective belief of a [party]."

Even though Gill only found a limited number of cases involving the fraud triangle, he offers some general observations.

- First, if you want to talk about the fraud triangle in court, don't call it a theory.
- Second, can you use the elements of the fraud triangle to show someone has the propensity (or not) to commit fraud? Probably not. It's a tool that we can use to better understand rationalizations, opportunities, and the reasons why people commit fraud. It was never designed as a litmus test to determine whether a particular individual is, or isn't, a fraudster.

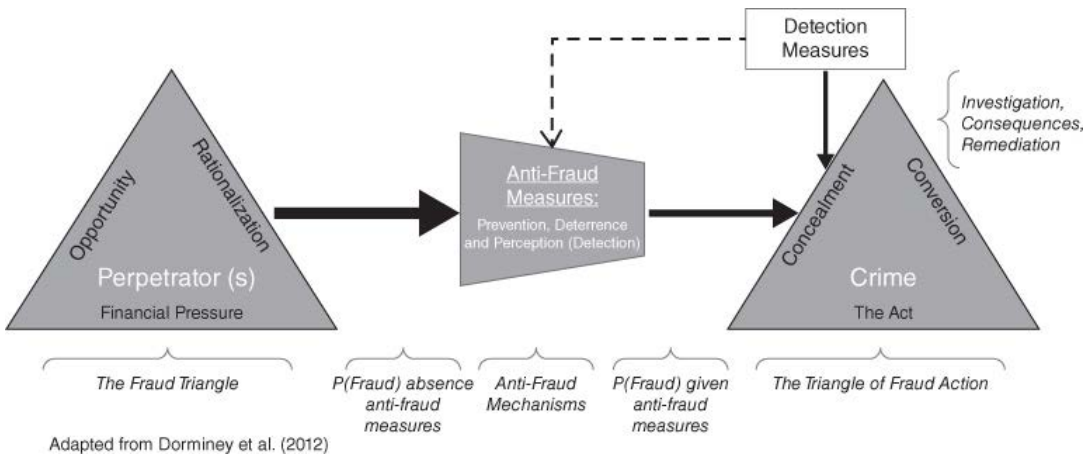
- Expert witnesses can't use the fraud triangle (or anything else that I'm aware of) to speculate about the mental state of a person accused of fraud. Courts are very wary of "state-of-mind" evidence in all cases. Often, that's a matter that the jury will be asked to determine.

The Meta-Model

If the fraud triangle, one of the most recognized tools in the antifraud profession, can't be used as a basis for offering testimony, what's a forensic accountant or fraud examiner to do? A corollary to the fraud triangle is the lesser known triangle of fraud action, sometimes referred to as the elements of fraud.[82] While the fraud triangle identifies the conditions under which fraud may occur, the triangle of fraud action describes the actions an individual must perform to perpetrate the fraud. The triangle of fraud action is positioned in relation to the fraud triangle in the following meta-model.

The model provides a framework for examining issues associated with fraud and financially motivated crime. On the left-hand side, the model identifies fraud as perceived by the (potential) fraud perpetrator (Figure 2-11). The fraud triangle[83] characterizes the perpetrator as a decision-maker, one who must examine the possibilities of fraud to determine if a fraudulent act can be successful in both (1) execution and (2) concealment. On the right-hand side, captured in the triangle of fraud action, the model focuses on the specific elements of the fraud or financial crime[84]: the act, the concealment, and the conversion of benefits that accrue to the perpetrator. Between the perpetrator (fraud triangle) and the criminal act (triangle of fraud action) are interventions, antifraud measures such as internal controls, corporate governance, and laws and regulations designed to reduce the incidence and impact of fraud. These interventions have been characterized as prevention, deterrence, and the perception of detection. Antifraud measures, in general, are outside the direct control of the perpetrator, but influence the would-be fraudster's assessment of the probability of success in terms of the fraudulent act, concealment, and conversion.

FIGURE 2-11 A META-MODEL OF FRAUD AND WHITE-COLLAR CRIME



82. W. Steve Albrecht, Conan C. Albrecht, and Chad O. Albrecht, Fraud Examination (2006); M.-J. Kranacher, R. Riley, and J. Wells, Forensic Accounting and Fraud Examination (Hoboken, NJ: John Wiley & Sons, 2011).
83. D. R. Cressey, Other People's Money (Montclair, NJ: Patterson Smith, 1953); W. Steve Albrecht, "Fraud in Government Entities," Government Finance Review (December 1991): 27–30.
84. W. Steve Albrecht, et al., Fraud Examination, 4th ed. (Mason, OH: South-Western Cengage Learning, 2012).

The three components of the triangle of fraud action are the act, concealment, and conversion. *The act* represents the execution and methodology of the fraud. *Concealment* represents disguising or hiding the fraud; fraud can be concealed by, for example, creating false journal entries, falsifying bank reconciliations, or destroying files, etc. *Conversion* is the process of turning ill-gotten gains into something of value to the perpetrator—conversion is completed in such a way that the benefit appears to come from legitimate sources such as laundered money, loan proceeds, an inheritance, lottery winnings.

The triangle of fraud action represents specific actions that can be documented in the form of evidence. Further, antifraud professionals may develop measures, controls, or structure in audits to illuminate evidence consistent with the act, the concealment, or the conversion. Such evidence can be used in detection and examination of potential fraud acts, and knowledge of their existence may act as a deterrent.

The triangle of fraud action is valuable to the investigator where proof of intent is required. While the fraud triangle points investigators to why people might commit fraud, the evidentiary trail might be weak or nonexistent, and most forensic accountants and fraud examiners do not have the expertise to be able to comment on one's inner state of mind associated with pressure or rationalization. As suggested by Gill, financial pressure and rationalization are not directly observable. Rather, the antifraud professional needs an evidenced-based approach to conduct examinations. The triangle of fraud action is helpful because each element can be directly observed and documented.

The triangle of fraud action is a model for detecting fraud and developing prosecutorial evidence. Evidence of the act, concealment, and conversion can be collected and presented during adjudication. When considered in concert, the elements of fraud make it difficult for the perpetrator to argue that the act was accidental or to deny their role in the act. Evidence of concealment, in particular, provides a compelling argument that the act was intentional.

CHAPTER 2: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

1.	**The authors cite all of the following as reasons why people follow laws <u>except</u>:** **A.** social conditioning/parental upbringing **B.** fear of punishment **C.** to act in a just and moral manner according to society's standards **D.** desire for rewards
2.	**Which of the following terms was coined by Edwin H. Sutherland in 1939 and captures the essence of the type of perpetrator that one finds at the heart of occupational fraud and abuse:** **A.** organizational crime **B.** fiduciary crime **C.** organized crime **D.** white-collar crime
3.	***Black's Law Dictionary* defines which of the following as a private or civil wrong or injury, other than breach of contract, for which the law will provide a remedy in the form of an action for damages:** **A.** organizational crime **B.** occupational fraud **C.** tort **D.** white-collar crime

4.	**Which of the following is correct regarding the typical fraud perpetrator:** **A.** the typical fraud perpetrator is generally not respected within their community **B.** the typical fraud perpetrator generally has been with the victim organization for less than a year **C.** the typical fraud perpetrator does not have a criminal background **D.** the typical fraud perpetrator usually does not have a college degree
5.	**Donald R. Cressey identified six categories of non-shareable financial pressures that prompted embezzlers to act. These included violation of ascribed obligations, business reversals, physical isolation, status gaining, employer-employee relationships, and _____.** **A.** financial greed **B.** problems resulting from personal failure **C.** depression or other mental health issues **D.** amoral value system
6.	**According to the authors, fraud deterrence begins in which of the following:** **A.** in the existence of sound internal controls **B.** in the organizational mission and values **C.** in the employee's mind **D.** in the beliefs of the culture at large
7.	**Which of the following is correct regarding independent businessmen, as identified in Donald R. Cressey's study:** **A.** the independent businessmen almost universally felt their illegal actions were predicated by an "unusual situation" **B.** Cressey defined independent businessmen as individuals who converted their employer's funds, or funds belonging to their employer's clients, by taking relatively small amounts over a period of time **C.** independent businessmen are defined by Cressey as people who take the money and run **D.** Cressey found that the non-shareable problems for independent businessmen usually resulted from physical isolation

8.	**While Dr. Steve Albrecht's research findings on fraud perpetrator characteristics were very similar to the non-shareable problems and rationalizations identified by Cressey, Albrecht introduced _____ into the actions of the fraudsters.** **A.** the role of compensation **B.** the role of the organization **C.** the role of social isolation **D.** the role of an unfair performance evaluation system
9.	**In a 2004 *CPA Journal* article, Wolfe and Hermanson argue that the fraud triangle could be enhanced to improve both fraud prevention and detection by considering which of the following elements:** **A.** internal control environment **B.** Myers-Briggs personality types **C.** the role of arrogance **D.** individual capability
10.	**The triangle of fraud action is sometimes referred to as which of the following:** **A.** the elements of fraud **B.** the fraud triangle **C.** the fraud diamond **D.** Crowe's Fraud Pentagon

THIS PAGE INTENTIONALLY
LEFT BLANK.

CHAPTER 2: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

1.	**A.** **CORRECT**. According to the authors, people follow laws to avoid punishment, to follow social norms, or to earn rewards. **B.** Incorrect. The fear of punishment is one reason cited by the authors to explain why people follow laws. **C.** Incorrect. People follow laws for a number of reasons, including to act in a just and moral manner according to society's standards. **D.** Incorrect. A desire for rewards is one of the reasons why people follow laws according to the author. *(See page 57 of the course material.)*
2.	**A.** Incorrect. Organizational crime occurs when entities, companies, corporations, not-for-profits, nonprofits, and government bodies, otherwise legitimate and law-abiding organizations, are involved in a criminal offense. **B.** Incorrect. The term "fiduciary crime" was not coined by Edwin H. Sutherland in 1939. **C.** Incorrect. Some of the crimes typically associated with organized crime include money laundering, mail and wire fraud, conspiracy, and racketeering. Organized crime is typically not at the heart of occupational fraud and abuse. **D.** **CORRECT**. In 1939, Edwin H. Sutherland defined white-collar crime as "crime in the upper, white-collar class, which is composed of respectable, or at least respected, business and professional men." The term white-collar crime captures the essence of the type of perpetrator that one finds at the heart of occupational fraud and abuse. *(See page 58 of the course material.)*
3.	**A.** Incorrect. Organizational crime involves criminal offenses, not civil wrongs or injuries. **B.** Incorrect. Occupational fraud and abuse is defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. **C.** **CORRECT**. *Black's Law Dictionary* defines "tort" as a private or civil wrong or injury, other than breach of contract, for which the law will provide a remedy in the form of an action for damages. When a tort is committed, the party who was injured is entitled to collect compensation for damages from the wrongdoer for that private wrong. **D.** Incorrect. The definition of white-collar crime typically involves financial and economic crimes. *(See pages 59 to 60 of the course material.)*

4.	**A.** Incorrect. It is not uncommon for a fraud perpetrator to be a respected member of the community, attend church services, and have a family. **B.** Incorrect. In over 90 percent of the fraud cases examined by the ACFE, the perpetrator had been with the victim organization for more than one year. **C. CORRECT**. Fraudsters typically do not have a criminal background. **D.** Incorrect. The typical fraud perpetrator is well educated. *(See page 61 of the course material.)*
5.	**A.** Incorrect. Financial greed was not one of the six categories identified by Cressey. **B. CORRECT**. Cressey's six categories of non-shareable financial pressures include violation of ascribed obligations, problems resulting from personal failure, business reversals, physical isolation, status gaining, and employer-employee relationships. **C.** Incorrect. The six categories of non-shareable financial pressures identified by Cressey do not include depression or other mental health issues. **D.** Incorrect. Amoral value systems was not one of the six categories as defined by Cressey. *(See page 64 of the course material.)*
6.	**A.** Incorrect. Internal controls can have a deterrent effect only when the employee perceives that such a control exists in both design and operation, and the controls are likely to uncover the potential fraud. **B.** Incorrect. The authors do not believe that fraud deterrence begins with the organizational mission and values. **C. CORRECT**. The authors state that fraud deterrence begins in the employee's mind. Employees who perceive that they will be caught are less likely to engage in fraudulent conduct. **D.** Incorrect. The culture at large is not the key to deterring employee fraud. *(See page 69 of the course material.)*
7.	**A. CORRECT**. The independent businessmen almost universally felt their illegal actions were predicated by an "unusual situation," which Cressey perceived to be in reality a non-shareable financial problem. **B.** Incorrect. Cressey defined long-term violators as individuals who converted their employer's funds, or funds belonging to their employer's clients, by taking relatively small amounts over a period of time. **C.** Incorrect. Absconders, not independent businessmen, are defined as people who take the money and run. **D.** Incorrect. Cressey found that the non-shareable problems for absconders usually resulted from physical isolation. *(See page 71 of the course material.)*

8.	**A.** Incorrect. Dr. Albrecht did not introduce the role of compensation into the actions of the fraudsters. **B.** **CORRECT**. Dr. Albrecht explicitly introduced the role of the organization into the actions of the fraudsters. This role was inherent in Cressey's efforts, but Albrecht brought these issues to the forefront. **C.** Incorrect. The role of social isolation was not introduced into Dr. Albrecht's fraud scale. **D.** Incorrect. Dr. Albrecht did not introduce the role of an unfair performance evaluation system into the actions of the fraudsters. *(See page 78 of the course material.)*
9.	**A.** Incorrect. Wolfe and Hermanson did not argue for the inclusion of the internal control environment as a way of enhancing the fraud triangle. **B.** Incorrect. Wolfe and Hermanson did not believe that the inclusion of Myers-Briggs personality types would enhance the fraud triangle. **C.** Incorrect. The role of arrogance was not discussed in the article authored by Wolfe and Hermanson. **D.** **CORRECT**. In a 2004 *CPA Journal* article, Wolfe and Hermanson argued that the fraud triangle could be enhanced to improve both fraud prevention and detection by considering a fourth element, capability. The authors suggest that capability plays an important role in whether fraud may actually occur. *(See page 80 of the course material.)*
10.	**A.** **CORRECT**. A corollary to the fraud triangle is the lesser-known triangle of fraud action, sometimes referred to as the elements of fraud. **B.** Incorrect. The term fraud triangle is not used interchangeably with the triangle of fraud action. **C.** Incorrect. The fraud diamond has four components, while the triangle of fraud action has only three. **D.** Incorrect. Unlike the triangle of fraud action, Crowe's Fraud Pentagon has five elements. *(See page 95 of the course material.)*

THIS PAGE INTENTIONALLY
LEFT BLANK.

CHAPTER 3: LEGAL, REGULATORY, AND PROFESSIONAL ENVIRONMENT

Chapter Objective

After completing this chapter, you should be able to:

- Identify the characteristics of the civil and criminal justice systems.

According to US Legal.com, a Daubert challenge is a hearing conducted before a judge where the validity and admissibility of expert testimony are challenged by opposing counsel. The expert is required to demonstrate that his/her methodology and reasoning are scientifically valid and can be applied to the facts of the case. The term comes from the 1993 U.S. Supreme Court case, Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), in which the Court articulated a new set of criteria for the admissibility of scientific expert testimony. In its 1999 Kumho Tire v. Carmichael opinion, the Court extended Daubert's general holding to include nonscientific expert testimony as well.[1] An expert who expects to testify in civil or criminal court about his or her work needs to be aware of and prepared for a Daubert challenge.

In a 2017 *Fraud Magazine* article, John D. Gill, ACFE Vice President of Education, penned an article titled: "The Fraud Triangle on Trial." In his article, Gill examined several U.S. court opinions that refer to the fraud triangle and was surprised to find cases where judges denied the admission of expert testimony about the triangle because they deemed it to be "unreliable" scientific theory.[2] The following are excerpts from Gill's summaries of three cases:

- Haupt v. Heaps, 131 P.3d 252 (2005). The appellate court "failed to locate even a single case in which the 'fraud triangles' [sic] theory has been adopted as a reliable scientific method in any court of law." The (fraud triangle) evidence was rejected for that reason and because the court felt the testimony was more prejudicial than probative.
- Travis v. State Farm Fire & Cas. Co., 2005 U.S. Dist. LEXIS 49957. "The trial judge excluded the (fraud triangle) testimony. In his opinion, the judge notes that applying the triangle relies more on professional judgment than "hard science." The judge writes, "it is also unlikely that there is a known rate of error or specific objective controls associated with the application of the fraud triangle." Further, Gill paraphrasing the judge: "expert evidence from fraud examiners is usually related to direct evidence that fraud has occurred or to descriptive evidence that will help the jury understand transactions and how they compare with or deviate from applicable standards."
- Kremsky v. Kremsky, 2017 U.S. Dist. LEXIS 22794. In its opinion, the court notes that an expert witness can't speak to the subjective belief of a party because it would basically

1. https://definitions.uslegal.com/d/daubert-challenge
2. John Gill, "The Fraud Triangle on Trial," Fraud Magazine, September/October 2017.

amount to unsupported speculation. The court writes, “Uncle [Stanton Kremsky] does not cite a case where an expert touting this ‘fraud triangle’ has been permitted to opine as to motive.” It further stated, “An expert cannot speak as to the subjective belief of a [party].”

Both the Daubert challenge and Gill’s cautionary tale are relevant to those professionals who conduct fraud examinations, especially those who give expert testimony in a court of law.

We’ll examine these and other topics associated with the legal, regulatory, and professional environment across several modules. Those modules, along with the learning objectives, include the following:

- Module 1 provides an overview of the criminal and civil justice systems within which forensic accountants and fraud examiners operate. The objective is for the reader to be able to differentiate between the criminal and civil legal systems and to begin to develop an appreciation for the complexities of pursuing legal action.
- Module 2 outlines the legal rights of individuals based on the U.S. Constitution. The goal in this module is for readers to be able to discuss the legal rights of individuals—related to employment, interviews, searches, surveillance, privileges, and standards—under the U.S. justice system.
- Module 3 takes a look at U.S. Constitution Fourth Amendment rights associated with probable cause. The goal here is for the reader to identify the requirements associated with probable cause when collecting evidentiary materials.
- Module 4 reviews the rules of evidence by considering the primary attributes of evidence, particularly those that allow evidentiary materials to be presented in a court of law. The take-away from module 4 will be the reader’s ability to describe the role of evidence and the elements to meet the criteria of what constitutes “evidence.”
- Modules 5 and 6 offer overviews of the criminal (Module 5) and civil (Module 6) justice systems. The learning objective of these modules is for the reader to recognize the legal environment in which he is working and be able to articulate the similarities and differences of each system.
- Module 7 takes an initial dive into basic accounting, including financial statements, offering a survival guide for those with more of a criminal justice, legal, or regulatory background, who have less familiarity with accounting principles. The goal here is to launch readers on a path toward the utilization of accounting data in forensic accounting engagements and fraud examinations.
- Module 8 provides an overview of the key elements of the regulatory system in which financial information is developed, particularly financial statement information. Readers will be able to describe the primary environment in which financial numbers are developed and presented.
- Module 9 provides an introduction to key organizational stakeholders, who oversee the development of accounting information, including responsibility for the internal control environment. The objective is for readers to identify the key players within the environment in which financial and nonfinancial information is generated.

MODULE 1: INTRODUCTION

Fraud may be prosecuted criminally or civilly. Almost any dispute between entities (individuals, businesses, organizations, government entities, etc.) can be prosecuted in civil court. Any time the legal issue at hand involves money, an opportunity arises for forensic accountant involvement. Similarly, any time the legal issue involves claims of fraudulent activity, fraud examiners and forensic accountants can play an important role in investigating and resolving the issue. In either case, the process begins when one or more parties make a claim against another.

In the criminal justice system, a person from the private sector may report a crime. Individuals, families, neighbors, businesses, charities, nonprofits, associations, industry, newspapers, TV, radio, and the Internet are some of the sources where a legal issue may come to light. These same organizations are part of the crime prevention fabric as well. One of the major crime prevention tools is the fear of getting caught. In fact, it is generally accepted that this fear is a greater deterrent than the fear of punishment. Most people think of law enforcement when they consider the legal environment, but other entities often play a part as well, such as public health departments, educational institutions, welfare and social justice organizations, public works departments, and public housing. The watchful eye of those members of the greater community is critical to the success of both the criminal and civil justice systems.

Furthermore, members of the community directly participate in the civil and criminal systems. They report crimes and civil actions; they serve as witnesses, jurors, and other officers of the court. One of the most important aspects of the American and Western judicial systems is the willingness to accept the outcomes of the legal process. Both sides to an issue are committed to their position; that is why they are in the civil or criminal justice system to begin with. Both sides commit considerable time and economic resources to pursuing their goals and positions. Yet despite the battles waged inside our courtrooms everyday—from local magistrates to the U.S. Supreme Court—when the final verdict is announced, generally the participants and society at large accept the outcomes. Another interesting aspect of our legal system is that most people are law-abiding citizens. If desired, many could get away with relatively minor crimes periodically and possibly even major crimes. But the vast majority of Americans and citizens of Western society agree to “play by the rules” because they believe that while some legal outcomes may be less than perfect, generally the system works, and our society is better off if everyone follows the rules.

Criminal cases are brought forth by the government through the criminal justice system. The government apprehends, tries, and punishes convicted individuals for criminal behavior. The foundation for this approach is that criminal behavior is considered a “crime against the state” as well as against individual victims. If the victims or others with a stake in the outcome are not satisfied with the results of the criminal justice system, they may pursue their claim through the civil justice system. Cases may also be pursued criminally and civilly at the same time. The primary difference between the criminal and civil systems is the potential remedy for the victim: the primary allowable remedy in the civil process is monetary damages, whereas the criminal justice system may result in fines, community service, probation, incarceration, censure, and even capital punishment. In the United States, however, there are no fraud crimes that carry the death penalty.

Most criminal cases never end up in the criminal justice system. This is known as the *criminal justice funnel*. The funnel analogy is derived from the fact that while many crimes go in the top at the wide part of the funnel, few come out at the bottom in the form of convictions and incarcerations. In fact,

most crimes are not discovered, and many that are discovered are not reported. Reports from victims, other citizens, law enforcement personnel, informants, investigators, and intelligence activities may result in the observation of criminal behavior. Nevertheless, there is a tremendous amount of discretion inherent in the American and Western criminal justice systems. Just because a criminal or civil offense is observed does not mean that it will be reported or pursued. Even if an actual crime in observed, before the criminal justice system can pursue the matter, the suspect must be identified and apprehended.

In addition to the criminal and civil justice systems, regulatory agencies also play an important role in monitoring illegal activities and pursuing those responsible. The U.S. Securities and Exchange Commission (SEC) regulates securities exchanges, securities brokers and dealers, investment advisors, and mutual funds. The SEC may bring civil or administrative actions to seek remedies for violations of law or the Commission's rules, and works closely with law enforcement agencies to bring criminal cases, when appropriate. The Public Company Accounting Oversight Board (PCAOB) was created by the Sarbanes–Oxley Act of 2002 to oversee the auditing firms of public companies. Its main purpose is to protect investors by promoting fair and informative financial reports. The board members are appointed by the SEC.

Governmental agencies regulate activities involving utilities, communications, and air transportation, to name a few. Taxpayer money provides the resources needed for government operations, and the Internal Revenue Service (IRS) is charged with collecting those taxes and enforcing the tax laws under the Internal Revenue Code. The IRS can also bring actions against taxpayers in civil and/or criminal court for noncompliance with the tax code.

MODULE 2: THE RIGHTS OF INDIVIDUALS

In this section, we discuss the right of the individual, particularly those persons accused of or potentially accused of committing a crime. Paul Cassell suggests that the "criminal justice system is shifting, at least to some modest degree, from a two-sided, "State v. Defendant" model to a three-sided model in which crime victims are free to enforce their own rights." Mr. Cassell suggests that "this change is long overdue, as crime victims have their own independent concerns in the process that ought to be recognized."[3]

In defense of his position, the author cites Paroline v. U.S. & Amy. Amy's attorney submitted a detailed restitution request for Amy, a victim of child pornography crimes. The request was supported by a forensic psychological evaluation and econometric projection. Amy sought restitution in the amount of $3,367,854 for lifetime psychological counseling costs and lost income. The government supported Amy's request. Following two evidentiary hearings, the district court denied Amy, finding that it was not possible to identify precisely what part of those losses was specifically attributable to the defendant, Paroline, as opposed to thousands of other criminals who were victimizing Amy. However, Amy sought review in the U.S. Court of Appeals for the Fifth Circuit that remanded the case to the district court for an award of full restitution.

When persons consider individual rights, most of those rights are associated with formal actions in the criminal and civil justice environments. Generally, individuals have far fewer rights as employees than as

3. P. Cassell, "Why Crime Victims Need Their Own Voice in the Criminal Justice Process," The Washington Post, 2014.

citizens. Most fundamentally, individual rights are grounded in four amendments to the U.S. Constitution associated with due process:

- The Fourth Amendment prohibits unreasonable searches and seizures
- The Fifth Amendment provides that a person cannot be compelled to provide incriminating information against himself in a criminal case
- The Sixth Amendment provides that an individual has the right to an attorney to defend himself and the right to confront witnesses against him
- The Fourteenth Amendment entitles a person to due process of law and equal protections under the law

As employees, individuals have an obligation to cooperate with their employer or be subject to dismissal. Other rights may be granted to employees as set out in employment contracts and collective bargaining agreements. Federal law and many state laws protect employees who report improper or illegal acts of their employer. Such laws normally protect the employee against overt retaliatory or punitive action by the employer, although as a practical matter, subtle forms of discrimination are hard to combat.

Interviews

An employee's or individual suspect's right to avoid self-incrimination applies to employers, investigators, and law enforcement personnel. An employee who refuses to cooperate during an interview while invoking the Fifth Amendment, however, may be subject to employment termination. In custodial settings by law enforcement, and in those settings where the suspected perpetrator has been taken into custody and denied freedom presumably against their will, federal law may require that a Miranda warning be read to the suspect. Because employers do not have the right to place employees in a custodial setting, an employee has limited Fifth Amendment rights. Public employers, however, are held to a higher standard, and their employees can invoke their Fifth Amendment protections without fear of reprisal.

The Miranda warnings consist of the following:

- The interviewee has a right to remain silent
- The interviewee's answers may be used against him
- The interviewee has a right to an attorney
- If the interviewee cannot afford an attorney, one will be provided at no cost
- The interviewee can decide at any time to invoke these rights

A second issue arises regarding employee interviews under the Sixth Amendment, and whether the employee has a right to legal counsel. As long as a nonpublic entity is conducting the interview, an employee does not have the right to have a lawyer present, nor does the employee have the right to consult his or her attorney prior to an interview. The employee maintains the right to consult an attorney if he or she requests one, however. With regard to the Fourteenth Amendment, private employers do

not have to offer employees due process of law. In contrast, law enforcement and public entities have such an obligation under this amendment. For example, federal employees may have a right of notice of charges and may have the right to rebut any charges put forward.

The Fourth, Fifth, Sixth, and Fourteenth Amendments are all federal rights. In many cases, other federal and state laws regulate the rights of individuals. While such statutes and laws cannot have the impact of limiting federal constitutional rights, those rights may be expanded. Some of the common means by which federal rights are altered are via employment contracts, collective bargaining and other union agreements, various nondiscrimination statutes, and the Fair Labor Standards Act.

In addition, individuals may be entitled to various common law protections with regard to interviews. These include:[4]

- Minimization of invasion of the employee's privacy
- Limitations on interview content to employee job duties and responsibilities
- Limitations on public disclosure of the employee's private facts
- Limitations on intentional infliction of emotional distress on the employee
- Limitations on defamation—unfounded facts and accusations made by the interviewer
- A duty to deal fairly and in good faith
- No false imprisonment—false imprisonment may be inferred based on the size, nature, and lighting of the room, the amount of force involved, any violent behavior by the interviewer, limitations of ability to leave the interview room, and number of persons involved

While interviews may be conducted subject to the rules, laws, and other issues cited above, confessions resulting from interviews and interrogations create additional challenges. First, in order for confessions to be valid, they must be deemed voluntary. Confessions cannot be obtained as a result of coercion or under threats of violence. Furthermore, promises by the interviewer of leniency can nullify a confession. Promises to recommend a lighter sentence or to report cooperation by the subject, however, are generally not thought to be coercive in nature. Courts have weighed the "substantial risk" of a false confession when determining whether a confession has been coerced.[5] Small deceptions are generally permitted and will not risk the validity of the confession. With regard to deceptions, a simple rule is to ask yourself, "Is what I am about to do, or say, apt to make an innocent person confess?" If the answer is "yes," the statement should not be made.[6]

Searches

The Fourth Amendment protects individuals against unreasonable searches and seizures. First, unreasonable searches and seizures are forbidden. All warrants for searches and arrest must be

4. Section 2.309, Fraud Examiner's Manual.
5. Fred E. Inbau et al., Criminal Interrogation and Confessions, 4th ed. (Gaithersburg, MD: Aspen Publishers Inc., 2001), 482.
6. Ibid., 486.

supported by probable cause, and all warrants must be reasonably specific as to persons, places, and things.[7] The overriding rule is that individuals have a "reasonable expectation of privacy." Whether a search or surveillance is reasonable is generally based on the totality of the circumstances. A search warrant based on probable cause has the effect of being reasonable. A major exception to the need for a warrant is in instances where law enforcement has reason to believe that a crime has been committed (or is about to be committed) and an immediate search is required.

Fourth Amendment protections are further refined in specific circumstances as follows.[8] First, public employers, e.g., government, are not required to obtain a search warrant when they conduct workplace searches for investigations of workplace misconduct. The issue is that workplace investigations are substantially different from those conducted by law enforcement because the goal is not law enforcement but rather efficient office operations, a premise upheld by the U.S. Supreme Court. Furthermore, while individuals have a reasonable expectation of privacy in many places, such as homes and automobiles, such an expectation does not apply in the workplace. For example, items of a personal nature may be left at home and need not be stored in the confines of an office, desk, or filing cabinet.

A workplace search is considered reasonable under two circumstances:

- The search must be justified at its inception because it is likely to reveal evidence of work-related misconduct. The requirement implies that a clear suspicion exists based on a preliminary review of the evidence.
- The search is necessary to further the investigation. An example of this concept is that the investigator is able to obtain files that are a required part of the investigation. The requirement implies that the search is likely to reveal pertinent information.

Assuming that the search is reasonable based on these criteria; the scope of the search must be no broader than is necessary to serve the organization's legitimate, work-related purpose. The investigator may, in fact, have no search limitations if the employee has no reasonable expectation of privacy in the place to be searched. For example, a general filing cabinet with travel reimbursement forms has no reasonable expectation of privacy whereas the individual's desk is much more likely to yield items of a personal nature. Thus, many workplace areas have no reasonable expectation of privacy for any employee. The key factor is *exclusive control*. If the individual has exclusive control over a particular area, a reasonable expectation of privacy is more likely to become an issue. As noted above, even with exclusive control, the only standard that an employer must meet is that the search is reasonable based on the above guidelines.

A second area of special consideration for the Fourteenth Amendment is searches incidental to arrest. First, an arrest can only be made based on probable cause. (A citizen may make an arrest only for a crime committed in his or her presence.) As such, law enforcement officers may search an area within his or her immediate control at the time of the arrest without a warrant for the purposes of self-protection and to prevent the destruction of evidence. If the arrest is later invalidated, however, the search is also invalidated. This potential suppression of evidence can be very frustrating to law enforcement

7. Section 2.310, Fraud Examiner's Manual.
8. Section 2.312, Fraud Examiner's Manual.

investigators. Of course, no warrant is required for evidence that is in plain view. Furthermore, borders and customs agents are provided an exception for searches without warrants.

Search of motor vehicles, including cars, truck, watercraft, and airplanes, may be conducted without a warrant if the law enforcement personnel believe that contraband is present or the vehicle contains other evidence of a crime. The risk of flight with regard to motorized vehicles makes them inherently more risky. Once moved, evidence may be removed or destroyed and such a risk necessitates prompt action. In addition, unlike a home where expectation of privacy is paramount, motorized vehicles are subject to a much lower expectation. The motorized vehicle may be moved to a police facility and inventoried prior to search, and law enforcement may proceed with the search without a warrant. The ability to search vehicles also applies to the contents of the vehicle (e.g., luggage) but does not extend to passengers. Passengers may not be searched without a prior arrest or warrant.

Individuals may waive their Fourth Amendment rights that prevent certain types of searches. Consent by an individual eliminates the need for a search warrant by law enforcement. Like confessions, the waiver of this right will be scrutinized to ensure that it was not coerced in any way. Thus, law enforcement personnel must be able to defend the waiver against claims of false imprisonment, force, violence, and limitations of ability to leave the area, as well as accusations of deceit, bribery, or misrepresentation. Unlike the Miranda warning related to statements, no warning must be made regarding an individual's right to refuse a search. Illegally obtained evidence may not be introduced in court. Furthermore, any information derived from illegal evidence cannot be introduced. This is known as "fruit from the forbidden tree."

Surveillance

Surveillance can be more complex than interviews and searches. Although the rules of conduct for interviews and searches have been defined through federal and state laws and interpretations by the U.S. Supreme Court, the conduct of surveillance has many more issues to consider. As such, counsel should be consulted when surveillance is contemplated. Such techniques include electronic surveillance, including audio and video monitoring and recording. Generally these techniques are not conducted by fraud examiners and forensic accountants because these professionals do not have the required training and skill set. Furthermore, such operations are more common when the suspected activity is complicated and involves multiple individuals, organizations, and jurisdictions. Many of these types of investigative operations are conducted by private investigators or law enforcement officers who have the necessary education, training, and experience.

Several types of surveillance are possible:

- Fixed-point surveillance (e.g., stakeout) involves observing activity from a stationary, discreet location
- Mobile surveillance
- Videography (if audio is also captured during the surveillance, different laws, rules, and regulations are in effect, because audio surveillance has much more stringent requirements)

- Audio or electronic surveillance (e.g., wiretapping)

Surveillance is generally legal. Once the investigator enters the realm of electronic (audio) surveillance, the laws and requirements become more complicated. Generally, federal law prevents the *interception and/or recording* of wire, oral, or electronic communications except by the following[9]:

- Law enforcement officers with a warrant
- Operator of a switchboard or common carrier providing services carrying out job duties and responsibilities
- An employee of the FCC carrying out job duties and responsibilities
- A party to a communication who has given prior consent to the interception (one-party consent)
- A person acting under the Foreign Intelligence Act of 1978

The warrant requirement is the most complicated issue faced by forensic accountants and fraud examiners. With the exception of 13 states, any party to a conversation may record their own conversation. Although the interception and recording of live communication is generally forbidden by federal law without a warrant, stored communication (including voicemail and e-mail) is not nearly as well protected. For example, employers can access stored voicemail and e-mail on their own servers but cannot access the same communications stored by an outside provider (e.g., messages stored on Sprint voicemail). More interestingly, any party to the communication may provide the necessary permission and access to persons not party to the communication.

Generally, video surveillance is permissible as long as it does not violate a person's reasonable expectation of privacy. Anyone in a public park, parking lot, or mall may be videotaped without violating any laws as long as no audio of the target is recorded. Where individuals have a reasonable expectation of privacy, however, such as in their own home, employee restrooms, employee locker rooms, or employee changing areas, video surveillance is not permitted without the existence of extenuating circumstances and a warrant.

Generally, a private employer is prohibited from conducting polygraph examinations (lie-detector tests) unless the employer has suffered economic loss and has reasonable suspicion that the particular employee was involved in the issue under investigation. Like other aspects of the investigation, reasonable suspicion is an evidence-based decision. Under no circumstances, however, can a nongovernment employer use a polygraph examination to screen applicants.

Discharging a Suspected Wrongdoer from Employment

Assuming that an internal, private investigation by an employer results in the conclusion that a particular individual committed a fraud act; can the employer dismiss that employee? Perhaps more intriguing, what if the suspected employee refuses to cooperate and that investigation cannot continue? What then? While public employers are governed by a stricter standard, employer rights are dictated by

9. Section 2.317, Fraud Examiner's Manual.

the jurisdiction in which they operate. Generally, employment is considered at will. This characteristic allows either the employee or the employer to sever the relationship at any time for almost any reason. Employees may have some protections against dismissal for improper reasons, however, even in at will states.

As such, it is advisable that employers document good cause for any termination in the employee's personnel file. Good cause might include the following:

- The employee's conduct was against written policy
- The employee's conduct made for unsafe or inefficient business operations
- The company completed a reasonable investigation to ensure that any such questionable act was committed by the employee and has evidence to support such a claim
- The investigation was fair, objective, and evidence suggested the elimination of alternative suspects
- The termination was nondiscriminatory, meaning that all persons committing such an act were or would be terminated
- The punishment fits the crime, meaning that the punishment is reasonable given the nature of the offense

Such incidents and punitive actions by the company should be carefully considered and well documented. Nothing prevents an employee from suing a former employer in civil court, even if the termination is arguably a reasonable response to the alleged offense.

Privileges

Legal privileges are protections against certain types of testimony. With the exception of the privilege against compelled self-incrimination, most of the following privileges are not constitutionally based:

- Attorney–client privilege
- Attorney work-product privilege
- Physician–patient privilege
- Marital privileges
- Miscellaneous privileges

Attorney–Client Privilege

The attorney–client privilege is the right to not disclose any confidential communication relating to the professional relationship, where the client can be an individual or a corporation. Interestingly, the privilege belongs to the client, and the client has the right to compel nondisclosure by the attorney, whereas the attorney may only assert the privilege if acting on behalf of the client. The attorney–client

privilege applies only to communications that are intended to be confidential. This privilege does not permit an attorney to conceal physical evidence or documents and does not apply to future acts of a crime or fraud.

Attorney Work−Product Privilege

Attorneys have a work−product privilege. The privilege protects all materials prepared by an attorney in anticipation of litigation and is designed to preserve the adversarial trial process by shielding materials that would disclose the attorney's theory of the case or trial strategy. Attorney work-product is defined as any written materials, charts, notes of conversations and investigations, and other materials directed toward preparation of a case. To preserve this privilege, the material must be prepared in anticipation of litigation or the factual context must make it probable that litigation will arise.

Physician–Patient Privilege

In most states, confidential communications made to a physician, as well as psychiatrists, psychotherapists, and psychologists, for the purpose of obtaining treatment or diagnosis are privileged. Consultations that take place with regard to litigation, however, are not covered (e.g., examinations by court-appointed physicians or expert witnesses). Furthermore, when patients are involved in litigation and put their medical condition at issue, they are deemed to have waived this privilege.

Marital Privileges

In some cases, marital privileges exist. The first is spousal immunity and protects a person from having to testify against his or her spouse—although such testimony is permitted, and cannot be stopped by the spouse. At the state level, a slight majority of states give the privilege to the spousal defendant, which protects them from adverse testimony. This privilege is usually allowed in both civil and criminal cases and covers statements made during the marriage and applies even if the parties are no longer married at the time of trial. Neither privilege applies to crimes or torts within a family.

Miscellaneous Privileges

Nearly all states recognize a privilege for confidential communications made to members of the clergy in their professional capacity as spiritual advisors. The government also has a variety of privileges that protect the disclosure of sensitive information in its possession. Finally, some courts recognize qualified privileges for trade secrets for businesses. Contrary to popular belief, there is no legal privilege for accountant–client relationships.

The Daubert Standard

According to the Wex Legal Information Institute at Cornell Law, the ruling in Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993) created what became known as the Daubert standard—the test currently used in the federal courts and some state courts related to the admissibility of expert testimony (expert opinions). Under the Daubert standard, the trial judge makes an assessment of whether an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Under this standard, the factors that may be considered in determining whether the methodology is valid include the following:

1. whether the theory or technique in question can be and has been tested;
2. whether it has been subjected to peer review and publication
3. its known or potential error rate
4. the existence and maintenance of standards controlling its operation;
5. whether it has attracted widespread acceptance within a relevant scientific community

In anticipation of a Daubert challenge, attorneys may ask a practicing forensic accountant or fraud examiner to provide the basis for their opinions by grounding them in textbook passages and chapters, professional guidance, journal articles, treatises, practitioner articles, and other materials that offer support for the expert's application of particular material in a particular context.

For example, a case might involve assertions that weather created circumstances that prevented a party from completing outdoor work on-time or on-budget. The forensic accountant might pull historical nonfinancial data (metrics) from the National Weather Service on quantities of rain and compare historical data to the actual data during the construction period. This activity is comparable to comparing actual data to an expectation (a budget, created from historical data). The forensic accountants have to be careful that they do not project their work to be that of a meteorologist. Rather, they are simply comparing what a contractor working outdoors might anticipate compared to what happened. The data might show that rain was twice as high during the construction period in comparison to historical averages. In such case, it's possible that construction dates were compromised and the contractor exceeded budget. Whether construction delays and cost overruns were explicitly associated with weather might require additional data analysis and examination. Nevertheless, it's common for accounting professionals when explaining variances from budget to identify extenuating circumstances, such as weather, an employee stoppage, an environmental event, etc. It's important to search for all possible causes and to rule out nonrelevant causes using data. It's pertinent that the forensic accountant was testing the assertion for reasonableness by essentially comparing "budget" to "actual," a common activity of accountants. Whether comparing historical weather data to actual would be admissible under the Daubert standard, in the end, is up to the judge.

In the Manpower case (U.S. court of Appeals for the Seventh Circuit, No. 12-2688, Manpower, Inc. v Insurance Company of the State of Pennsylvania, October 1, 2013), the appeals court reversed a lower court ruling concluding that the lower court's exclusion of an accounting expert's opinion was an inappropriate use of the Daubert standard. Specifically, the lower court had ruled that the expert had followed the prescribed methodology by calculating lost incremental profits by taking lost revenues minus noncontinuing expenses. Rather the lower court was concerned with the inputs to the calculations, suggesting that the result "turns on whether the expert used reliable methods when selecting the numbers used in his calculations—specifically, projected total revenues and projected total expenses." The lower court was troubled by model inputs. The appeals court reversed the lower court decision, suggesting that the model inputs were judgments for which the jury could decide their appropriateness. From the appellate court's opinion, "The district court usurps the role of the jury, and therefore abuses its discretion, if it unduly scrutinizes the quality of the expert's data and conclusions rather than the reliability of the methodology the expert employed."

It's important for forensic accountants and fraud examiners to attempt to use appropriate methods and be able to explain why they selected their method for a particular case. It's also important to use data, facts and circumstances, grounded in the evidence. At the same time, it's prudent to expect that all of one's will be carefully examined and scrutinized.

MODULE 3: PROBABLE CAUSE

USA Today journalist Yu reports that "shares of Caterpillar fell 2% after a report commissioned by the government accuses the manufacturer of tax and accounting fraud."[10] According to Yu, Caterpillar, which makes construction equipment products, said it wasn't given a copy of the report, which was viewed and originally reported by The New York Times. Law enforcement officials raided Caterpillar's corporate headquarters and facilities in Peoria, Ill. last week to execute a search and seizure warrant. According to the article, Caterpillar made several statements:

- The warrant is focused on the collection of documents and electronic information.
- We are vigorously contesting the proposed increases to tax and penalties for these years of approximately $2 billion.
- We believe that the relevant transactions complied with applicable tax laws and did not violate judicial doctrines.

Underlying any arrest or warrant is a probable cause. Probable cause is the standard by which law enforcement may make an arrest, conduct a personal or property search, or obtain a warrant. The term also refers to the standard used by grand juries when they believe that a crime has been committed. One of the first issues associated with probable cause is to define the players. A witness is a person who is not suspected of the crime at issue. As one moves to the top of the culpability scale, a target is believed to stand a better than fifty percent probability of being criminally charged with a crime. Somewhere between witnesses and targets are subjects. Subjects may have committed unethical conduct and may be involved in suspicious activity but they have not crossed the line to the point where their behavior is considered likely to be judged criminal (based on the current state of the investigation and the evidence). As evidence is developed and the investigation proceeds, players' roles may change. For example, subjects may become targets or subjects may be relegated to witnesses.

The origins of probable cause rest with the Fourth Amendment to the U.S. Constitution, which states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Despite this phraseology, the threshold for probable cause is not as high as one might expect.

In *Terry v. Ohio* (1968), the U.S. Supreme Court established that some brief seizures may be made without probable cause. Known as the Terry Stop, the court ruled that if a police officer has reasonable suspicion (not probable cause) that a crime has been committed or will soon be committed, that officer may briefly detain an individual, search him or her for weapons, and question the person.

10. Roger Yu, "Caterpillar Shares Fall after Tax, Accounting Fraud Report," USA Today, March 8, 2017.

In 1974, in *The United States v. Matlock*, the U.S. Supreme Court ruled that the co-occupant of a residence may permit a search in the absence of any other co-occupant. This rule is known as the *co-occupant consent rule* and established that an officer who makes a search with a reasonable belief that the search was consented to (i.e., voluntary) by a resident does not need to have probable cause for the search.

Finally, in *Illinois v. Gates* (1983), the U.S. Supreme Court lowered the threshold for probable cause by ruling that a "substantial chance" or "fair probability" of criminal activity could establish probable cause and that a better-than-even chance of criminal behavior is not required.

Related more specifically to fraud, financial crimes, and white-collar crime, in recent times, law enforcement and other investigators have resorted to more sophisticated methods for identifying and investigating fraud. They have, therefore, turned to tools traditionally set aside for organized crime, drug trafficking, and similar investigations such as wiretaps, video surveillance, undercover operations, seizure of records, and allowing less culpable individuals to plead guilty to lesser charges for their testimony against decision makers and those considered more culpable. In addition to these investigative techniques, alleged perpetrators also are pursued in both the civil and criminal justice systems. These tools and techniques allow investigators and prosecutors to gain leverage over the defendant, maximize pressure on alleged perpetrators, and achieve as much cooperation as possible. Charges of mail fraud, wire fraud, money laundering, racketeering, or conspiracy typically come from these investigations.

Not surprisingly, most frauds and financial crimes are solved using documentary and electronic evidence. Such evidence is typically the key to, or the basis for, most white-collar crime cases. The challenge, and where probable cause comes into play, is the issue of how to obtain the necessary evidence (i.e., physical and electronic). Generally, investigators can obtain documents and datafiles using three approaches:

- Voluntary consent
- Subpoena
- Search warrant

Subpoenas are issued by grand juries and used to compel witnesses to testify. They may also be used to compel people to turn documents and electronic files over to the authorities (known as a subpoena duces tecum). While grand juries have great leeway related to issuing subpoenas, the Fourth Amendment requires reasonableness. To meet the reasonableness standard, the subpoena must be likely to generate evidence that is (a) relevant to the issue under consideration, (b) be particular and reasonably specific, and (c) be limited to a reasonable time frame. One of the shortcomings of the subpoena approach to obtaining documents is that the investigator is relying on the subpoena recipient to determine what documents fall under the subpoena's particular details. An investigator reviewing the records may come to a different conclusion than a suspect or a suspect's lawyer. Even assuming good faith on the part of the subpoena recipient, the person may not provide all the necessary or required evidence and the investigators would have no way of knowing what documents were missed. Given the above, subpoenas are best used for witnesses and subjects who are less likely to be adversarial to the receipt of the document and information request.

An issue arises concerning the choice of voluntary production of documents and physical evidence or grand jury subpoenas, especially when the subject offers to voluntarily supply evidence. Voluntary consent gives the defense lawyer and/or their client time to gather and review relevant documents, negotiate limitations on irrelevant material, copy documents that are essential to the operations of the client's business, and schedule document production that does not disrupt day-to-day business operations. One of the shortcomings of the subpoena is that its use may prevent criminal investigators from sharing the documentary evidence with other government agencies that may be conducting parallel inquiries. One should note that the discovery process used to gather documents in civil actions is almost always through subpoena, and generally, each side is at the mercy of the other in the sense that they must trust that the other side has provided all available documents that meet the criteria set out in the subpoena.

Beyond subpoenas, search warrants may be used to obtain documents, other physical evidence, and electronic medium. Search warrants are issued by a judge based on probable cause and put the investigator in charge of the evidentiary search. As noted in the review of the three important court cases above, the threshold for probable cause is not overwhelmingly high: there must be some evidence (probable cause) that a crime has been committed and some belief (probable cause) that the search warrant will yield evidentiary support from the person or place that is the subject of the warrant that will help solve the crime. The limitations of the search warrant are in the details included in the warrant itself. It must include details of the place to be searched, the people involved, and types of evidence likely to be seized. As such, a search warrant requires a reasonable level of specificity. Assuming these items are covered by the warrant, the types of records seized include the following:

- Any property that constitutes evidence of the commission of a criminal offense
- Contraband, the fruits of crime, or things otherwise criminally possessed
- Property designed or intended for use, or that are or have been used, as a means of committing a criminal offense

What is the threshold of probable cause in order to obtain a judge's signature on a warrant? Generally, probable cause made through an affidavit is sufficient. Furthermore, a judge considering the warrant application may find probable cause based entirely on hearsay evidence. Finally, in extraordinary circumstances, warrants may even be issued based on an oral application. These are typically reserved for emergencies.

The warrant has several advantages over a subpoena. First, a warrant allows the holder of the warrant, not the target or the defense counsel, to decide which documents are relevant and must be produced. Second, a warrant avoids, but does not eliminate, the possibility of the destruction of evidence. An interesting attribute of a warrant is that while the search is being conducted, it gives the investigator the ability to interview key witnesses. If handled properly, those key witnesses will not have had the opportunity to consult with counsel or prepare for the interview. In law enforcement investigations where the target is operating an illegal enterprise or has an organization tied up in unlawful activities, the warrant permitting the seizure of documents provides tremendous advantages. By seizing documents and computers, as a practical matter, they take away an entity's ability to continue their activities as a

going concern. Regarding the seized items, all that is required is that the person holding the warrant provides the target with a written inventory of any property taken. The main disadvantage of the warrant is that this document can later be challenged because it lacks specificity.

MODULE 4: RULES OF EVIDENCE

As the headline depicts, a "Trail of evidence points to evangelist in DeKalb fraud scheme."[11] According to the article, DeKalb County cut big checks to an evangelist, month after month for two years, on faith that he did important work for Commissioner Elaine Boyer. The commissioner turned in invoices saying that Rooks Boynton, the head of a nonprofit ministry, gave her policy advice and did research. No one within the county government probed any further as she tapped taxpayers for installments of $1,500 to $5,000 at a time. What did Boynton do to earn that money, which topped $83,000? The Atlanta Journal-Constitution after months investigating found no reports, research materials, or memos from Boynton. No county e-mails documenting a working relationship. No policymakers who recall working with the evangelist and eventually, Commissioner Boyer admitted it was all a kickback scheme.

Without evidence there is no proof; without proof there are no convictions or civil verdicts. As the Bible says, "the truth shall set you free." In the world of fraud and forensic accounting, truth needs to be grounded in evidence—physical and/or electronic. One of the surest ways to lose a conviction is to base a case on the "bad person" theory and not conduct a thorough and complete investigation. Conclusions must be grounded in the evidence.

Evidence is anything legally presented at trial to prove a contention and convince a jury. Generally, evidence is admissible in court if it is relevant, its probative value outweighs any prejudicial effects, and it is trustworthy, meaning that it is subject to examination and cross-examination. For the purposes of exploring the rules of evidence, evidence may be testimonial, real (e.g., documents) or demonstrative, or circumstantial or direct (e.g., testimony of an eye witness). At the federal level, rules of evidence apply in both civil and criminal courts. Most states have their own rules of evidence but those rules are generally modeled after the federal rules of evidence.

At trial, attorneys attempt to prove *facts at issue*. These facts at issue are not evidence, but facts supported by evidence. For example, whether or not the defendant was at the victim's home on the night of a crime is a fact at issue; evidence (such as a fingerprint) is offered to prove or disprove the fact. The fingerprint is evidence; the fingerprint, while a fact, is not a fact at issue. The first hurdle for evidence is that it must be admissible. To gain admissibility, the evidence may not be irrelevant to the facts at issue, immaterial, or incompetent (impeachable). Prior to admissibility, the attorney must lay the foundation by demonstrating relevance, materiality, and competence (reliability). The threshold for relevance is that it must make a material fact more or less probable than without the evidence. Even relevant evidence, however, may be excluded from judicial proceedings if it is prejudicial, confusing, or misleading. Materiality refers to the potential impact that a piece of evidence may have. If the evidence has a tendency to affect the determination of the facts at issue, it is considered material. For evidence to be competent, it must be considered reliable. The ultimate value of any piece of evidence is in the eyes of the trier of fact (e.g., juror, judge, magistrate, etc.).

11. J. Edwards, "Trail of Evidence Points to Evangelist in DeKalb Fraud Scheme," The Atlanta Journal-Constitution, August 26, 2014.

Real evidence is that evidence that "speaks for itself" and does not require explanatory testimony. A baseball bat with a victim's blood, hair, and DNA on it speaks for itself. To be admissible, real evidence must be authenticated. Authentication is a function of several attributes. First, the evidence must be collected properly. For example, investigators should not overtly mark evidence (it should be discretely done) or leave their fingerprints on it during collection. Once collected, the evidence must be preserved so that it is not altered or damaged. The evidence must be identifiable as it moves through the judicial system. One of the common elements is that the chain of custody must be preserved. Even though real evidence speaks for itself, it is still subject to interpretation. Simply because a baseball bat was used as a weapon to kill a person and a third-party's fingerprints are on the bat does not make the third person the killer. One of the strengths of real evidence is that jurors, judges, and other triers of fact can see, touch, feel, smell, and possibly hear or taste the evidence.

Demonstrative evidence is any evidence that purports to educate, summarize, or amplify real evidence. PowerPoint slides, summary schedules, graphics, pictures, reenactments, models, etc. are all forms of demonstrative evidence. Demonstrative evidence tends to tell a story and complements other forms of evidence such as real and testimonial evidence. Some examples of demonstrative evidence include the following:

- Photographs and videotapes
- Maps, charts, diagrams, and drawings
- Scale models
- Computer reconstructions or animation
- Scientific tests or experiments

Because demonstrative evidence is not real, it must not create prejudice and it must not materially alter any significant aspect of the facts at issue. Thus, demonstrative evidence is subject to examination for representational faithfulness.

As noted above, documentary evidence is at the heart of most fraud and forensic accounting investigations. Five considerations must be given to any piece of documentary evidence:

1. The document must not have been forged.
2. Original documents are preferable.
3. The document must not be hearsay or objectionable.
4. The document needs to be authenticated.
5. The document must be reliable.

While an original document is preferable, the *best evidence rule* allows copies to be presented at trial under certain circumstances. Mechanical copies of documents are generally allowed assuming that the copy can be authenticated. Note that copies can also qualify as real evidence if they are used to

demonstrate that an original document was altered. Duplicates are typically accepted if they are copies of search warrants, mortgages, lease agreements, duplicate sales slips, official documents, public records, government sealed records, summaries, testimonies, and written admissions.

Chain of custody refers to those individuals who had possession of physical evidence and what they did with it. Essentially, fraud professionals and forensic accountants must be able to establish the origins of evidence and that the evidence has not been altered as a result of the investigation. The chain of custody protects against the possible corruption of evidence as a result of the investigators losing control of it. Close monitoring of all physical evidence is important in a fraud investigation. In civil litigation, much of the discovery work is done through copies transferred among parties. Although it is important to establish the integrity of evidence, generally, the chain of evidence does not normally play a central role in civil disputes. Attorneys for both sides typically stipulate that the evidence is valid.

Testimonial evidence brings about a discussion of hearsay. What happens if one person hears another person make a statement or one person makes a statement that so-and-so said something? Hearsay is a statement made other than those made during legal proceedings. Each person must testify based on his or her own first-hand experience. Presentation in court allows the jury to hear the evidence and allows opposing council to cross-examine the testimony. Despite the need to have live testimony, a number of hearsay exceptions exist. First, if the truth of the statement is not at issue and it does not impact actual guilt or innocence, the statement may be admissible. For example, a person's statements about his or her frustration levels heard by another person (first-hand) is admissible because it is not about guilt or innocence, it's about state of mind. Any statement, oral or written, that can be corroborated is generally admissible. Another interesting aspect of hearsay admissibility is *statements against interest*, defined as any statement that contradicts a prior statement. Such statements against interest are generally admissible. Other types of hearsay that are admissible include the following:

- Business and government records
- Absence of an entry in business records
- Recorded recollections
- Former testimony
- Present sense impressions
- Then existing mental, emotional, or physical condition
- Statements to medical personnel
- Printed matter, learned treatises, and refresher writings

MODULE 5: CRIMINAL JUSTICE SYSTEM

According to Insurance Fraud News, a ringleader of a group that allegedly staged wrecks and accompanying injuries in Harrison, Marion, and Taylor counties in West Virginia to get insurance

payouts pleaded guilty.[12] Dallas Lewis, 55, of Clarksburg, entered a plea before U.S. Magistrate to felony conspiracy to commit mail fraud and will be sentenced at a later date by U.S. District Judge Irene M. Keeley. Lewis is likely to face a recommended sentence of somewhere around five years in prison due to the amount of money involved, the number of victims, and his role as an organizer.

Assistant U.S. Attorney, Traci Cook, explained that Lewis was involved directly in only one of the wrecks but he instructed others on how to stage the wrecks, arranged for drivers, victims inside the vehicles, and even witnesses. According to Cook, requests for damages from insurance companies totaled about $655,000. She cited the investigation by agents of the West Virginia Insurance Commission's Fraud Unit and the U.S. Postal Inspection Service. Lewis was the fourth of the eight defendants in the case to plead guilty.

Most cases never end up in the criminal justice system. Those that do, however, follow a relatively generic path. Readers should keep in mind that each jurisdiction, federal, state, and local, will have their own specific procedures and are advised to consult attorneys in that jurisdiction regarding specific issues and concerns that may impact the case.[13] Targets may enter the criminal justice system from three routes: a warrantless arrest by the police based upon probable cause, an investigation that leads to the filing of an *Information* (a brief, written complaint in support of an arrest by law enforcement), or a grand jury proceeding that leads to an indictment and a subsequent arrest warrant issued by a judge. Assuming an arrest, law enforcement personnel provide the investigative outcomes and evidence to the prosecuting attorney, who decides whether charges will be filed against the target. Those persons formally charged by the prosecutor must appear before a judge "without unnecessary delay." Judges decide if probable cause exists to move forward. For less serious crimes, the judge may decide a verdict and penalty at this time. Another option is a diversion, where the defendant agrees to take some specified action to avoid prosecution.

For more serious crimes, a defense attorney may be assigned, or the defendant will be represented by an attorney of his or her choice. The following may also be evaluated at this time to determine pretrial release and bail: alleged drug use, residence, employment, family ties, and wealth. If the case comes to the criminal justice system through a grand jury, the jury panel decides if sufficient evidence exists to bring the case to trial. The choice of arrest or grand jury is a strategic one. In some cases, law enforcement and prosecutors may decide to let a grand jury prepare an indictment because of their subpoena power. The grand jury may also be used to investigate criminal activity, particularly in drug and other complex criminal organizations.

Assuming that the criminal case proceeds beyond the indictment stage where the defendant is officially charged, the next step is an arraignment hearing. During the arraignment, the defendant is informed of the crime and the charges against him, advised of his rights, and asked to enter a plea: guilty, not guilty, or *Nolo Contendere*, a plea in which the defendant accepts the penalty without admitting guilt. (A Nolo Contendere plea for all practical purposes is a plea of guilty.) If the judge accepts a guilty plea, a penalty will be issued and no trial will be scheduled. Assuming a "not guilty" plea or a plea of "guilty by reason of insanity," the judge will put a trial date on the court calendar.

---

12. Insurance Fraud NEWS, "Leader of West Virginia Crash Ring Pleads Guilty," May 25, 2017.
13. In addition, an entirely different system is available to juveniles.

Unless the defendant chooses a bench trial (one where the judge alone presides), a trial by jury ensues. During a jury trial, the judge still decides matters of law, but the jury decides whether the evidence as presented is sufficient to convict the defendant. If the jury acquits the defendant, the person goes free. If the person is found guilty, a sentencing hearing is scheduled. The sentence may be determined by the jury or the judge, depending on the jurisdiction. During a sentencing hearing, aggravating and/or mitigating circumstances are presented, and often a presentence investigation is undertaken to identify those circumstances that may warrant consideration. That presentence investigation may include victim impact statements. Sentences are tied to the offense and include death sentences (there is no death sentence for fraud in the United States), incarceration, probation, fines, restitution, and other penalties such as drug treatment, house arrest, electronic monitoring, sanctions, denial of federal benefits, community service, and boot camps. For some crimes, incarceration may be mandated.

Subsequent to the guilty verdict and sentence, the convicted person may appeal the verdict, the sentence, or both. Although not applicable in fraud cases, death sentences have automatic appeal. Jail is reserved for sentences of less than one year's duration, whereas prison is reserved for sentences greater than a year. The prison system has varying levels of custody, including community-based facilities, minimum security, medium security, and maximum security. Once a sentence has been fulfilled or is shortened for good behavior, the person is typically placed on parole. Often times, people confuse probation and parole. Probation is a penalty and is used as an alternative to prison, whereas parole is used to describe the corrections process subsequent to having served time in prison. Parole is often used as a reward for good behavior during time served. During the parole period, a parole officer is assigned.

Recidivism refers to the process in which a formerly convicted person reenters the criminal justice system. Unfortunately, many arrestees have a criminal history and the greater the number of prior arrests, the higher the probability of future arrests. Within the United States, more than half of convicted criminals will return to jail during their lifetime, frequently for more serious offenses. The criminal justice system is society and the government's response to an unfortunate fact of life: people commit crimes. Despite the impact on the victims and society in general, the Constitution and case law dictates that law enforcement and grand juries must respect the rights of individuals. Most criminal justice actions are handled at the state and local levels. The U.S. Congress has established the federal response for crimes such as bank robbery, kidnapping, mail fraud, tax fraud, and interstate crimes, but state constitutions, counties, and municipalities further define and refine the criminal justice system. It should be understood that in criminal cases, dual jurisdiction often exists. For example, a bank fraud is not only a federal crime but also a local one. Law enforcement officials decide among themselves which agency will handle the investigation and prosecution.

The hallmark of the criminal justice system in the United States is discretion. At almost every level, people are the decision makers. For example, people, including victims, decide whether to report crimes; law enforcement decides if a crime occurred and what the official response should be. This discretion is pervasive throughout the system: police, other law enforcement, prosecutors, judges and magistrates, correctional officials, and parole authorities. The discretion creates a professional level of responsibility on the part of participants including training, supervision, and periodic performance assessment and reviews.

In the criminal justice system, not only may individuals be named as defendants, but businesses and other organizations may be prosecuted as well. Prosecution can be used to obtain punishment for the wrongdoing entities, and as a means for changing future behavior and forcing cultural changes. Assuming that appropriate cases are prosecuted, entity prosecutions might result in deterrence on a very large scale, possibly industry wide. Prosecution of the entity still allows for prosecution of individuals as well, such as board members, officers, executives, shareholders, and employees. Generally, businesses may be held liable, assuming that the scope of the infraction was within the duties of the individual who committed the crime, and the individual was acting as an agent for the entity. In addition, the agent's action was intended to benefit the entity. Factors that affect the decision to prosecute an entity are similar to those for individual prosecution and include the sufficiency of evidence, likelihood of success at trial, probability of deterrence and rehabilitation, and adequacy of nonprosecutorial remediation options. Other factors are also considered:

- Nature and seriousness of offense
- Corporation's history
- Timely and voluntary disclosure
- Willingness to cooperate
- Corporate compliance program
- Corporate remedial action(s)
- Replacement of management
- Discipline/termination of wrongdoers
- Payment of restitution
- Disproportionate harm to employees, shareholders, and pensioners
- Adequacy of prosecution for individuals
- Adequacy of other remedies: civil, regulatory
- Consistent with the remainder of the criminal justice system, prosecutors have wide discretion in these types of situations

MODULE 6: CIVIL JUSTICE SYSTEM

As noted above, the government prosecutes criminal cases on behalf of society, including the victims. Private parties may also enter the justice system in an attempt to right a wrong or resolve a dispute through the civil justice system. Fraud is just one such wrong that may enter the civil justice system; others include torts, breach of contract, breach of implied contract, negligence, and misrepresentations. The primary purpose of a civil action is to recover losses and possibly reap punitive damages. In fact, money and other similar damages are the main outcome in the civil justice system. In civil cases,

however, Cease and Desist Orders and similar penalties may be attached. The way a fraud perpetrator suffers the risk of incarceration is through the criminal justice system. Fraud examiners and forensic accountants often find their skills put to good use in the civil justice system, not only in matters where fraud claims are made but also where lost profits, wages, value, and other similar allegations are made on behalf of a victim plaintiff. Most civil actions are handled in state court in the jurisdiction of the plaintiff, the party prosecuting the civil case or the jurisdiction of the defendant. Federal courts may be used for larger cases (those involving more than $75,000 or those that are multi-jurisdictional) because the plaintiffs gain greater access to witnesses and documents due to the broad jurisdiction.

Complaints and Pretrial Activity

Civil lawsuits begin when the plaintiff files a complaint in an appropriate jurisdiction. The complaint must provide assurance to the court that it has jurisdiction, outline the grounds for relief, and make a demand for judgment. Because the complaint is filed before the plaintiff may have all of its facts (i.e., before discovery, which is discussed below), the complaint does not need to be overly particular. Interestingly, fraud civil complaints must be specific and outline the fraud misrepresentations (the act), to whom (the impacted victim), how the misrepresentations were false, and other particular details in order to understand the fraud act. Yet, because the plaintiff most likely does not have complete access to the defendant's information and records, the plaintiff may not have a complete story. Normally the defendant files an answer to the complaint, denies liability, and may add counterclaims against the plaintiff or even ask the court for a dismissal. The process to file a complaint and to await the defendant's response can be very time-consuming, and in very larges cases can extend over a year or more. Of course, time is money so the more time spent, the greater the legal fees to the plaintiff and defense lawyers and others involved in the case.

Once the complaint and answer have been filed (and assuming that the case continues in the civil courts) discovery begins. Discovery is the process by which each side may explore the merits of the other side's arguments by obtaining documentary and testimonial evidence. Any matter or material relevant to the civil action that is not privileged is subject to discovery. Normally, discovery may take at least four forms.

Initially, interrogatories are passed to the opposing council. Interrogatories are questions that require answers and those answers become part of the testimonial record. As such, answers are provided under oath. Although interrogatories are one of the least expensive means to obtain evidence from the opposing party because of an inability to ask follow-up questions, except through additional interrogatories, they may not be effective. Opposing parties tend to provide truthful responses yet minimal information.

Subsequent to interrogatories, opposing parties submit "requests to produce documents" to one another. These requests may include copies of contracts, notes from meetings, calendars, invoices, and accounting records of all sorts including general ledgers, trial balances, journal entries, journal entry backup, financial statements, and tax returns. Just about any information that is captured in paper or electronic form is subject to discovery. In very complex cases, the review of discovered documents alone can take years. While attorneys and experts can become almost overwhelmed with produced documents, most are remiss to limit the amount of document production for fear of missing that critical piece of paper that blows their case wide open.

Third, attorneys start to take sworn testimony from opposing parties in the form of depositions. Depositions that are grounded in the evidence and documents are popular and provide very useful information. The format is that the deponent (the person being deposed) provides sworn testimony based on questions developed by opposing council. Assuming that the attorney is well prepared and accomplished, he or she can use the deposition exercise to evaluate a number of issues:

- How good of a witness will this person be; how good will they come across in front of a jury; can I get this person angry, aggressive, defensive, or emotional?
- What is the opposing side's theory of the case; what arguments are they likely to make in court; how deep is the evidence trail behind their theory of the case?
- Is their witness making informed statements grounded in the evidence, or is this person likely to shoot from the hip?
- How does this person react when I propose or suggest my side's theory of the case? Does this person refute my theory with evidence; are they dismissive; are they emotional?

Thus, the deposition process not only provides the opportunity to obtain additional evidence, it provides a good opportunity, especially with key witnesses, including fraud examiners and forensic accounting expert witnesses, to evaluate each side's case and their witness quality. As depositions proceed, it is often common for each side to develop additional requests for the production of documents based on deposition testimony of various parties. For example, a former accountant may know of the existence of a box of records in a storage area that was previously overlooked in a prior request for the production of documents.

The fourth and last stage of discovery is an attempt by counsel to get the other side to agree to certain basic aspects and facts of the case through "requests for admission." This process helps determine what issues are points of contention as the trial approaches, and what points can be agreed upon by both sides. Thus, a request for admission attempts to narrow the scope of the trial to its essential points of contention.

Negotiated Settlements

Once discovery is completed and before trial, judges will often attempt to cajole both sides into settling the case based on the relative merits of their evidence and legal positions. In fact, some attorneys estimate that fewer than five percent of civil actions ever come to trial. There are three major forms of negotiated remedies: out-of-court settlements, arbitration, and mediation. Out-of-court settlements occur when both sides come to a settlement position after examination of their own clients, the evidence, the qualities of their fact witnesses, the strength of their expert opinions, and other important aspects of the case. Assuming that the two sides are reasonably close, the attorneys will confer with their clients and negotiate with the opposing attorney. This process can take weeks or months and may even start during the deposition phase. Normally a negotiated settlement will not be achievable prior to the end of, or near the end of, discovery.

If a negotiated settlement between opposing attorneys in concert with their clients does not work, a second approach is mediation. In this environment, an independent, objective mediator will work with both sets of opposing counsel to help reach a settlement between the two (and their clients). The mediator does not decide who should win, but his or her responsibility is to assist both sides to more objectively assess the merits of their case and work toward a mutually agreeable resolution. Since the mediator has no authority on which to decide cases, any settlement is voluntary on the part of the opposing parties.

A third possibility is arbitration. Like a mediator, an arbitrator is an independent third party who has the authority to determine the outcome of the case. Thus, the arbitrator acts like the judge and jury, listening to the primary aspects of each side's case and deciding what he or she believes to be the most appropriate outcome based on the merits of the cases presented. Arbitration may be binding, meaning that the "verdict" of the arbitrator is final, or it can be nonbinding. Even a nonbinding "verdict" may bring the parties closer together and may result in an out-of-court settlement because of the ability of the arbitrator to independently and objectively evaluate the merits of each side's case.

Pretrial Motions and the Civil Trial

Assuming that the discovery process is complete and any out-of-court attempts to settle the case fail, a slew of pretrial motions are likely to follow:

- Writ of Attachments to prevent defendants from disposing of assets
- Sequestration, in which the court takes possession of certain assets pending the outcome of the trial
- Motions for Injunctive Relief to prevent a defendant from transferring or moving assets pending the trial's outcome
- Motions to Dismiss
- Motions to Make (some aspects of the civil action) More Definite and Certain
- Motions in Limine to prohibit reference to prejudicial matte
- Motions to Strike inflammatory, prejudicial, or irrelevant material from trial
- Motions for Continuance to postpone a hearing or trial
- Motions for Summary Judgment that request the judge to decide the merits of the case without a trial based on material and testimony submitted

Normally, counsel is going to object to motions proposed by the other side of the civil action and a judge will need to decide on the motions in advance of the trial.

It will take months, if not years, for a civil action to actually be heard in a court of law. While many aspects of the civil trial mirror that of a criminal trial, a few important differences exist. First, in most cases the jurors number six persons, and if the opposing attorneys agree, a unanimous verdict is not required. Furthermore, a civil action only requires a preponderance of the evidence, meaning that the evidence

stacks up slightly more heavily on one side than the other. This contrasts with the criminal threshold of "beyond a reasonable doubt." During civil trials the plaintiff goes first, followed by the defense. Then the plaintiff gets a chance to rebut the defense's position. Once a verdict is received, either side may appeal the liability issues and/or the damages portion of the verdict. Furthermore, a plaintiff or defendant who wins monetary damages in a lawsuit will normally have to take additional steps to collect the award. Such steps may include obtaining a financial judgment, garnishing wages, and levying assets. A postjudgment discovery process may be necessary to locate assets available to satisfy a judgment or identify assets that have been moved or transferred in an attempt to avoid satisfying the judgment.

BASIC ACCOUNTING PRINCIPLES

Basic Accounting Principles—A Survivor's Guide to Accounting

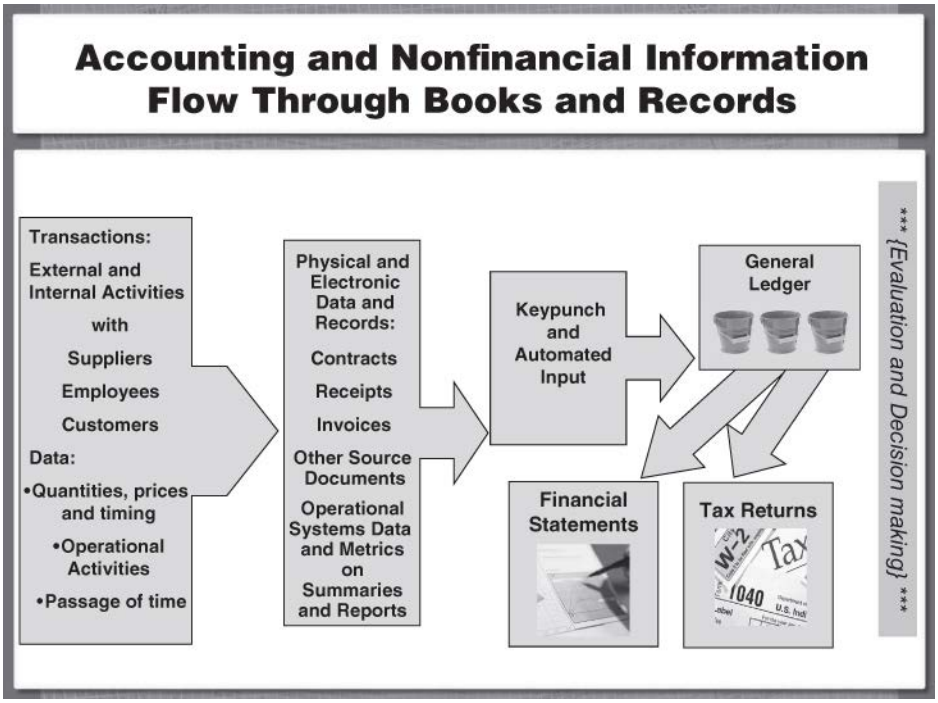
Dr. Sean Stein Smith, Assistant Professor at Lehman College, publishing in the AccountingWeb, states that accountants are well-positioned to take a leading role in efficiency initiatives. In his article, he suggests that there are several specific examples in which accountants can leverage big data to help combat fraud and possibly fraudulent activities[14]:

1. Analyze customer profitability, shopping habits, and shipping locations to determine purchase and payment patterns using big data tools to analyze shifts and trends, as well as irregularities, in real time.
2. Take advantage of improved data collection and processing at operational facilities to improve inventory and other asset control. If operations has the ability to produce and monitor inventory information in real time, accountants can certainly take this information and use it to assist in inventory counts, valuation, and custody.
3. Leverage the more frequent and real-time reporting requirements demanded of both organizations and financial professionals. More frequent reporting, and the data and analytics desired by the recipients of this information, necessitate that accounting professionals become more adept at leveraging internally available information and technology. Additionally, and perhaps most important of all, increased scrutiny and reporting allow accounting professionals greater opportunities to examine and analyze the data before it is disseminated to stakeholders.

In this section, we present an overview of the accounting system that every fraud examiner or forensic accountant needs to understand for successfully navigating financial books and records. Figure 3-1 depicts the flow of accounting information.

14. S. S. Smith, "3 Ways Accountants Can Use Big Data to Fight Fraud," June 15, 2015, https://www.accountingweb.com/.

FIGURE 3-1 ACCOUNTING AND NONFINANCIAL INFORMATION FLOW THROUGH BOOKS AND RECORDS



Basic (accounting) bookkeeping involves the recording, classifying, and summarizing of economic events in a logical manner for the purpose of providing accounting, financial, and nonfinancial information for decision making.

Auditors are concerned with determining whether information recorded in the accounting books and records properly reflects the underlying economics of the transactions. Thus, auditors need to know how to audit and how to evaluate recorded activity for compliance with generally accepted accounting principles (GAAP). Like auditors, the fraud examiner and forensic professional need to have some understanding of transactions and how those transactions are reflected in the books and records. If the facts at issue are associated with allegations of financial statement fraud, the investigator needs to have a thorough understanding of GAAP, auditing procedures, and the impact of any applicable regulations. As noted, fraud examiners and forensic specialists must be able to follow the money. But they must also be able to recognize and identify red flags and anomalous situations where the accounting numbers and amount reflected in underlying accounting records do not make sense or do not seem to add up. Recognition and identification of red flags inherently assumes that the investigator has some expectation of how the numbers should look. This requires some knowledge of basic accounting as well as knowledge of expected relationships between accounting metrics and nonfinancial data generated inside and outside of the organization. Of course, the fraud examiner and forensic accountant must also possess expertise in accumulating and interpreting evidence. The antifraud professional must design procedures to identify anomalies, investigate those anomalies, form and test hypotheses, and evaluate the evidence generated.

As a starting point, activities occur between the company and its stakeholders (board of directors, executive team, management, employees, creditors, bankers, suppliers, employee recruits, customers, suppliers, communities, government agencies, labor unions, etc.). These interactions result from

negotiations and generate paper and electronic documentation of the activities and financial details such as location, prices, quantities, and timing (e.g., dates). Some of the financial aspects of these activities are considered financial transactions, and from those, various forms of physical and electronic paperwork are created: receipts, invoices, contracts, requests for proposal, proposals, purchase orders, bills of lading, shipping documents, funds transfer authorizations, and other source documents. This documentation may be captured in physical form such as printed documents and receipts or entirely in electronic format. The physical and electronic documentation captures the essential terms of the transactions and provides a primary means of inputting data into the formal accounting system. In other cases, the passage of time generates the need for accounting transactions. An example is that over time, the value of a delivery truck declines in the pursuit of revenue. Accounting needs to capture the decline in value across time. In another example, the passage of time generates interest obligations owed to creditors. Again, issue is a result of an organization—stakeholder interactions in prior periods; yet, this obligation needs to be reflected in the accounting system.

Transactions are input (recorded) into the accounting system through journal entries and electronic interfaces with operational (nonaccounting) information systems and posted into the general ledger. The general ledger is analogous to a series of buckets where the accounting transactions are organized and stored. Periodically, the information in the general ledgers is reconciled back to the underlying source documents as well as information provided by nonaccounting systems and external stakeholders, such as banks, credit card companies, vendors, and customers. For example, banks provide monthly statements and the activities reflected on them can be reconciled to the cash "bucket" in the general ledger. The reconciliation process is conducted to ensure the integrity of the information in the general ledger. Once the entity's financial managers are satisfied with the integrity of the general ledger, the financial statements, tax returns, and other summarized financial and nonfinancial information can be created, distributed, and shared for the purposes of performance assessment (evaluation) and decision making.

One of the critical general ledger "buckets" for the fraud examiner and forensic accountant is the cash general ledger account. Most antifraud professionals follow the money. The company receives cash from its customers in the form of currency, checks directly from customers, and checks and electronic deposits from credit card companies. Although fewer in number, entities also receive cash from stockholder investments, loans from creditors, and from sales of old or used equipment. Entities disburse cash by writing checks and distributing them to employees, suppliers, creditors, and others. Cash disbursements can be made via the U.S. Postal Service, wire transfers, and through electronic funds transfer (EFT). All of these cash transactions are captured with various physical and electronic medium and are input into the entity's accounting system and ultimately into the cash general ledger account ("bucket").

At the same time, the entity's bank is capturing and recording the transaction as well. Optimally, good accounting practice mandates that these two systems (the company's cash account and the bank's records of those same transactions) be checked for agreement each month through a formal reconciliation. Similar to cash, most transactions are tracked not only by the company but also by other parties to the transaction, such as customers, vendors, and creditors. Thus, fraud examiners and forensic accountants review the company's accounting books and records as well as the corresponding information from third parties to look for discrepancies from which fraud investigations are often launched.

Not only do fraud examiners and forensic accountants need to monitor transactions from the perspective of the company and corresponding outsiders but they also need to ensure that the accounting information corresponds to the company's nonaccounting information because many business activities are not captured in the accounting system, but rather a function of operational management information systems and data from a variety of other sources. For example, a contract between a company and a customer to deliver goods and services next year is referred to as "backlog" and is not reflected in the accounting records until the company starts to fulfill its contractual obligation. Yet, backlog is a critical metric, the detail of which is carefully measured, monitored, and evaluated across time.

Notice how the information sources and flow are depicted in Figure 3.1 that starts on the left by capturing data reflecting financial transactions, nonfinancial operational systems, and the passage of time into the accounting system. Management information systems (MIS) are used to provide the data required by managers to run their operations. For example, a petroleum plant would carefully monitor raw materials inventory levels, the transfers of raw materials into the manufacturing process, and various aspects of production to ensure quality, the amount of manufacturing output, and inventory levels of finished product. These data are critical for plant managers; they could not do their job without detailed and accurate information. In some systems, data from the nonaccounting systems are designed to interface electronically with the accounting information systems. In others, summarized data from the MIS systems are used as a manual input into the accounting system. In either case, antifraud professionals and forensic accountants will use data from nonaccounting sources as a means of looking for discrepancies with data reflected in the accounting records, a source of red flags.

Nonfinancial data can be generated from many sources. As an example, consider a bar owner who is suspected of underpaying taxes. A method commonly used is to look for data that is not normally captured in the accounting system. To illustrate, as described in DiGabrile, one crafty fraud examiner took all of the invoices supporting cost of goods sold, added up the quantities purchased, and multiplied the quantities by the selling prices on the bar's menu. The approach resulted in hundreds of thousands of dollars of underreported revenue. Because quantities presented on an accounting record (i.e., an invoice that describes prices, quantities, and dates) are not captured by the accounting system, it becomes a nonfinancial information source upon which to identify discrepancies. To be successful, fraud examiners and forensic accountants need to continually seek out information sources from independent third parties and from internal sources that are not directly reflected in the accounting system as a means of evaluating data captured and reported in accounting reports, such as financial statements and tax returns. Even the reconciliation of tax returns to financial statements often reveals discrepancies between the two that serve as red flags that require additional investigative inquiry.

Other basic but critical aspects of the accounting process that fraud examiners and forensic accountants need to know include the following:

- Types of financial statements
- How cash transactions are categorized: operating, investing, and financing activities
- A second categorization approach: assets, liabilities, stockholders equity, revenues, and expenses

- Every transaction affects at least two general ledger "buckets" (accounts)
- Accrual accounting: the revenue recognition principle and the expense matching principle
- Accounting choices and exceptions: materiality and conservatism
- The importance of what's not on the financial statements. Consider the following example:

Value of Checking Account?	
Cash in from Owner	$750
• Loan from Bank	0
– Inflows	$750
• Purchase Office Equipment	$300
• Purchase Production Machine	250
• Rent	275
• Purchase Supplies	75
– Outflows	$900
• Inflows from Customers Sales	$300
• Remaining cash in checking	**$150**

The checking account for this start-up business has an initial deposit of $750 from the owner, pays for various items totaling $900, and collects $300 from sales to customers. These transactions leave a month-end checking account balance of $150. The ultimate question: Is the business owner better off at the end of the month than at the beginning? On the one hand, he started with $750 in cash but only has $150 now; that doesn't sound so good. On the other hand, the owner now has equipment and production machinery that have value and an ongoing business operation—also valuable. Another issue not addressed in the accounting system is the sales potential. Is a $300 sale per month a maximum or is that the result of a few days' sales at the end of the first month of business after the infrastructure was put in place? While this example has only a few transactions, what if the business had 100, 1,000, or 10,000 cash transactions? The point is that simply looking at checking account information is not enough. The accounting profession has responded to this anomaly by transferring the above information into a series of financial statements: balance sheet, income statement, and the cash flow statement. These documents meaningfully reorganize the above data for effective performance assessment and decision making.

Balance Sheets

The balance sheet measures the financial condition of an entity at a point in time. It does this by measuring the resources that a business has, its assets, and compares the business's resources (assets) to the sources from which those resources came. Resources are acquired with money provided from one of two sources: creditors (suppliers, banks, etc.) and the company's owners. Amounts owed to creditors are liabilities, and funds contributed by the owner are the stockholders' (or owner's) equity. Although a little confusing, the owner's contribution comes from two sources: investments of cash into the business and earnings (income) from prior periods that owners have left in the business (retained earnings) to fund additional investment and operational expansions. The balance sheet is set up in the fundamental accounting equation where assets must always equal liabilities plus owner's equity. From the balance sheet, the financial condition can be evaluated. Too many liabilities make the company vulnerable to

bankruptcy. Liabilities, however, reflect the owner's ability to use "other people's money" to fund the business, suggesting that more liabilities are good. Simplistically, one challenge for business owners is to balance liabilities against owner's equity to maximize the use of other people's money without increasing the business's risk of bankruptcy. Of course, negative owner's equity suggests that liabilities exceed the value of the assets as recorded on the balance sheet and that is seldom, if ever, good news.

Income Statement

The second major financial statement is the income statement. This summarizes information about a company's financial performance over a period of time (e.g., month, quarter, year). The income statement measures inflow from customers arising from sales of goods and services (revenue) versus outflow required to operate the business (expenses). The terms inflows and outflows are carefully chosen because sometimes sales to customers result in receivables, not cash. Similarly, outflows consider the fact that some items required to run the business are paid in advance (e.g., insurance is often paid in advance of a six-month or one-year policy), while others are paid after they are used (e.g., employees are paid after they render services because it takes time to collect time cards, summarize the hours, input them into a payroll system, calculate taxes and other withholdings, and cut checks). We address the differences in timing between cash flows in more detail below (see accruals).

Statement of Cash Flows

The third and final major financial statement is the statement of cash flows. This takes each "cash" transaction and categorizes it into one of three categories after considering how it affects the business. The three categories are cash flow from operating activities, investing activities, and financing activities. Operating cash flows are those cash transactions associated with day-to-day business activities: production and sales of goods and services and cash outflows to pay for operational expenses. Net operating cash flows are expected to be positive because a business should be taking in more cash from its customers than it is paying out to suppliers, employees, and for other expenses necessary to operate the business. The second category of cash flows includes payments for the acquisition of long-term assets and cash received from the sale of older or obsolete long-term assets. These are referred to as investing activities and, generally, the net of these types of cash transactions are expected to be negative because companies should be expending cash on long-term assets to secure a productive future.

The last category of cash flows includes receipts and payments associated with business financing choices and have four major types of activities:

1. Cash inflows from new loans.
2. Cash outflows from the repayment of loans (excluding interest which is categorized as operating).
3. Cash inflows from new stock investors.
4. Cash outflows to stock investors in the form of dividends.

Given these types of receipts and payments, financing cash flow could be negative or positive. In the early years in the life of a business, financing cash flows are more likely to be positive and, as a company matures, financing cash flows may turn toward the negative.

One of the challenges of accounting data is that it can be evaluated from multiple perspectives. As noted above, all cash transactions can be categorized as operating, investing, or financing. Since that categorization is associated only with the cash flow statement, those same transactions can also be categorized based on their effect on the other two statements: balance sheet and income statement. More interestingly, when evaluating the impact of a transaction on the balance sheet and income statement, each transaction has at least two effects. Some examples might help.

Example 1

A customer receives a service this month but will not pay for that service until next month, and the amount of the service is $100.

Assessment: Note that this transaction has no (zero) cash flow impact. It has two other effects:

- The business has a receivable amount of $100 from a customer (balance sheet)
- The business has made a sale of $100 (revenue on the income statement)

Example 2

A customer receives a service this month, paid cash at the time of the sale, and the amount of the service is $200.

Assessment: Note that this transaction has a $200 cash flow impact that is categorized as operating. It also has two other effects:

- The business has received cash of $200 (an asset on the balance sheet)
- The business has made a sale of $200 (revenue on the income statement)

Example 3

The company pays its one employee $25 on the twentieth of the month for the employee's work during the first half of the month.

Assessment: Note that this transaction has a $25 cash flow impact that is categorized as operating. It also has two other effects:

- The business has paid out cash of $25 (reducing the cash asset on the balance sheet)
- The business has a payroll expense of $25 (expense on the income statement)

Example 4

The company owes its one employee $30 as of the end of the month for the employee's work during the second half of the month.

Assessment: Note that this transaction has no (zero) cash flow impact. It has two other effects:

- As of month end, the business owes the employee $30 (liability on the balance sheet)
- The business has a payroll expense of $30 (expense on the income statement)

Example 5

During the month, the company pays its insurance company $120 for a twelve-month policy. Note that the company is trying to create financial statements for the current month only.

Assessment: Note that this transaction has a $120 cash flow impact that is categorized as operating. It also has three other effects:

- The business has paid out cash of $120 (reducing the cash asset on the balance sheet)
- The business has an insurance expense of $10 for the current month (expense on the income statement)
- The business has a resource that has future value (asset), totaling $110 for the remaining eleven months of the insurance policy (prepaid asset on the balance sheet)

Example 6

The company receives a check from a customer in the amount of $125 for services rendered during the previous month.

Assessment: Note that this transaction has a $125 cash flow impact that is categorized as operating. It has two other effects:

- The business's receivable amount has been reduced by $125 as a result of the customer payment (reducing a balance sheet asset)
- The business has additional cash of $125 (increasing the cash asset on the balance sheet)

Note that even though this transaction arose from a sale to a customer, sales were recorded in the prior month and there is no income statement impact in the current month.

Accrual Accounting

Examples one, four, five, and six bring up the issue of accrual accounting. It recognizes the impact of a company's activities that affect its financial condition (balance sheet) or financial performance (income statements) that may not coincide with the timing of cash flows. Accruals are used to capture the financial impact of transactions for which the cash flows associated with the transaction are recorded in other periods (e.g., cash flows were in a prior month or year or the cash flow will occur in a future month or year). Whether or not a noncash transaction qualifies for treatment as an accrual transaction that must be recorded in the accounting books and records is determined by two matters: the revenue recognition principle and the matching principle.

The revenue recognition and matching principles are further refined through generally accepted accounting principles called Statements of Financial Accounting Standards, also known as SFASs, which are developed by the Financial Accounting Standards Board (FASB) as well as other authoritative guidance.[15] While the revenue recognition and matching principles provide conceptual guidelines, the guidance contained in the SFASs and other authoritative guidelines takes precedence. The revenue recognition principle requires that the revenue be recorded in the period earned, and the expense matching principle requires that expenses be matched against the revenues they helped to generate. The intent of these two principles is that revenues and expenses are recorded in the proper period. More specifically, revenue is recognized when the following three criteria have been met:

1. Customers have received goods or services.
2. All material uncertainty (risk) has been passed along to the customer.
3. Collection of cash related to revenue is likely.

Following revenue recognition, expenses are matched to revenue under three conditions:

1. Costs are incurred to generate revenue (e.g., wages).
2. Assets (capitalized costs) are no longer a resource with future value because they have been consumed to earn revenue (e.g., depreciation).
3. Assets (capitalized costs) are no longer a resource with future value due to obsolescence.

Most people who are new to accounting believe that accounting is very rules driven and specific, and with regard to many aspects of accounting, they are correct. Such a belief, however, ignores the vast number of areas where management is required to exercise its judgment. The biggest problem area for accounting regulators is revenue recognition. Despite the above guidance, management has tremendous latitude related to the accounting principles they choose, the period that is most appropriate to record a specific type of transaction, the estimated useful life of an asset, and the estimated collectability of receivables from customers, to name a few.

15. In addition to SFASs, FASB issues Statements on Financial Accounting Concepts (SFAC); Interpretations, which clarify, explain, or elaborate on FASB Statements, Accounting Research Bulletins (ARB), or Accounting Pinciples Board (APB) Opinions; Technical Bulletins; Exposure Documents; and Discussion Papers.

Two additional conceptual principles provide accounting discretion. First, if a transaction or series of transactions are deemed "immaterial," the accountants can handle the transaction in any manner they wish. The theory is that if the amount is immaterial, how it is accounted for has little or no significant impact on decision making. While no specific number is agreed upon, some general rules of thumb are one percent of assets, one percent of revenues (sales), or five percent of pretax net income. For billion-dollar companies, transactions deemed immaterial can have very large dollar amounts associated with those thresholds.

A third and final area of discretion is related to a principle called conservatism. It suggests that if two outcomes are equally likely, the one that has the more negative effect is the better choice in situations where negative impact includes understating assets and revenues and overstating liabilities and expenses. Recently, standard setters and regulators seem more interested in determining the best estimate of financial condition and performance versus presenting the most pessimistic picture, but conservatism remains an influential concept.

Performance Assessment and Decision Making

One of the primary benefits of the financial and nonfinancial data generated, examined, interpreted, and monitored through the accounting process is for their use as inputs in performance assessment and decision making. Importantly, performance evaluation and decision making are ultimately grounded in professional judgment. Judgment is a function of education, training, and experience. Often accounting and nonaccounting information serve as the foundation of assessment and decisions. As sometimes stated, the accounting and nonaccounting data and analysis will seldom tell one what to do, it will most often eliminate many bad courses of action, leaving management and stakeholders with a relatively few choices (e.g., two, three, or four) upon which decision makers can focus their attention. Evaluation is typically done at the internal (e.g., trends across time) and external (company comparison to the industry and/or key competitors) levels.

One analysis is to prepare common-sized financial statements: balance sheets, income statements, and cash flows. With common-sized statements, balance sheet line items are presented as a percentage of total assets, and income and cash flow statement line items are presented as a percentage of total net sales or gross revenue. The percentages can then be examined internally across time and temporally to competitors and industry metrics.

Ratio analysis is another evaluation technique. There are five categories of ratios:

- Liquidity ratios
- Operating efficiency ratios
- Operating profitability ratios
- Business risk (operating) analysis ratios
- Financial risk (leverage) analysis ratios

Much has been written about these ratios, their calculation, use, and interpretation. In the following table, we will present each of the five categories, the specific ratios, and the usual formula for calculation.

Ratios	Formulation
Liquidity Ratios	
Current Ratio	Current Assets/Current Liabilities
Quick Ratio	Cash + Marketable Securities + Receivables/Current Liabilities
Days in Receivable	365/Net Sales/((Beginning A/R + Ending A/R) ÷ 2)
Days in Inventory	365/Cost of Goods Sold/((Beginning Inventory + Ending Inventory) ÷ 2)
Days in Accounts Payable	365/Accounts Payable/((Beginning Inventory + Ending Inventory) ÷ 2)
Cash Conversion Cycle	Days in Inventory + Days in Receivable − Days in Accounts Payable
Operating Efficiency Ratios	
Fixed Asset Turnover	Net Sales/((Beginning Fixed Assets + Ending Fixed Assets) ÷ 2)
Asset Turnover	Net Sales/((Beginning Assets + Ending Assets) ÷ 2)
Operating Profitability Ratios	
Cost of Sales/Sales (%)	Cost of Goods Sold/Net Sales
Gross Margin (%)	Gross Profit (Net Sales – Cost of Goods Sold)/Net Sales
Operating Profit Margin (%)	Operating Profit (Net Sales – Operating Expenses)/Net Sales
Profit Margin (%)	Net Income/Net Sales
Return on Assets (%) (ROA)	Net Income/((Beginning Assets + Ending Assets) ÷ 2)
Return on Equity (%) (ROE)	Net Income/((Beginning Stockholders' Equity + Ending Stockholders' Equity) ÷ 2)
Business Risk (Operating) Ratios	
Operating Income (EBIT) Volatility (Coefficient of Variation)	Average earnings before interest and taxes for several time periods/ Standard deviation of earnings before interest and taxes for several time periods
Sales Volatility (Coefficient of Variation)	Average net sale for several time periods/Standard deviation of sales for several time periods
Degree of Operating Leverage	Percentage change in earnings before interest and taxes/Percentage change in sales
Financial Risk (Leverage) Analysis Ratios	
Debt to Assets	Total Debt (short and long-term liabilities)/Assets
Equity to Assets	Stockholders' Equity/Assets
Debt to Equity	Total Debt (short and long-term liabilities)/Stockholders' Equity
Interest Coverage Ratio	Earnings before interest and taxes/Interest Expense
Operating Cash Flow Ratio	Operating cash flow/Current Liabilities

The Dupont model is a method of performance measurement that demonstrates how the tools of evaluation fit together for a more comprehensive analysis. For example, return on assets can be expressed as a function of net income, net sales, and assets as follows:

ROA = Profit Margin * Asset Turnover = (Net Income/Net Sales) * (Net Sales/Average Assets)

Return on assets can be also described as a function of net income, stockholders' equity, and assets as follows:

ROA = ROE * Equity to Assets = (Net Income/Average Stockholders' Equity) * (Stockholders' Equity/Assets)

Further, return on equity can be also described as a function of net income, net sales, stockholders' equity, and assets as follows:

ROE = Profit Margin * Asset Turnover * Equity to Assets = (Net Income/Net Sales) * (Net Sales/Average Assets) * (Stockholders' Equity/Assets)

Of course, as noted throughout the discussion of accounting, financial and nonfinancial data, and analysis above and throughout this text, forensic accountants and fraud examiners are experts with metrics, numbers, and analysis. As such, the FAFE professional will be correlating financial and nonfinancial data, metrics, and numbers from a variety of sources to evaluate their reasonableness and compare hypotheses (fraud theories) and assertions (claims made by parties to a civil dispute). It's important that the professional consider hypotheses and assertions from many angles and attempt to examine data and interpret findings with an open mind and let the evidence lead them to defensible conclusions and opinions.

REGULATORY SYSTEM

An understanding of the regulatory system—entities such as the SEC and Public Company Accounting Oversight Board (PCAOB), laws such as the Sarbanes–Oxley Act (SOX), and Dodd-Frank—is an important aspect of the fraud examiner's and forensic accountant's education related to fraud detection and deterrence. While accounting, per se, is not regulated, various aspects of the accounting profession and the financial reporting process come under the purview of multiple regulatory bodies.

The AICPA and Statement on Auditing Standards No. 99

While the FASB develops generally accepted accounting principles, the purview of auditing of nonpublic companies falls under the guidelines of the American Institute of Certified Public Accountants (AICPA).

Subsequent to the passage of the Sarbanes–Oxley Act of 2002, regulation of public companies became the responsibility of the newly created Public Company Accounting Oversight Board (PCAOB), but the AICPA retained the authority to set standards and make rules in five major areas:

- Auditing standards (for nonpublic companies)
- Compilation and review standards
- Other attestation standards
- Consulting standards
- Code of professional conduct

An audit is performed to ensure that the financial statements are fairly presented and are free from material misstatement. Note that this does not imply that financial statements are entirely correct or accurate. More specifically related to fraud, AICPA Statement on Auditing Standards (SAS) No. 99 directs that an audit should be planned and performed to obtain "reasonable assurance" about whether the financial statements are free of material misstatements, whether caused by error or fraud.

Furthermore, auditing standards require that an audit be completed with due professional care, which, in turn, requires that the auditor exercises professional skepticism. The causes of misstatements are errors

and fraud. Fraud can arise from one of two sources: misappropriation of assets that rises to the level of materiality or (material) financial reporting fraud. (The ACFE lists three sources of what it defines as *occupational fraud*: asset misappropriations, fraudulent financial statements, and corruption. The latter category is distinguished from the first two in that it requires a coconspirator, sometimes not employed by the entity.) Examples of financial reporting fraud include the falsification of underlying accounting books and records and omission of certain transactions.

Professional skepticism entails three overlapping concepts:

- An attitude that includes a questioning mind and a critical assessment of audit evidence
- Conducting of the engagement that recognizes the possibility of material misstatement due to fraud
- Dissatisfaction with less-than-persuasive evidence

From the Fraudster's Perspective

Adapted from the whitecollarfraud.com blog by Sam E. Antar

Sunday, March 4, 2007

White-Collar Crime: How Criminals Exploit Your Humanity

As a criminal, I considered your humanity as a weakness to be exploited in the commission of my crimes. I have often said that white-collar crime is a crime of deceit, and white-collar criminals are artful liars.

A great president, Ronald Reagan, once said, "Trust, but verify," when dealing with the Soviet Union during the cold war. However, as a criminal I took advantage of your initial inclination to trust me. I did everything in my power, to charm you by pointing out the good deeds I had done, in an effort to corrode your objectivity, professional skepticism, and cynicism.

During my many unpaid speaking engagements, people often ask if I am still a criminal today. My answer is that you do not know if I am a criminal today since I live with temptation and sin every day. Just because I travel the country and give unpaid presentations on white-collar crime and pay all travel expenses out of pocket, how do you know if I am building a false wall of integrity around me as I did during my criminal years at Crazy Eddie? You never know anyone's intentions.

Stated more succinctly, an auditor should have a questioning mind, recognize that financial statements may be materially misstated, and require persuasive evidence (evidence-based decision making).

SAS No. 99 specifically recognizes the importance of the fraud triangle: incentives (pressures), opportunity, and rationalization. SAS No. 99 offers an eight-step approach when considering the risk of materially misstated financial statements due to fraud.

Step 1 states that at the outset of an audit engagement auditors should undertake a staff discussion concerning the risks of fraud. The staff discussion should consist of brainstorming as well as considering

how and where the financial statements might be susceptible to fraud and emphasize the need for professional skepticism.

Step 2 involves gathering information necessary to identify fraud risks, including inquiries of management, the audit committee, internal auditors, and others; the results of analytical procedures; identified fraud risk factors; and other information that may be suggestive of fraud.

During **Step 3**, auditors attempt to identify risks that may result in fraud, giving consideration to the types of risks, the significance or magnitude of the risk, the likelihood of the risk, and the pervasiveness of the risk.

In **Step 4**, the auditor assesses fraud risks after consideration of programs and controls to prevent fraudulent financial reporting. The auditors must rely on their understanding of the systems of internal control and evaluate whether they actually address the fraud risks identified. Since internal controls are designed to reduce the opportunity for fraud, this reassessment after recognition of internal control policies and processes is an important step in the process.

Step 5 requires the auditor to develop specific responses to fraud risks. As the risk of materially misstated financial statements increases, the auditor may respond in several ways. For example, the auditor can assign more experienced staff to the engagement, give more attention to accounting policies and choices, and apply less predictable audit procedures. In short, the auditor needs to increase the amount and quality of audit evidence by altering the nature, timing, and extent of audit procedures. A critical aspect of step 5 is assessing the possibility of management override. Despite a well-designed and implemented system of internal controls, certain individuals in management and the executive suite have tremendous influence and control. At times, the influence and control is so powerful that some managers may be able to override the system of internal controls. Essentially, the system of internal controls operates fine but for the actions of a few select, powerful individuals. The risk of management override should not be underestimated even in the most successful and well-run entities. To address the issue of management override, auditors should examine adjusting journal entries, support for adjusting journal entries, accounting estimates, underlying rationale and support for accounting estimates, and unusual (one time), significant transactions and the underlying rationale and support for the accounting treatment of these transactions.

Step 6 considers the audit evidence and requires auditors to continually assess fraud risk throughout the audit. The auditor needs to evaluate analytical procedures performed as substantive tests, evaluate risk of fraud near completion of fieldwork, and respond to identified material misstatements.

In Step 7, the auditor must communicate his findings as follows:

- All fraud to an appropriate level of management
- All management fraud to the audit committee
- All material fraud to management and the audit committee
- If reportable conditions related to the internal control environment have been identified, the auditor must communicate those to the audit committee

Step 8 ensures that the auditor has documented each of these steps in the consideration of fraud:

- Staff discussion
- Information used to identify risk of fraud
- Fraud risks identified
- Assessed risks after considering programs and controls
- Results of assessment of fraud risk
- Evaluation of audit evidence
- Communications requirements

The Sarbanes–Oxley Act of 2002

The Sarbanes–Oxley Act of 2002 was signed into law on July 30, 2002, to address corporate governance and accountability as well as public accounting responsibilities in improving the quality, reliability, integrity, and transparency of financial reports. The Act provides sweeping measures aimed at

- Establishing higher standards for corporate governance and accountability
- Creating an independent regulatory framework for the accounting profession
- Enhancing the quality and transparency of financial reports
- Developing severe civil and criminal penalties for corporate wrongdoers
- Establishing new protections for corporate whistleblowers

The Act has authorized the SEC to issue implementation rules on many of its provisions intended to improve corporate governance, financial reporting, and audit functions. The SEC has issued the following implementation rules pertaining to the Act:

- New standards of professional conduct for attorneys
- Standards and procedures related to listed company audit committees
- Strengthening of the commission's requirements regarding auditor independence
- Disclosure in management's discussion and analysis about off-balance sheet arrangements and aggregate contractual obligations
- Disclosures regarding a Code of Ethics for Senior Financial Officers and Audit Committee Financial Experts
- Retention of records relevant to audits and reviews
- Insider trades during pension fund blackout periods

- Conditions for use of non-GAAP financial measures
- Certifications of disclosure in companies' quarterly and annual reports

These implementation rules are expected to create an environment that promotes strong marketplace integrity, new criminal and civil penalties for violations of securities laws, improve the probability of detection and deterrence of corporate misstatements, and restore public trust in the quality and transparency of financial information. Table 3-1 summarizes important provisions of the Act aimed at improving corporate governance, financial reports, and audit functions.

TABLE 3-1 CORPORATE GOVERNANCE AND ACCOUNTING PROVISIONS OF THE SARBANES–OXLEY ACT OF 2002

Sec.	Provisions
101	**Establishment of Public Company Accounting Oversight Board (PCAOB)**
	1. The PCAOB will have five financially literate members.
	2. Members are appointed by the SEC for five-year terms, will serve on a full-time basis, and may be removed by the SEC "for good cause."
	3. Two of the members must be or have been CPAs, and the remaining three must not be or have been CPAs.
	4. The chair may be held by one of the CPA members, who must not have been engaged as a practicing CPA for five years.
103	**The PCAOB shall:**
	1. Register public accounting firms (foreign and domestic) that prepare audit reports for issuers.
	2. Establish, or adopt, by rule, auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers.
	3. Conduct inspections of registered public accounting firms.
	4. Conduct investigations and disciplinary proceedings and impose appropriate sanctions.
	5. Enforce compliance with the Act, the rules of the Board, and other applicable rules and regulations.
	6. Establish budget and manage the operations of the Board and its staff.
107	**Commission Oversight of the Board:**
	1. The SEC shall have oversight and enforcement authority over the PCAOB.
	2. The SEC can, by rule or order, give the PCAOB additional responsibilities.
	3. The PCAOB is required to file proposed rules and proposed rule changes with the SEC.
	4. The SEC may approve, reject, or amend such rules.
	5. The PCAOB must notify the SEC of pending investigations and coordinate its investigation with the SEC Division of Enforcement.
	6. The PCAOB must notify the SEC when it imposes any final sanction on any accounting firm or associated person.
	7. The PCAOB findings and sanctions are subject to review by the SEC, which may enhance, modify, cancel, reduce, or require remission of such sanction.
108	**Accounting Standards:**
	1. The SEC may recognize as "generally accepted" any accounting principles that are established by a standard-setting body that meets the Act's criteria.
	2. The SEC shall conduct a study on the adoption of a principles-based accounting system.

Sec.	Provisions
201	**Auditor Independence: Services outside the Scope of Practice of Auditors:** 1. Registered public accounting firms are prohibited from providing any nonaudit services to an issuer contemporaneously with the audit including but not limited to (1) bookkeeping or other services related to the accounting record or financial statement of the audit client, (2) financial information systems design and implementation, (3) appraisal or valuation services, (4) actuarial services, (5) internal audit outsourcing services, (6) management functions or human resources, (7) broker or dealer, investment advisor, or investment banking, (8) legal services and expert services unrelated to the audit, and (9) any other services that the PCAOB determines, by regulation, to be impermissible. 2. The PCAOB may, on a case-by-case basis, exempt from these prohibitions any person, issuer, public accounting firm, or transaction, subject to review by the SEC. 3. Nonaudit services not explicitly prohibited by the Act, such as tax services, can be performed upon preapproval by the audit committee and full disclosure to investors.
203	**Audit Partner Rotation:** The lead audit or coordinating partner and reviewing partner of the registered accounting firm must rotate off of the audit every five years.
204	**Auditor Reports to Audit Committees:** The registered accounting firm must report to the Audit Committee 1. All critical accounting policies and practices to be used 2. All alternative treatments of financial information within generally accepted accounting principles, ramifications of the use of such alternative disclosures and treatments, and the preferred treatment 3. Other material written communication between the auditor and management
206	**Conflicts of Interest:** The registered accounting firm is prohibited from performing an audit for an issuer whose CEO, CFO, controller, chief accounting officer, or person in an equivalent capacity employed by the accounting firm during the one-year period preceding the audit.
207	**Study of Mandatory Rotation of Registered Public Accounting Firms:** The Comptroller General of the United States will conduct a study on the potential effects of requiring the mandatory rotation of public accounting firms.
301	**Public Company Audit Committees:** 1. Each member of the audit committee shall be an independent member of the board of directors. 2. To be considered independent, the member of the audit committee should not receive any compensations other than for service on the board, not accept any consulting, advisory, or other compensatory fee from the company, and not be an affiliated person of the issuer or any subsidiary thereof. 3. The SEC may make exemptions for certain individuals on a case-by-case basis. 4. The audit committee shall be directly responsible for the appointment, compensation, and oversight of the work of any registered public accounting firm associated by the issuer. 5. The audit committee shall establish procedures for the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters, and the confidential, anonymous submission by employees of the issuer or concerns regarding questionable accounting or auditing matters. 6. The audit committee shall have the authority to engage independent counsel and other advisers necessary to carry out its duties. 7. The audit committee shall be properly funded.

Sec.	Provisions
302	**Corporate Responsibility for Financial Reports:** 1. The signing officers (e.g., CEO, CFO) shall certify in each annual or quarterly report filed with the SEC that (1) the report does not contain any untrue statement of a material fact or omitted material facts that cause the report to be misleading and that (2) financial statements and disclosures fairly present, in all material respects, the financial condition and results of operations of the issuer. 2. The signing officers are responsible for establishing and maintaining adequate and effective controls to ensure reliability of financial statements and disclosures. 3. The signing officers are responsible for proper design, periodic assessment of the effectiveness and disclosure of material deficiencies in internal controls to external auditors and the audit committee.
303	**Improper Influence on Conduct of Audits:** It shall be unlawful for any officer or director of an issuer to take any action to fraudulently influence, coerce, manipulate, or mislead auditors in the performance of financial audit of the financial statements.
304	**Forfeiture of Certain Bonuses and Profits:** 1. CEOs and CFOs who revise company financial statements for the material noncompliance with any financial reporting requirements must pay back any bonuses or stock options awarded because of the misstatements. 2. CEOs and CFOs shall reimburse the issuer for any bonus or other incentive-based or equity-based compensation received or any profits realized from the sale of securities during that period for financial restatements due to material noncompliance with financial reporting and disclosure requirements.
306	**Insider Trades During Pension Fund Blackout Periods:** 1. It shall be unlawful for any directors or executive officers directly or indirectly to purchase, sell, or otherwise acquire or transfer any equity security of the issuer during any blackout periods. 2. Any profits resulting from sales in violation of this section shall inure to and be recoverable by the issuer.
401	**Disclosures in Periodic Reports:** 1. Each financial report that is required to be prepared in accordance with GAAP shall reflect all material correcting adjustments that have been identified by the auditors. 2. Each financial report (annual and quarterly) shall disclose all material off-balance-sheet transactions and other relationships with unconsolidated entities that may have a material current or future effect on the financial conditions of the issuer. 3. The SEC shall issue final rules providing that pro forma financial information filed with the Commission (1) does not contain an untrue statement of a material fact or omitted material information and (2) reconciles with the financial condition and results of operations. 4. The SEC shall study the extent of off-balance sheet transactions, including assets, liabilities, leases, losses, and the use of special purpose entities, and whether the use of GAAP reflects the economics of such off-balance sheet transactions.
402	**Extended Conflict of Interest Provisions:** It is unlawful for the issuer to extend credit to any directors or executive officers.
404	**Management Assessments of Internal Controls:** 1. Each annual report filed with the SEC shall contain an internal control report which shall (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting and (2) contain an assessment of the effectiveness of the internal control structure and procedures as of the end of the issuer's fiscal year. 2. Auditors shall attest to, and report on, the assessment of the adequacy and effectiveness of the issuer internal control structure and procedures as part of audit of financial reports in accordance with standards for attestation engagements.

Sec.	Provisions
406	**Code of Ethics for Senior Financial Officers:** The SEC shall issue rules to require each issuer to disclose whether it has adopted a code of ethics for its senior financial officers and the nature and content of such code.
407	**Disclosure of Audit Committee Financial Expert:** The SEC shall issue rules to require each issuer to disclose whether at least one member of its audit committee is a "financial" expert as defined by the Commission.
409	**Real Time Issuer Disclosures:** Each issuer shall disclose information on material changes in the financial condition or operations of the issuer on a rapid and current basis.
501	**Treatment of Securities Analysts:** Registered securities associations and national securities exchanges shall adopt rules designed to address conflicts of interest for research analysts who recommend equities in research reports.
601	**SEC Resource and Authority:** SEC appropriations for 2003 are increased to $776,000,000, from which $98 million shall be used to hire an additional 200 employees to provide enhanced oversight of audit services.
602	**Practice before the Commission:** 1. The SEC may censure any person, or temporarily bar or deny any person the right to appear or practice before the SEC if the person does not possess the requisite qualifications to represent others, has willfully violated Federal Securities laws, or lacks character or integrity. 2. The SEC shall conduct a study of "Securities Professionals" (e.g., accountants, investment bankers, brokers, dealers, attorneys, investment advisors) who have been found to have aided and abetted a violation of Federal Securities laws. 3. The SEC shall establish rules setting minimum standards for professional conduct for attorneys practicing before the commission.
701	**GAO Study and Report Regarding Consolidation of Public Accounting Firms:** The GAO shall conduct a study regarding consolidation of public accounting firms since 1989 and determine the consequences of the consolidation, including the present and future impact and solutions to any problems that may result from the consolidation.
802	**Criminal Penalties for Altering Documents:** 1. It is a felony to knowingly alter, destroy, falsify, cover up, conceal, or create documents to impede, obstruct, or influence any existing or contemplated federal investigation. 2. Registered public accounting firms are required to maintain all audit or review work-papers for five years.
903 904 906	**White Collar Crime Penalty Enhancements:** 1. The maximum penalty for mail and wire fraud is ten years. 2. The SEC may prohibit anyone convicted of securities fraud from being a director or officer of any public company. 3. Financial reports filed with the SEC (annual, quarterly) must be certified by the CEO and CFO of the issuer. The certification must state that the financial statements and disclosures fully comply with provisions of Securities Acts and that they fairly present, in all material respects, financial results and conditions of the issuer. Maximum penalties for willful and knowing violations of these provisions of the Act are a fine of not more than $500,000 and/or imprisonment of up to five years.
1001	**Corporate Tax Returns:** The federal income tax return of public corporations should be signed by the CEO of the issuer.
1005	**Authority of the SEC:** The Commission may prohibit a person from serving as a director or officer of a publicly traded company if the person has committed securities fraud.

Certification Obligations for CEOs and CFOs

One of the most significant changes affected by the Sarbanes–Oxley Act is the requirement that the Chief Executive Officer and the Chief Financial Officer of public companies personally certify annual and quarterly SEC filings. These certifications essentially require CEOs and CFOs to take responsibility for their companies' financial statements and prevent them from delegating this responsibility to their subordinates and then claiming ignorance when fraud is uncovered in the financial statements. There are two types of officer certifications mandated by Sarbanes–Oxley: criminal certifications, which are set forth in Section 906 of the Act and codified at 18 USC § 1350; and civil certifications, which are set forth in Section 302.

Criminal Certifications (§ 906) Periodic filings with the SEC must be accompanied by a statement, signed by the CEO and CFO, which certifies that the report fully complies with the SEC's periodic reporting requirements and that the information in the report fairly presents, in all material respects, the financial condition and results of operation of the company. These certifications are known as *criminal certifications* because the act imposes criminal penalties on officers who violate the certification requirements. Corporate officers who *knowingly* violate the certification requirements are subject to fines of up to $1,000,000 and up to ten years imprisonment, or both. Corporate officers who *willfully* violate the certification requirements are subject to fines of up to $5,000,000 and up to twenty years imprisonment, or both.

Civil Certifications (§ 302) Section 302 of the Act requires the CEO and CFO to personally certify the following in their reports:

1. They have personally reviewed the report.
2. Based on their knowledge, the report does not contain any material misstatement that would render the financials misleading.
3. Based on their knowledge, the financial information in the report fairly presents, in all material respects, the financial condition, results of operations, and cash flow of the company.
4. They are responsible for designing, maintaining, and evaluating the company's internal controls; they have evaluated the controls within ninety days prior to the report; and they have presented their conclusions about the effectiveness of those controls in the report.
5. They have disclosed to the auditors and the audit committee any material weaknesses in the controls and any fraud, whether material or not, that involves management or other employees who have a significant role in the company's internal controls.
6. They have indicated in their report whether there have been significant changes in the company's internal controls since the filing of the last report.

Note that in items two and three the CEO and CFO are not required to certify that the financials are accurate or that there is no misstatement. They are simply required to certify that *to their knowledge* the financials are materially representative and not misleading. This does not mean, however, that senior

financial officers can simply plead ignorance about their companies' SEC filings in order to avoid liability. The term *fairly presents* in item three is a broader standard than what is required by GAAP. In certifying that their SEC filings meet this standard, the CEO and CFO essentially must certify that the company (1) has selected appropriate accounting policies to ensure the material accuracy of the reports; (2) has properly applied those accounting standards; and (3) has disclosed financial information that reflects the underlying transactions and events of the company. Furthermore, the other new certification rules (see 1, and 4–6 above) mandate that CEOs and CFOs take an active role in their companies' public reporting, and in the design and maintenance of internal controls.

It is significant that in item four, the CEO and CFO have to certify not only that they are responsible for their companies' internal controls but also that they have evaluated the controls *within ninety days prior to their quarterly or annual report*. Essentially, this certification requirement mandates that companies actively and continually reevaluate their control structures to prevent fraud.

Item five requires the CEO and CFO to certify that they have disclosed to their auditors and their audit committee any material weaknesses in the company's internal controls, and also any fraud, *whether material or not*, that involves management or other key employees. Obviously, this is a very broad reporting requirement that goes beyond the "material" standard contemplated in SAS 82. The CEO and CFO now must report to their auditors and audit committee any fraud committed by management. This places a greater burden on the CEO and CFO to take part in antifraud efforts and to be aware of fraudulent activity within their companies in order to meet this certification requirement.

Item six is significant because periodic SEC filings must include statements detailing significant changes to the internal controls of publicly traded companies.

Management Assessment of Internal Controls

In conjunction with the § 302 certification requirements on the responsibility of the CEO and CFO for internal controls, § 404 of SOX requires all annual reports to contain an internal control report that (1) states management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting and (2) contains an assessment of the effectiveness of the internal control structure and procedures of the company for financial reporting. The filing company's independent auditor will also be required to issue an attestation report on management's assessment of the company's internal control over financial reporting. This attestation report must be filed with the SEC as part of the company's annual report.

New Standards for Audit Committee Independence

Section 301 of the Act requires that the audit committee for each publicly traded company shall be directly responsible for appointing, compensating, and overseeing the work of the company's outside auditors. The Act also mandates that the auditors must report directly to the audit committee—not management—and makes it the responsibility of the audit committee to resolve disputes between management and the auditors. Section 301 also requires that the audit committee must have the authority and funding to hire independent counsel and any other advisors it deems necessary to carry out its duties.

Composition of the Audit Committee

The Sarbanes–Oxley Act mandates that each member of a company's audit committee must be a member of its board of directors and must otherwise be independent. The term independent means that the audit committee member can receive compensation from the company only for his or her service on the board of directors, the audit committee, or another committee of the board of directors. The company may not pay them for any other consulting or advisory work.

Financial Expert

Section 407 of the Act requires every public company to disclose in its periodic reports to the SEC whether or not the audit committee has at least one member who is a financial expert, and if not to explain the reasons why. The Act defines a financial expert as a person who, through education and experience as a public accountant or an auditor, or a CFO, comptroller, chief financial officer, or a similar position (1) has an understanding of generally accepted accounting principles and financial statements; (2) has experience in preparing or auditing financial statements of comparable companies and the application of such principles in accounting for estimates, accruals, and reserves; (3) has experience with internal controls; and (4) has an understanding of audit committee functions.

Establishing a Whistle-Blowing Structure

The Act makes it the responsibility of the audit committee to establish procedures (e.g., a hotline) for receiving and dealing with complaints and anonymous employee tips regarding irregularities in the company's accounting methods, internal controls, or auditing matters.

New Standards for Auditor Independence

Perhaps the greatest concern arising out of the public accounting scandals of 2001 and 2002 was the fear that public accounting firms that received multimillion-dollar consulting fees from their public company clients could not maintain an appropriate level of objectivity and professional skepticism in conducting audits for those clients. In order to address this concern, Congress, in § 201 of the Sarbanes–Oxley Act, established a list of activities that public accounting firms are now prohibited from performing on behalf of their audit clients. The prohibited services are as follows:

- Bookkeeping services
- Financial information systems design and implementation
- Appraisal or valuation services, fairness opinions, or contribution-in-kind reports
- Actuarial services
- Internal audit outsource services
- Management functions or human resources
- Broker or dealer, investment adviser, or investment banking services
- Legal services and expert services unrelated to the audit
- Any other service that the Public Company Accounting Oversight Board proscribes

There are certain other nonaudit services—most notably tax services—that are not expressly prohibited by Sarbanes–Oxley. In order for a public accounting firm to perform these services on behalf of an audit client; however, that service must be approved in advance by the client's audit committee. Approval of the nonaudit services must be disclosed in the client's periodic SEC reports.

Mandatory Audit Partner Rotation

Section 203 of the Act requires public accounting firms to rotate the lead audit partner or the partner responsible for reviewing the audit every five years.

Conflict of Interest Provisions

Another provision of Sarbanes–Oxley aimed at improving auditor independence is § 206, which seeks to limit conflicts or potential conflicts that arise when auditors cross over to work for their former clients. The Act makes it unlawful for a public accounting firm to audit a company if—within the prior year—the client's CEO, CFO, controller, or chief accounting officer worked for the accounting firm and participated in the company's audit.

Auditor Reports to Audit Committees

Section 301 requires that auditors report directly to the audit committee, and § 204 makes certain requirements as to the contents of those reports. In order to help ensure that the audit committee is aware of questionable accounting policies or treatments that were used in the preparation of the company's financial statements, § 204 states that auditors must make a timely report of the following to the audit committee:

- All critical accounting policies and practices used
- Alternative GAAP methods that were discussed with management, the ramifications of the use of those alternative treatments, and the treatment preferred by the auditors
- Any other material written communications between the auditors and management

Auditors' Attestation to Internal Controls

As was stated previously, § 404 of the Act requires every annual report to contain an internal control report, which states that the company's management is responsible for internal controls and also assesses the effectiveness of the internal control structures. Section 404 requires the company's external auditors to attest to and issue a report on management's assessment of internal controls.

Improper Influence on Audits

The Act also makes it unlawful for any officer or director of a public company to take any action to fraudulently influence, coerce, manipulate, or mislead an auditor in the performance of an audit of the company's financial statements. This is yet another attempt by Congress to ensure the independence and objectivity of audits in order to prevent accounting fraud and strengthen investor confidence in the reliability of public company financial statements.

Enhanced Financial Disclosure Requirements

Off-Balance Sheet Transactions

As directed by § 401 of the Act, the rules require disclosure of:

> *all material off-balance sheet transactions, arrangements, obligations (including contingent obligations), and other relationships the company may have with unconsolidated entities or persons that may have a material current or future effect on the company's financial condition, changes in financial condition, liquidity, capital expenditures, capital resources, or significant components of revenues or expenses.*

These disclosures are required in all annual and quarterly SEC reports.

Pro Forma Financial Information

Section 401 also directs the SEC to issue rules on pro forma financial statements. These rules require that pro forma financials must not contain any untrue statements or omissions that would make them misleading, and that they are reconciled to GAAP. These rules apply to all pro forma financial statements that are filed with the SEC or that are included in any public disclosure or press release.

Prohibitions on Personal Loans to Executives

Section 402 makes it illegal for public companies to make personal loans or otherwise extend credit, either directly or indirectly, to or for any director or executive officer. There is an exception that applies to consumer lenders if the loans are consumer loans of the type the company normally makes to the public, and on the same terms.

Restrictions on Insider Trading

Section 403 establishes disclosure requirements for stock transactions by directors and officers of public companies, or by persons who own more than ten percent of a publicly traded company's stock. Reports of changes in beneficial ownership by these persons must be filed with the SEC by the end of the second business day following the transaction.

Under § 306, directors and officers are also prohibited from trading in the company's securities during any pension fund blackout periods. This restriction only applies to securities that were acquired as a result of their employment or service to the company. A blackout period is defined as any period of more than three consecutive business days in which at least 50% of the participants in the company's retirement plan are restricted from trading in the company's securities. If a director or officer violates this provision, he or she can be forced to disgorge to the company all profits received from the sale of securities during the blackout period.

Codes of Ethics for Senior Financial Officers

Pursuant to § 406 of the Act, the SEC establishes rules that require public companies to disclose whether they have adopted a code of ethics for their senior financial officers and if not, to explain the reasons why. The new rules also require immediate public disclosure any time there is a change of the code of ethics or a waiver of the code of ethics for a senior financial officer.

Enhanced Review of Periodic Filing

Section 408 of the Act requires the SEC to make regular and systematic reviews of disclosures made by public companies in their periodic reports to the SEC. Reviews of a company's disclosures, including its financial statements, must be made at least once every three years. Prior to this enactment, reviews were typically minimal and tended to coincide with registered offerings.

Real-Time Disclosures

Under § 409, public companies must publicly disclose information concerning material changes in their financial condition or operations. These disclosures must be "in plain English" and must be made "on a rapid and current basis."

Protections for Corporate Whistleblowers under Sarbanes–Oxley

The Sarbanes–Oxley Act establishes broad new protections for corporate whistleblowers. There are two sections of the Act that address whistleblower protections: Section 806 deals with civil protections and Section 1107 establishes criminal liability for those who retaliate against whistleblowers.

Civil Liability Whistleblower Protection

Section 806 of the Act, which is codified at 18 USC § 1514A, creates civil liability for companies that retaliate against whistleblowers. It should be noted that this provision does not provide universal whistleblower protection; it only protects employees of publicly traded companies. Section 806 makes it unlawful to fire, demote, suspend, threaten, harass, or in any other manner discriminate against an employee for providing information or aiding in an investigation of securities fraud. In order to trigger § 806 protections, the employee must report the suspected misconduct to a federal regulatory or law enforcement agency, a member of Congress or a committee of Congress, or a supervisor. Employees are also protected against retaliation for filing, testifying in, participating in, or otherwise assisting in a proceeding filed or about to be filed relating to an alleged violation of securities laws or SEC rules.

The whistleblower protections apply even if the company is ultimately found not to have committed securities fraud. As long as employees reasonably believe they are reporting conduct that constitutes a violation of various federal securities laws, then they are protected. The protections cover retaliatory acts not only by the company but also by any officer, employee, contractor, subcontractor, or agent of the company.

If a public company is found to have violated § 806, the Act provides for an award of compensatory damages sufficient to "make the employee whole." Penalties include reinstatement; back pay with interest; and compensation for special damages including litigation costs, expert witness fees, and attorneys' fees.

Criminal Sanction Whistleblower Protection

Section 1107 of Sarbanes–Oxley—codified at 18 USC § 1513—makes it a crime to knowingly, with the intent to retaliate, take any harmful action against a person for providing truthful information relating to the commission or possible commission of any federal offense. This protection is only triggered when

information is provided to a law enforcement officer; it does not apply to reports made to supervisors or to members of Congress, as is the case under § 806.

In general, the coverage of § 1107 is much broader than the civil liability whistleblower protections of § 806. While the § 806 protections apply only to employees of publicly traded companies, § 1107's criminal whistleblower protections cover all individuals (and organizations) regardless of where they work. Also, § 806 only applies to violations of securities laws or SEC rules and regulations. Section 1107, on the other hand, protects individuals who provide truthful information about the commission or possible commission of *any federal offense*. Violations of § 1107 can be punished by fines of up to $250,000 and up to ten years in prison for individuals. Corporations that violate the Act can be fined up to $500,000.

Enhanced Penalties for White-Collar Crime

As part of Congress' general effort to deter corporate accounting fraud and other forms of white-collar crime, the Sarbanes–Oxley Act also enhances the criminal penalties for a number of white-collar offenses.

Attempt and Conspiracy

The Act amends the mail fraud provisions of the United States Code (Chapter 63) to make attempt and conspiracy to commit offenses subject to the same penalties as the offense itself. This applies to mail fraud, wire fraud, securities fraud, bank fraud, and health-care fraud.

Mail Fraud and Wire Fraud

Sarbanes–Oxley amends the mail fraud and wire fraud statutes (18 USC § 1341, 1343), increasing the maximum jail term from five to twenty years.

Securities Fraud

Section 807 of the Act makes securities fraud a crime under 18 USC § 1348, providing for fines up to $250,000 and up to twenty-five years in prison.

Document Destruction

Section 802 of the Act makes destroying evidence to obstruct an investigation or any other matter within the jurisdiction of any U.S. department illegal and punishable by a fine of up to $250,000 and up to twenty years in prison. This section also specifically requires that accountants who perform audits on publicly traded companies to maintain all audit or review work papers for a period of five years. Violations of this rule may be punished by fines up to $250,000 and up to ten years in jail for individuals, or fines up to $500,000 for corporations. (Although § 802 only requires work papers to be maintained for five years, keep in mind that under § 103 of the Act the Public Company Accounting Oversight Board is directed to set standards that require public accounting firms to maintain audit work papers for seven years. Accounting firms should design their document retention policies accordingly.) Section 1102 of the Act makes it a criminal offense to corruptly alter, destroy, mutilate, or conceal a record or document with the intent to impair its integrity or use in an official proceeding or to otherwise obstruct, influence, or impede any official proceeding or attempt to do so. Violations of this section are punishable by fines up to $250,000 and imprisonment for up to twenty years.

Freezing of Assets

During an investigation of possible securities violations by a publicly traded company or any of its officers, directors, partners, agents, controlling persons, or employees, the SEC can petition a federal court to issue a forty-five-day freeze on "extraordinary payments" to any of the foregoing persons. If granted, the payments will be placed in an interest-bearing escrow account when the investigation commences. This provision was enacted to prevent corporate assets from being improperly distributed while an investigation is underway.

Bankruptcy Loopholes

Section 803 amends the bankruptcy code so that judgments, settlements, damages, fines, penalties, restitution, and disgorgement payments resulting from violations of federal securities laws are nondischargeable. This is intended to prevent corporate wrongdoers from sheltering their assets under bankruptcy protection.

Disgorgement of Bonuses

One of the most unique aspects of the Sarbanes–Oxley Act is § 304, which states that if a publicly traded company is required to prepare an accounting restatement due to the company's material noncompliance, as a result of misconduct, with any financial reporting requirement under securities laws, then the CEO and CFO must reimburse the company for

- Any bonus or other incentive-based or equity-based compensation received during the twelve months after the initial filing of the report that requires restating
- Any profits realized from the sale of the company's securities during the same twelve-month period

While the Act requires the CEO and CFO to disgorge their bonuses if the company's financial statements have to be restated because of misconduct, it makes no mention of *whose* misconduct triggers this provision. There is nothing in the text of § 304 that limits the disgorgement provision to instances of misconduct by the CEO and CFO. Presumably then, the CEO and CFO could be required to disgorge their bonuses and profits from the sale of company stock even if they had no knowledge of and took no part in the misconduct that made the restatement necessary.

Now we understand the underlying accounting principles that allow financial statement frauds to occur and the impact of the Sarbanes–Oxley Act to discourage these acts.

The Public Company Accounting Oversight Board (PCAOB)

Title I of Sarbanes–Oxley establishes the Public Company Accounting Oversight Board whose purpose is:

> *to oversee the audit of public companies that are subject to the securities laws, and related matters, in order to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies the securities of which are sold to, and held by and for, public investors. (Section 101)*

In short, the Board is charged with overseeing public company audits, setting audit standards, and investigating acts of noncompliance by auditors or audit firms. The Board is appointed and overseen by the Securities and Exchange Commission. It is made up of five persons, two who are or have been CPAs and three who have never been CPAs. The Act lists the Board's duties, which include the following:

- Registering public accounting firms that audit publicly traded companies
- Establishing or adopting auditing, quality control, ethics, independence, and other standards relating to audits of publicly traded companies
- Inspecting registered public accounting firms
- Investigating registered public accounting firms and their employees, conducting disciplinary hearings, and imposing sanctions where justified
- Performing such other duties as are necessary to promote high professional standards among registered accounting firms, to improve the quality of audit services offered by those firms, and to protect investors
- Enforcing compliance with the Sarbanes–Oxley Act, the rules of the Board, professional standards, and securities laws relating to public company audits

Registration with the Board

Public accounting firms must be registered with the Public Company Accounting Oversight Board in order to legally prepare or issue an audit report on a publicly traded company. In order to become registered, accounting firms must disclose, among other things, the names of all public companies they audited in the preceding year; the names of all public companies they expect to audit in the current year; and the annual fees they received from each of their public audit clients for audit, accounting, and nonaudit services.

Auditing, Quality Control, and Independence Standards and Rules

Section 103 of the Act requires the Board to establish standards for auditing, quality control, ethics, independence, and other issues relating to audits of publicly traded companies. On December 18, 2003, the Board adopted Auditing Standard No. 1, *References in Auditors' Reports to the Standards of the Public Company Accounting Oversight Board*. This standard requires that auditors' reports on engagements conducted in accordance with the Board's standards include a reference that the engagement was performed in accordance with the standards of the PCAOB. This supersedes historically requisite references to generally accepted auditing standards (GAAS). Adopted rules do not take effect until the SEC approves them, as detailed in § 107 of the Act. Although the Act places the responsibility on the Board to establish audit standards, it also sets forth certain rules that the Board is required to include in those auditing standards. These rules include the following:

- Audit work papers must be maintained for at least seven years.

- Auditing firms must include a concurring or second partner review and approval of audit reports, and concurring approval in the issuance of the audit report by a qualified person other than the person in charge of the audit.
- All audit reports must describe the scope of testing of the company's internal control structure and must present the auditor's findings from the testing, including an evaluation of whether the internal control structure is acceptable, and a description of material weaknesses in internal controls and any material noncompliance with controls.

Inspections of Registered Public Accounting Firms

The Act also authorizes the Board to conduct regular inspections of public accounting firms to assess their degree of compliance with laws, rules, and professional standards regarding audits. Inspections are to be conducted once a year for firms that regularly audit more than 100 public companies and at least once every three years for firms that regularly audit 100 or fewer public companies.

Investigations and Disciplinary Proceedings

The Board has the authority to investigate registered public accounting firms (or their employees) for potential violations of the Sarbanes–Oxley Act, professional standards, any rules established by the Board, or any securities laws relating to the preparation and issuance of audit reports. During an investigation, the Board has the power to compel testimony and document production.

The Board has the power to issue sanctions for violations or for noncooperation with an investigation. Sanctions can include temporary or permanent suspension of a firm's registration with the Board (which would mean that firm could no longer legally audit publicly traded companies), temporary or permanent suspension of a person's right to be associated with a registered public accounting firm, prohibition from auditing public companies, and civil monetary penalties of up to $750,000 for an individual and up to $15,000,000 for a firm.

Dodd-Frank

The Dodd-Frank Wall Street Reform and Consumer Protection Act (generally referred to as Dodd-Frank) was signed into law on July 21, 2010, in response to the financial crisis of 2008. Major highlights of this financial reform legislation included the following:

- **Consumer Protection**—The Consumer Financial Protection Bureau, housed within the Federal Reserve system, was established to ensure that consumers receive the financial information necessary to protect them from hidden fees, abusive credit terms, and deceptive lender practices.
- **Regulate Wall Street and Reduce Big Bonuses**—A provision of this legislation gives shareholders the right to a nonbinding vote on executive pay ("say on pay") and golden parachutes.
- **End Too-Big-To-Fail Bailouts**—By imposing harsher capital and leverage requirements, Dodd-Frank seeks to discourage financial firms from becoming too large. It also develops a safe process to liquidate those firms that collapse, financially.

- **Identify and Prevent Future Financial Crises**—The Financial Stability Oversight Council was established to monitor systemic risk and take action before large, complex organizations threaten U.S. economic stability.
- **Transparency and Accountability for Complex Financial Instruments**—Closes loopholes that permit irresponsible and abusive practices for over-the-counter derivatives, asset-backed securities, hedge funds, and mortgage brokers.
- **Investor Protection**—The Credit Rating Agency-related provisions increase the agencies' liability for inaccurate ratings and give the SEC leverage in imposing sanctions and bringing cases against these agencies for material misstatements or fraud. Other noteworthy provisions within the law encourage whistleblower reports and increase SEC funding to strengthen investor protection activities.

Since the enactment of Dodd-Frank, approximately 30% of the regulations have yet to be implemented. Regulatory policy is a function of the administration and political party in power. Currently, there are areas where rollbacks of the original legislation are being considered, including adjusting the size at which banks are subject to regulatory oversight and exempting "small" banks—banks with assets of less than $100 billion—from some loan, mortgage, and trading requirements. For example, the ***Volcker Rule***, which prohibits making certain kinds of speculative investments with customers' money, would not apply to small banks.

Committee of Sponsoring Organizations' (COSO) Enterprise Risk Management Framework (ERM)

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission is a joint initiative of the American Accounting Association (AAA), the American Institute of CPAs (AICPA), the Financial Executives Institute (FEI), the Institute for Management Accountants (IMA), and the Institute of Internal Auditors (IIA). In September 2004, COSO released their ERM framework, recognized by the SEC as the critical methodology for Sarbanes–Oxley Section 404 compliance. It outlined the principles and components of effective risk management processes. Furthermore, the ERM framework describes how risks should be identified, assessed, and addressed. Interestingly, the framework emphasizes not only how effective risk management processes work but also the possibility of enhanced profitability and return as a result of process evaluation and streamlining.

The fundamental purpose of the ERM framework approach is to help entities ensure that they will be able to achieve their operational and financial objectives and goals including:

- Achieving high-level strategic goals and the entity's mission
- Effective and efficient use of the company's operational resources
- Reliability of the company's financial reporting systems
- Compliance in meeting applicable laws and regulations

- Safeguarding of company resources by preventing loss through fraud, theft, waste, inefficiency, bad business decisions, etc.

In order to achieve its objectives, the ERM framework outlines the various components of good risk management processes. Some of those components consider an entity's risk tolerance and risk appetite. Other components evaluate the entity's internal environment; its ability to set objective; the need to identify events that could have an effect on an entity's ability to achieve its objectives; its risk assessment including response; its control environment, information, communication, and its ability to monitor activities and events.

The COSO ERM Framework also has some specific suggestions for creating an antifraud environment:

- Consider and document fraud vulnerabilities
- Consider and document strategic objectives, the entity's risk appetite, risk tolerances, and consider them in the context of fraud probabilities
- Identify and document events that create risks of fraud
- Document enterprise risks by looking at the likelihood and impact of fraud vulnerabilities at all levels of the company
- Evaluate possible responses to fraud risks
- Implement and document antifraud control activities, policies, and procedures
- Communicate fraud prevention information, policies, and procedures throughout the company
- Monitor and document the success and failure of antifraud prevention controls and react to any findings

In 2017, COSO released Enterprise Risk Management–Integrating with Strategy and Performance. This new document builds on its 2004 guidance and is the first major design revision. It recognizes the evolving risks in a dynamic business environment. The updated edition is designed to help organizations create, preserve, and realize value while improving their approach to managing risk. The update, developed by PwC under the direction of the COSO Board, highlights the importance of enterprise risk management in strategic planning. It also emphasizes embedding ERM throughout an organization, as risk influences strategy and performance throughout the organization.

IIA Practice Advisories 1210.A1 and 1210.A2

Internal audit can be an integral resource in creating an antifraud environment. The Institute of Internal Auditors (IIA) has issued Practice Advisories 1210.A1 and 1210.A2 that address identification of fraud and the internal auditors' responsibility for fraud detection, respectively. The IIA standards require the internal auditor to have sufficient knowledge to identify the indicators of fraud. The standards further recognize that fraud can be perpetrated for the benefit of, or to the detriment of, the organization and by individuals outside as well as inside the organization.

Examples of frauds designed to benefit the organization include the following:

- Sale or assignment of fictitious or misrepresented assets
- Improper payments such as illegal political contributions, bribes, kickbacks, and payoffs to government officials, intermediaries of government officials, customers, or suppliers
- Intentional improper representation or valuation of transactions, assets, liabilities, or income
- Intentional improper transfer pricing (e.g., valuation of goods exchanged between related organizations)
- Intentional improper related-party transactions
- Intentional failure to record or disclose significant information to outside parties
- Prohibited business activities such as those that violate government statutes, rules, regulations, or contracts
- Tax fraud

Examples of fraud perpetrated to the detriment of the organization include the following:

- Acceptance of bribes or kickbacks
- Diversion to an employee or outsider of a potentially profitable transaction
- Embezzlement, including efforts to falsify financial records to cover up the act
- Intentional concealment or misrepresentation of events or data
- Claims submitted for services or goods not actually provided to the organization

Management and internal audit have differing roles with respect to fraud detection. The normal course of work for the internal audit activity is to provide an independent appraisal, examination, and evaluation of an organization's activities as a service to the organization. The objective of internal auditing in fraud detection is to assist members of the organization in the effective discharge of their responsibilities by furnishing them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed. The engagement objective includes promoting effective control at a reasonable cost. The IIA standards recognize that management has primary responsibility for the prevention, deterrence, and detection of fraud.

Nevertheless, in carrying out their responsibilities internal auditors should consider the following:

- Whether the organizational environment fosters control consciousness (tone at the top)
- Whether realistic organizational goals and objectives are set
- Written policies (e.g., code of conduct) and the response to policy violations
- Authorization for transactions, both existence and implementation

- Policies, practices, procedures, reports, and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas
- Communication channels provide management with adequate and reliable information
- The response to recommendations to establish or enhance cost-effective antifraud controls

When red flags are identified and the internal auditor suspects that fraud may have occurred, the appropriate levels of corporate governance should be informed. The chief audit executive has the responsibility to report immediately any significant fraud to senior management and the board. When the incidence of significant fraud has been established with reasonable certainty, senior management and the board should be notified immediately. When conducting fraud investigations, internal auditors should

- Assess the probable level and the extent of complicity in the fraud within the organization
- Determine the knowledge, skills, and other competencies needed to carry out the investigation effectively to ensure the appropriate types and levels of technical expertise
- Design procedures to identify the perpetrators, the extent of the fraud, the techniques used to perpetrate the fraud, and the underlying causes
- Coordinate activities with management personnel, legal counsel, and other specialists as appropriate
- Be cognizant of the rights of alleged perpetrators and personnel and the reputation of the organization itself

Once a fraud investigation is concluded, internal auditors should assess the facts known to determine if controls need to be implemented or strengthened to reduce future vulnerability and design engagement tests that will help to disclose the existence of similar frauds. A draft of the proposed final communications on fraud should be submitted to legal counsel for review.

THE ROLE OF CORPORATE GOVERNANCE

According to the COSO study, "Fraudulent Financial Reporting: 1998–2007," one of the critical findings was that the SEC named the CEO and/or CFO for some level of involvement in 89% of the fraud cases, up from 83% of cases in 1987−1997. Within two years of the completion of the SEC's investigation, about 20% of CEOs and/or CFOs had been indicted, and over 60% of those indicted were convicted. While the authors found relatively few **differences in** board of director characteristics between firms engaging in fraud and similar firms not engaging in fraud, 26% of the fraud firms changed auditors between the last clean financial statements and the last fraudulent financial statements; whereas, only 12% of no-fraud firms switched auditors during that same time. About 60% of the fraud firms that changed auditors did so during the fraud period, while the remaining 40% changed in the fiscal period just before the fraud began.[16]

16. See M. S. Beasley, J. V. Carcello, D. R. Hermanson, and T. L. Neal, Fraudulent Financial Reporting 1998–2007: An Analysis of U.S. Public Companies (Durham, NC: COSO, 2010).

The board of directors, the audit committee, executives, and management are responsible for the corporate governance environment in an organization.[17] The primary role of corporate governance is to protect investors, create long-term shareholder value, ensure investor confidence, and support strong and efficient capital markets.[18] Most of the board's work regarding governance is discharged through committees. To effectively carry out its primary functions, a committee must ensure its independence.

A good corporate governance environment will set the "tone at the top" by creating a culture of honesty and integrity, with the leadership of the organization practicing what they preach. As the saying goes, a fish starts to stink at the head, and if corporate leadership doesn't act in a responsible manner, it is doubtful that their subordinates will act differently.

Corporate leadership should also strive to create a positive work environment with efforts to increase employee morale, hiring, and promoting employees who follow the company's ethical guidelines, providing adequate supervision and training, and creating and monitoring antifraud programs and controls. Effective corporate governance mechanisms include:

1. Organizational code of conduct supported by an embedded culture of honesty and ethical behavior.
2. An independent and empowered board of directors.
3. An independent and empowered audit committee.
4. Organizational policies and reward systems that are consistent with espoused ethical values.
5. Confidential disclosure methods.
6. Effective legal risk assessment.

17. Readers may also want to become familiar with SEC Staff Accounting Bulletin (SAB) No. 99 on materiality and International Auditing and Assurance Standards Board ISA 240, "The Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements."

18. Zabihollah Rezaee, Corporate Governance Post-Sarbanes–Oxley: Regulations, Requirements, and Integrated Processes (Hoboken, NJ: John Wiley & Sons, 2007).

CHAPTER 3: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

1.	**Which of the following is correct regarding the criminal justice system:** **A.** few criminal cases result in convictions and incarcerations **B.** fraud cases may only be prosecuted civilly **C.** regulatory agencies do not play a role in the criminal justice system **D.** civil and criminal cases cannot be pursued simultaneously
2.	**The overriding rule regarding searches and search warrants is that individuals have which of the following:** **A.** a right to not self-incriminate **B.** an expectation of absolute privacy within their home or vehicle **C.** a reasonable expectation of privacy **D.** a right to privacy in the workplace (such as lockers, desks, etc.)
3.	**In the context of searches, the expression "fruit from the forbidden tree" means which of the following:** **A.** any information derived from confidential informants cannot be introduced if the CI has a felony record **B.** any information from evidence that was in "plain view" of law enforcement cannot be introduced **C.** any information derived from voluntary consent to search cannot be introduced **D.** any information derived from illegal evidence cannot be introduced

4.	**The Daubert standard is related to the admissibility of expert testimony (expert opinions). Under the Daubert standard, the trial judge makes an assessment of whether an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Which of the following is <u>not</u> one of the considerations in determining whether the methodology is valid:** **A.** whether the theory or technique in question can be used and has been tested **B.** whether the theory or technique in question has been verified through a double-blind study that includes a control group **C.** whether the theory or technique has been subject to peer review and publication **D.** whether the theory or technique has attracted widespread acceptance within a relevant scientific community
5.	**A search warrant has several advantages over a subpoena. Which of the following is <u>not</u> one of the advantages described by the authors:** **A.** a warrant allows the holder of the warrant, not the target of the defense counsel, to decide which documents are relevant and must be produced **B.** a warrant avoids, but does not eliminate, the possibility of the destruction of evidence **C.** a warrant gives the investigator the ability to interview key witnesses while the search is being conducted **D.** a warrant gives the investigator the ability to seize any unlawful item that may be discovered in the search if it is part of a class B (or higher) felony
6.	**Which of the following is correct regarding real evidence:** **A.** real evidence requires explanatory testimony **B.** to be admissible, real evidence must be authenticated **C.** demonstrative evidence is considered real evidence **D.** the facts at issue of a case are real evidence
7.	**Which of the following is correct regarding the best evidence rule:** **A.** copies of documents are never allowed at trial **B.** copies of documents can never be considered real evidence **C.** copies of documents can be presented at trial under certain circumstances **D.** while copies of some documents are allowable in court, copies of search warrants and public records are not

8.	**The chain of custody protects against the _____ of evidence as a result of investigators losing control of it.** **A.** shredding **B.** possible corruption **C.** leaking **D.** unauthorized distribution
9.	**Which of the following is correct regarding the civil justice system:** **A.** only the government may use the civil justice system **B.** fraud is considered a criminal, rather than civil, offense **C.** most civil actions are handled in state court **D.** fines and imprisonment are the main outcome in the civil justice system

THIS PAGE INTENTIONALLY
LEFT BLANK.

CHAPTER 3: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

1.	**A.** CORRECT. Most criminal cases never end up in the criminal justice system. This is known as the criminal justice funnel. The funnel analogy is derived from the fact that while many crimes go in the top at the wide part of the funnel, few come out at the bottom in the form of convictions and incarcerations. **B.** Incorrect. Fraud may be prosecuted criminally or civilly. **C.** Incorrect. In addition to the criminal and civil justice systems, regulatory agencies also play an important role in monitoring illegal activities and pursuing those responsible. For example, the IRS can bring actions against taxpayers in civil and/or criminal court for noncompliance with the tax code. **D.** Incorrect. Cases may be pursued criminally and civilly at the same time. *(See pages 107 to 108 of the course material.)*
2.	**A.** Incorrect. The right to not self-incriminate has to do with being interviewed, not being the subject of a search warrant. **B.** Incorrect. Citizens do not have an expectation of absolute privacy within their home or vehicle. The Fourth Amendment protects individuals against unreasonable searches and seizures. All warrants for searches and arrest must be supported by probable cause, and all warrants must be reasonably specific as to persons, places, and things. **C.** CORRECT. The overriding rule is that individuals have a "reasonable expectation of privacy." Whether a search or surveillance is reasonable is generally based on the totality of the circumstances. A search warrant based on probable cause has the effect of being reasonable. **D.** Incorrect. While individuals have a reasonable expectation of privacy in many places, such as homes and automobiles, such an expectation does not apply in the workplace. For example, items of a personal nature may be left at home and need not be stored in the confines of an office, desk, or filing cabinet. *(See page 111 of the course material.)*

3.	**A.** Incorrect. The term “fruit from the forbidden tree” does not refer to information derived from confidential informants. **B.** Incorrect. No warrant is required for evidence that is in plain view, which means that evidence can be introduced in court. **C.** Incorrect. Consent by an individual eliminates the need for a search warrant by law enforcement. Like confessions, the waiver of this right will be scrutinized to ensure that it was not coerced in any way. **D.** **CORRECT**. Illegally obtained evidence may not be introduced in court. Furthermore, any information derived from illegal evidence cannot be introduced. This is known as “fruit from the forbidden tree.” *(See page 112 of the course material.)*
4.	**A.** Incorrect. One of the considerations is whether the theory or technique in question can be used and has been tested. **B.** **CORRECT**. Under the Daubert standard, consideration does not need to be given as to whether the theory or technique in question has been verified through a double-blind study that includes a control group. **C.** Incorrect. One of the considerations under the Daubert standard is whether the theory or technique has been subject to peer review and publication. **D.** Incorrect. Whether the theory or technique has attracted widespread acceptance within a relevant scientific community is a consideration under the Daubert standard related to the admissibility of expert testimony. *(See pages 115 to 116 of the course material.)*
5.	**A.** Incorrect. One of the authors’ stated benefits of a search warrant is that it allows the holder of the warrant, not the target or the defense counsel, to decide which documents are relevant and must be produced. **B.** Incorrect. A stated benefit of obtaining a search warrant is that it avoids, but does not eliminate, the possibility of the destruction of evidence. **C.** Incorrect. According to the author, an interesting attribute of a warrant is that while the search is being conducted, it gives the investigator the ability to interview key witnesses. If handled properly, those key witnesses will not have had the opportunity to consult with counsel or prepare for the interview. **D.** **CORRECT**. Warrants giving the investigator the ability to seize any unlawful item that may be discovered in the search if it is part of a class B (or higher) felony is not a claim the authors make. *(See page 119 of the course material.)*

6.	**A.** Incorrect. Real evidence is evidence that "speaks for itself" and does not require explanatory testimony. **B.** **CORRECT**. To be admissible in court, real evidence must first be authenticated. **C.** Incorrect. Because demonstrative evidence is not real, it must not create prejudice and it must not materially alter any significant aspect of the facts at issue. **D.** Incorrect. At trial, attorneys attempt to prove facts at issue. These facts at issue are not evidence, but facts supported by evidence. *(See page 121 of the course material.)*
7.	**A.** Incorrect. Under certain circumstances, the best evidence rule allows copies to be presented at trial. **B.** Incorrect. Copies can qualify as real evidence if they are used to demonstrate that an original document was altered. **C.** **CORRECT**. While an original document is preferable, the best evidence rule allows copies to be presented at trial under certain circumstances. **D.** Incorrect. Duplicates are typically accepted if they are copies of search warrants, mortgages, lease agreements, duplicate sales slips, official documents, public records, government sealed records, summaries, testimonies, and written admissions. *(See pages 121 to 122 of the course material.)*
8.	**A.** Incorrect. The goal of the chain of custody is not to protect against the shredding of evidence. **B.** **CORRECT**. Chain of custody refers to those individuals who had possession of physical evidence and what they did with it. Essentially, fraud professionals and forensic accountants must be able to establish the origins of evidence and that the evidence has not been altered as a result of the investigation. The chain of custody protects against the possible corruption of evidence as a result of the investigators losing control of it. **C.** Incorrect. The potential leaking of evidence will not be affected by the chain of custody. **D.** Incorrect. The purpose of the chain of custody is not to minimize the unauthorized distribution of evidence. *(See page 122 of the course material.)*

9.	**A.** Incorrect. The government prosecutes criminal cases on behalf of society, including the victims. Private parties may also enter the justice system in an attempt to right a wrong or resolve a dispute through the civil justice system. **B.** Incorrect. Fraud is an example of a wrong that may enter the civil justice system; others include torts, breach of contract, breach of implied contract, negligence, and misrepresentations. **C.** **CORRECT**. Most civil actions are handled in state court in the jurisdiction of the plaintiff, the party prosecuting the civil case or the jurisdiction of the defendant. Federal courts may be used for larger cases (those involving more than $75,000 or those that are multi-jurisdictional) because the plaintiffs gain greater access to witnesses and documents due to the broad jurisdiction. **D.** Incorrect. The primary purpose of a civil action is to recover losses and possibly reap punitive damages. In fact, money and other similar damages are the main outcome in the civil justice system, not imprisonment. *(See pages 125 to 126 of the course material.)*

APPENDIX: 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 A-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.

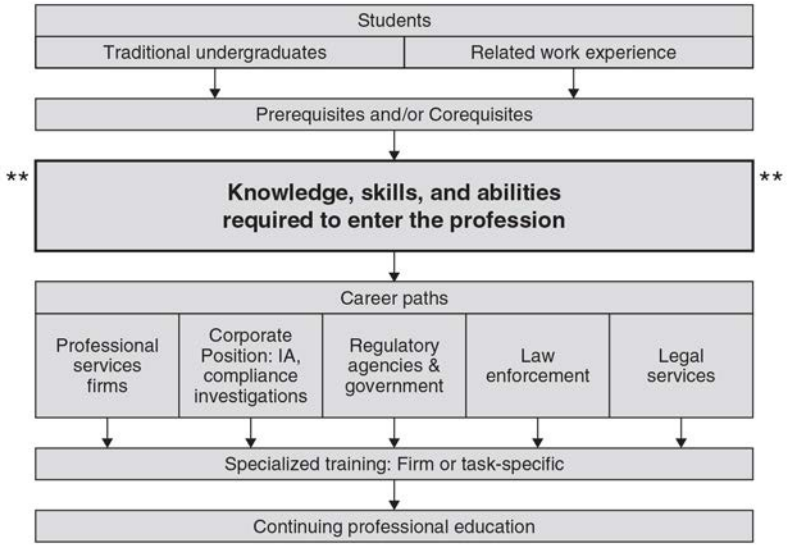
Professional Services Firms

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.

1. www.bls.gov/ooh/business-and-financial/mobile/accountants-andauditors.htm.

2. Figure A-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.

FIGURE A-1



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

Professionals with 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 2008 RTTN, fraud schemes at nonprofit and government agencies lasted approximately two years, as compared to the eighteen months they lasted at public companies. The challenges, related to fraud examination and 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 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:

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/managingbusinessrisk.pdf.

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 antimoney 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 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:

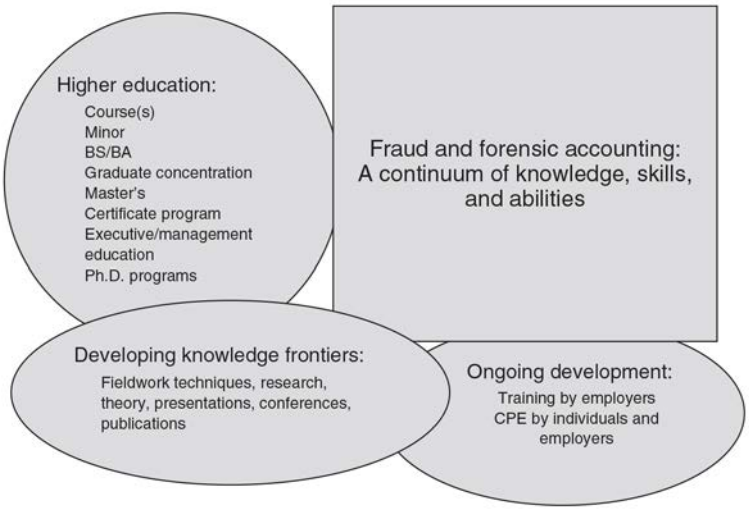
- AAFM: The American Academy of Financial Management offers sixteen separate financial certifications recognized worldwide
- MFP: Master Financial Professional
- CWM: Chartered Wealth Manager

- 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 A-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 A-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.

FIGURE A-2 FRAUD EXAMINATION AND FORENSIC ACCOUNTING. A CONTINUUM OF KNOWLEDGE, SKILLS, AND ABILITIES



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 A-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.

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.

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

Basic Auditing Concepts

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

Transaction Processing Cycles and Control Environment

- Internal control concepts and an ability to recognize potential weaknesses in a company's internal control structure
- Corporate governance and culture (e.g., tone at the top), including ethics and entity-level controls
- Operational processes and transaction flows within an organization, and tracing transactions (cash and noncash) from source documents to initial entry in the accounting system through the various 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?

GLOSSARY

Abuse: Petty crimes committed against organizations, such as excessive lunch hours or breaks, coming to work late or leaving early, using sick time when not sick, and pilfering supplies or products.

Abusive conduct: Counterproductive, fraudulent, or other activities of employees that are detrimental to the organization.

Accidental fraudster: An otherwise "good citizen" who succumbs to a perceived pressure, takes advantage of an opportunity, and is able to rationalize his or her behavior.

Altered payee scheme: check tampering scheme in which an employee intercepts a company check intended for a third party and alters the payee designation so the check can be converted by the employee or an accomplice.

Anatomical physical responses: Involuntary reactions by the body to stress. They include increased heart rate, shallow or labored breathing, and excessive perspiration. These reactions are typical clues associated with deception.

Attorney–client privilege: A right that precludes disclosure of communications between an attorney and client, but only if the client (1) retained the attorney, (2) did so to obtain legal advice, (3) thereafter communicated with the attorney on a confidential basis, and (4) has not waived the privilege.

Authorized maker scheme: A check tampering scheme in which an employee with signature authority on a company account writes fraudulent checks for his own benefit and signs his own name as the maker.

Benchmark admission: A small admission made to wrongdoing that signals a subject's willingness to confess. It is made as a result to an alternative question posed by the interviewer that gives the subject two ways to answer, either of which is an admission of culpability. Example: "Did you just want extra money, or did you do this because you had financial problems?"

Bid pooling: A process by which several bidders conspire to split contracts, thereby ensuring that each gets a certain amount of work.

Bid rigging: A process by which an employee assists a vendor to fraudulently win a contract through the competitive bidding process.

Bid splitting: A fraudulent scheme in which a large project is split into several component projects so that each sectional contract falls below the mandatory bidding level, thereby avoiding the competitive bidding process.

Billing schemes: A scheme in which a fraudster causes the victim organization to issue a fraudulent payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

Bribery: The offering, giving, receiving, or soliciting of something of value for the purpose of influencing an official act.

Business diversions: A scheme that typically involves a favor done for a friendly client. Business diversions can include situations in which an employee starts his own company, and while still employed by the victim, steers existing or potential clients away from the victim and toward the employee's new company.

Capitalized expenses: When expenditures are capitalized as assets and not expensed off during the current period, income will be overstated. As the assets are depreciated, income in subsequent periods will be understated.

Cash larceny: The theft of an organization's cash after it has been recorded in the accounting system.

Cash receipts schemes: Frauds that target incoming sales or receivables. Typically, the perpetrators in these schemes physically abscond with the victim organization's cash instead of relying on phony documents to justify the disbursement of the funds. Cash receipts frauds generally fall into two categories: skimming and cash larceny.

Certified fraud examiner (CFE): A professional who is trained to conduct complex fraud examinations from inception to conclusion. A CFE has training in all aspects of fraud examination, including identifying fraudulent transactions, obtaining evidence, and interviewing witnesses.

Chain of custody: A record of who has had possession of an item of evidence and what they've done with it. The chain of custody must be preserved or else the item cannot be used at trial.

Character testimony: A verbal clue to deception whereby an untruthful witness may attempt to add credibility to his lie by suggesting that the interviewer "check with my minister" or "ask my wife."

Check-for-currency substitution: A skimming method whereby the fraudster steals an unrecorded check and substitutes it for recorded currency in the same amount.

Check tampering: A type of fraudulent disbursement that occurs when an employee converts an organization's funds by either (1) fraudulently preparing a check drawn on the organization's account for his own benefit, or (2) intercepting a check drawn on the organization's account that is intended for a third party and converting that check to his own benefit.

Collusion: A secret agreement between two or more people for a fraudulent, illegal, or deceitful purpose, such as overcoming the internal controls of their employer.

Commercial bribery: The offering, giving, receiving, or soliciting of something of value for the purpose of influencing a business decision without the knowledge or consent of the principal.

Commission: A form of compensation calculated as a percentage of the amount of sales an employee generates. A commissioned employee's wages are based on two factors, the amount of sales generated and the percentage of those sales he or she is paid.

Comparability and consistency: Secondary qualitative characteristics that state that a company's information must be presented with the same consistent method from year to year, in order for it to be useful for analytical purposes in decision making.

Concealed check scheme: A check tampering scheme in which an employee prepares a fraudulent check and submits it, usually along with legitimate checks, to an authorized maker who signs it without a proper review.

Conflict of interest: An undisclosed economic or personal interest in a transaction by an employee, manager, or executive that adversely affects the company.

Conversion: The unauthorized assumption of a right of ownership over the goods of another to the exclusion of the owner's rights. When an employee steals company assets, he or she also converts the use of them.

Corporate Sentencing Guidelines: A U.S. federal law passed in 1991 that provides sanctions for organizations that have engaged in criminal conduct. The sanctions can be mitigated if the organization can prove that it complied with one or more of seven steps designed to prevent or deter fraud.

Covert operations: An investigatory procedure in which the investigator assumes a fictitious identity in order to gather evidence.

Deposit lapping: A method of concealing deposit theft that occurs when an employee steals part or all of the deposit from one day and then replaces it with receipts from subsequent days.

Duty of loyalty: The requirement that an employee/agent must act solely in the best interest of the employer/principal, free of any self-dealing, conflicts of interest, or other abuse of the principal for personal advantage.

Duty of reasonable care: The expectation that a corporate officer, director, or high-level employee, as well as other people in a fiduciary relationship, will conduct business affairs prudently with the skill and attention normally exercised by people in similar positions.

Economic extortion: Obtaining property from another with the other party's "consent" having been induced by using threats of economic reprisal.

Employee deviance: Conduct by employees that is detrimental to both employer and employee, such as goldbricking, work slowdowns, and industrial sabotage.

Evidence: 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.

Excuse clause: A clause inserted in a signed statement that encourages the confessor to sign the statement. It offers a moral, not legal, excuse for the wrongdoing. Example: "I wouldn't have done this if it had not been for pressing financial problems. I didn't mean to hurt anyone."

False (fictitious) refund scheme: One of two main categories of register disbursements. A scheme in which a fraudulent refund is processed at the cash register to account for stolen cash.

False void scheme: One of two main categories of register disbursements. A scheme in which an employee accounts for stolen cash by voiding a previously recorded sale.

Fictitious expense reimbursement schemes: A scheme in which an employee seeks reimbursement for wholly nonexistent items or expenses.

Fictitious revenue: The recording of sales of goods or services that never occurred.

Fiduciary relationship: In business, it is the trusting relationship that the employee is expected to hold toward the employer, requiring the employee's scrupulous good faith to act in the employer's best interests.

Financial statement fraud: A type of fraud where an individual or individuals purposefully misreport financial information about an organization in order to mislead those who read it.

Fleeing position: A posture adopted by an individual under stress during an interview. The head is facing the interviewer, while the feet and legs are pointed toward the door in an unconscious effort to flee the interview.

Force balancing: A method of concealing receivables skimming whereby the fraudster falsifies account totals to conceal the theft of funds. This is also sometimes known as "plugging." Typically, the fraudster will steal a customer's payment but nevertheless post it to the customer's account so that the account does not age past due. This causes an imbalance in the cash account.

Forced reconciliation: A method of concealing fraud by manually altering entries in an organization's books and records or by intentionally miscomputing totals. In the case of noncash misappropriations, inventory records are typically altered to create a false balance between physical and perpetual inventory.

Forged endorsement scheme: A check tampering scheme in which an employee intercepts a company check intended for a third party and converts the check by signing the third party's name on the endorsement line of the check.

Forged maker scheme: A check tampering scheme in which an employee misappropriates a check and fraudulently affixes the signature of an authorized maker thereon.

Forgery: The signing of another person's name to a document (such as a check) with a fraudulent intent, or the fraudulent alteration of a genuine instrument.

Fraud: Any crime for gain that uses deception as its principal modus operandi. There are four legal elements that must be present: (1) a material false statement, (2) knowledge that the statement was false when it was uttered, (3) reliance on the false statement by the victim, and (4) damages as a result.

Fraud deterrence: Discouraging fraudulent activities through the threat of negative sanctions.

Fraud examination: A process of resolving allegations of fraud from inception to disposition. It involves not only financial analysis, but also taking statements, interviewing witnesses, writing reports, testifying to findings, and assisting in the detection and prevention of fraud.

Fraud prevention: Removal of the root causes of fraudulent behavior, such as economic deprivation and social injustices.

Fraud risk: Risk of material misstatements in financial statements arising from fraudulent financial reporting and misappropriations of assets.

Fraud theory approach: The methodology used to investigate allegations of fraud. It involves developing a theory based on a worst-case scenario of what fraud scheme could have occurred, then testing the theory to see whether it is correct.

Fraud triangle: A model developed to explain the research of Cressey, who noted that most occupational frauds were caused by a combination of three elements: non-shareable financial problems, perceived opportunity, and the ability to rationalize conduct.

Fraudulent disbursements: Schemes in which an employee illegally or improperly causes the distribution of funds in a way that appears to be legitimate. Funds can be obtained by forging checks, submission of false invoices, or falsifying time records.

Fraudulent write-offs: A method used to conceal the theft of noncash assets by justifying their absence on the books. Stolen items are removed from the accounting system by being classified as scrap, lost or destroyed, damaged, being bad debt, scrap shrinkage, discount and allowances, returns, etc.

Full disclosure: A standard for financial reporting that states that any material deviation from generally accepted accounting principles must be explained to the reader of the financial information. Any potential adverse event must be disclosed in the financial statements.

Generally accepted accounting principles: Recognition and measurement concepts that have evolved over time and have been codified by the Financial Accounting Standards Board and its predecessor organizations. The standards serve to guide regular business practices and deter financial statement fraud.

Ghost employee: An individual on the payroll of a company who does not actually work for the company. This individual can be real or fictitious.

Horizontal analysis: A technique for analyzing the percentage change in individual financial statement items from one year to the next.

Illegal gratuities: The offering, giving, receiving, or soliciting of something of value for, or because of, an official act.

Illustrators: Motions made primarily by the hands to demonstrate points when talking. The use of illustrators usually changes during deception.

Imperative ethical principle: The school of ethical thought advocating concrete ethical principles that cannot be violated (e.g., the end does not justify the means).

Improper asset valuation: Generally accepted accounting principles require that most assets be recorded at their historical (acquisition) cost with some exceptions. This type of fraud usually involves the fraudulent overstatement of inventory or receivables or the misclassification of fixed assets.

Kickbacks: Schemes in which a vendor pays back a portion of the purchase price to an employee of the buyer in order to influence the buyer's decision.

Lapping: A method of concealing the theft of cash designated for accounts receivable by crediting one account while abstracting money from a different account. This process must be continuously repeated to avoid detection.

Larceny: The unlawful taking and carrying away of the property belonging to another with the intent to convert it to one's own use.

Liability/expense omissions: Deliberate attempts to conceal liabilities and expenses already incurred.

Maker: The person who signs a check.

Manipulators: Motions made by individuals such as picking lint from clothing, playing with objects such as pencils, or holding one's hands while talking. Manipulators are displacement activities, done to reduce nervousness.

Mischaracterized expense scheme: An attempt to obtain so that the perpetrator is reimbursed for an amount greater than the actual expense.

Multiple reimbursement schemes: An attempt to obtain more than one reimbursement for the same business-related expense.

Need recognition scheme: A pre-solicitation-phase bid-rigging conspiracy between the buyer and contractor where an employee of the buyer receives something of value to convince his company that they have a "need" for a particular product or service.

Non-shareable problems: Financial difficulties that would be hard for a potential occupational offender to disclose to outsiders, such as excessive debt, gambling, drug use, business reversals, or extramarital affairs.

Norming or calibrating: The process of observing behavior before critical questions are asked. The purpose is to help assess the subject's verbal and nonverbal reactions to threatening questions.

Oaths: Certain phrases used frequently by liars to add weight to their false testimony. Examples include "honestly," "frankly," "to tell the truth," and "I swear to God."

Occupational fraud and abuse: he use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

Off-book fraud: A fraud that occurs outside the financial system and therefore has no direct audit trail. Several kinds of off-book frauds are discussed in this book. Skimming is the most common off-book fraud.

Official act: The decisions or actions of government agents or employees. Traditionally, bribery statutes proscribed only payments made to influence public officials.

Organizational controls: Deterrence mechanisms used by organizations to discourage employee deviance and fraud, which include company policy, selection of personnel, inventory control, security, and punishment.

Overpurchasing: A method of overstating business expenses in which a fraudster buys two or more business expense items at different prices (such as airline tickets). The perpetrator returns the more expensive item for a refund but he claims reimbursement for this item. As a result, he is reimbursed for more than his actual expenses.

Overstated expense reimbursements: Schemes in which reimbursement for personal expenses by claiming they are business-related expenses are inflated on an expense report.

Overstated refund scheme: A false refund scheme in which an employee overstates the amount of a legitimate customer refund, gives the customer the actual amount of the refund, and steals the excess.

Overstatements: Type of financial statement fraud in which an individual exaggerates a company's assets or revenues to meet certain objectives.

Pass-through scheme: A subcategory of a shell company scheme in which actual goods or services are sold to the victim company, with the fraudster acting as middleman and inflating the prices of the goods or services.

Pay-and-return scheme: A fraud in which an employee intentionally mishandles payments that are owed to legitimate companies, then steals the excess payments when they are returned by the vendor.

Perception of detection: The thought in the employee's mind that his or her fraudulent conduct will be discovered.

Periodicity: A "time period" assumption, which deems that economic activity be divided into specific time intervals, such as monthly, quarterly, and annually.

Perpetual inventory: A method of accounting for inventory in the records by continually updating the amount of inventory on hand as purchases and sales occur.

Personal purchases scheme: category of billing scheme in which an employee simply buys personal items with his company's funds or credit card.

Physical inventory: A detailed count and listing of merchandise on hand.

Physical padding: A fraud concealment scheme in which the fraudsters try to create the appearance that there are more assets on hand in a warehouse or stockroom than there actually are (e.g., by stacking

empty boxes to create the illusion of extra inventory).

Predator: A fraudster who continuously seeks out victims to defraud.

Purchasing scheme: Conflict of interest scheme in which a victim company unwittingly buys something at a high price from a company in which one of its employees has a hidden interest.

Ratio analysis: A means of measuring the relationship between two different financial statement amounts.

Rationalization: The process by which an occupational fraudster explains and justifies his or her illegal conduct. Examples include: “I was only borrowing the money,” “The company doesn’t treat me fairly,” “I must commit financial statement fraud because otherwise, employees will lose their jobs.”

Receivables skimming: A type of skimming scheme that involves the theft of incoming payments on accounts receivable. This form of skimming is more difficult to detect than sales skimming because the receivables are already recorded on the victim organization’s books. In other words, the incoming payments are expected by the victim organization. The key to a receivables skimming scheme is to conceal either the fact that the payment was stolen or the fact that the payment was due.

Related-party transactions: Occur when a company does business with another entity whose management or operating policies can be controlled or significantly influenced by the company or by some other party in common. There is nothing inherently wrong with related-party transactions, as long as they are fully disclosed.

Relevance and reliability: Primary qualitative characteristics of financial reports as they relate to usefulness for decision making. Relevance implies that certain information will make a difference in arriving at a decision. Reliability means that the user can depend on the factual accuracy of the information.

Resource diversions: Unlike business diversions, resource diversions consist of diverting assets from the victim company.

Reversing transactions: A method used to conceal cash larceny. The perpetrator processes false transactions to void a sale or refund cash, which cause sales records to reconcile to the amount of cash on hand after the theft.

Rubber stamp supervisor: A supervisor who neglects to review documents, such as timecards, prior to signing or approving them for payment.

Salaried employees: mployees who are paid a set amount of money per period (weekly, two-week period, monthly, etc.). Unlike hourly employees, salaried employees are paid the same regardless of the actual number of hours they work.

Sales scheme: Conflict of interest scheme in which a victim company unwittingly sells something at a low price to a company in which one of its employees has a hidden interest.

Sales skimming: type of skimming scheme that involves the theft of sales receipts, as opposed to

payments on accounts receivable. Sales skimming schemes do not cause an imbalance in the victim organization's books because the sales transaction is not recorded.

Search warrant: A legal order issued by a judge upon presentation of probable cause to believe the items being sought have been used in the commission of a crime.

Shell company: A fictitious entity created for the sole purpose of committing fraud.

Shrinkage: The unaccounted-for reduction in an organization's inventory that results from theft and is a common red flag of fraud.

Skimming: The theft of cash prior to its entry into the accounting system.

Slush fund: A noncompany account into which company money has been fraudulently diverted and from which bribes may be paid.

Social controls: Informal deterrence mechanisms that help discourage employee deviance and fraud, such as loss of prestige and embarrassment to friends and family.

Specifications scheme: A pre-solicitation-phase bid-rigging conspiracy between the buyer and vendor where an employee of the buyer receives something of value to set the specifications of the contract to accommodate that vendor's capabilities.

Subpoena duces tecum: A legal order requiring the production of documents.

Surveillance: An evidence gathering technique involving the secretive and continuous observance of a suspect's activities.

Turnaround sales: A purchasing scheme where an employee knows his company plans to purchase a certain asset, takes advantage of the situation by purchasing the asset himself, and then sells the asset to his employer at an inflated price.

Unconcealed larceny: Schemes in which an employee steals an asset without attempting to conceal the theft in the organization's books and records.

Underbilling: A sales scheme that occurs when an employee underbills a vendor in which she has a hidden interest. As a result, the company ends up selling its goods or services at less than fair market value, which creates a diminished profit margin or loss on the sale.

Understated sales: Variation of a sales skimming scheme in which only a portion of the cash received in a sales transaction is stolen. This type of fraud is not off-book because the transaction is posted to the victim organization's books, but for a lower amount than what the perpetrator collected from the customer.

Understatements: Type of financial statement fraud in which an individual minimizes a company's liabilities or expenses to meet certain objectives.

Utilitarian ethical principle: The school of ethical thought that advocates situational ethics—each behavior should be evaluated on its own merits (e.g., the end justifies the means).

Vertical analysis: The relationship or percentage of component part items to a specific base item.

Vicarious or imputed liability: A legal theory that holds the organization liable for the criminal conduct of its employees.

Wages-in-kind: A concept that deals with the motivations of employees to correct what they perceive as workplace “wrongs” by means of counterproductive behavior, including fraud and abuse.

White-collar crime: Term coined by Edwin Sutherland. Originally, the definition included criminal acts only of corporations and individuals acting in their corporate capacity (e.g., management fraud or crime). However, it is now used to define almost any financial or economic crime.

INDEX

D

E

F

G

H

About the Authors

Mary-Jo Kranacher is a certified public accountant (CPA), certified fraud examiner (CFE), and certified in financial forensics (CFF). She is the ACFE Endowed Professor of Fraud Examination at York College, CUNY, an ACFE Regent Emeritus, and former ACFE Higher Education Committee Chairperson. She was the Editor-in-Chief of The CPA Journal, published by the New York State Society of CPAs, from January 2006 through June 2013.

Professor Kranacher has written scores of articles and delivered dozens of antifraud presentations at conferences and seminars for professional, governmental, and academic organizations, including: the Association of Certified Fraud Examiners (ACFE), American Accounting Association (AAA), Institute of Management Accountants (IMA), Institute of Internal Auditors (IIA), Internal Revenue Service (IRS), New York Association of Government Accountants (NYAGA), New York Internal Control Association (NYICA), New York Certified Fraud Examiners (NYCFE), various state CPA societies, Fortune 500 companies, and U.S. and international academic universities. She conducts antifraud consulting engagements and also develops and implements fraud detection and deterrence training programs for international business and government delegations.

She coauthored *Forensic Accounting and Fraud Examination* with Richard A. (Dick) Riley, Jr. and Joseph T. Wells (John Wiley & Sons, 2010), and served on a West Virginia University research project, funded by the U.S. Department of Justice, which culminated in the development of a model curriculum for fraud and forensic accounting education.

Professor Kranacher has been recognized for her work with the following awards: 2009 ACFE Educator of the Year; 2010 York Alumni Distinguished Faculty; 2010 Fraud Magazine Columnist Recognition; 2012 ACFE Hubbard Award; and 2013 KPMG-AAA Competitive Manuscript Award for Best Research Paper.

Richard A. (Dick) Riley, Jr., is the Louis F. Tanner Distinguished Professor of Public Accounting at West Virginia University. He is also the Director of Research for the Institute for Fraud Prevention. Since 2002, Dr. Riley has performed expert financial analysis and litigation support services, offering deposition and trial testimony. He has published four books: Financial Statement Fraud: Prevention and Detection with Zabi Rezaee (John Wiley & Sons, 2010); Forensic Accounting and Fraud Examination with Joseph Wells and Mary-Jo Kranacher (John Wiley & Sons, 2011); Fraud Examination for Fraudulent Financial Reporting with Steven Albrecht, Chad Albrecht, and Mark Zimbelman (MyEducator.com, 2015); Forensic Accounting and Fraud Examination: Knowledge, Skills, and Abilities with Richard Dull (WVU Press, 2015). Dr. Riley has been recognized nationally for his contributions in forensic accounting and fraud examination: The Association of Certified Fraud Examiners (ACFE) 2008 Educator of the Year; 2012 ACFE Hubbard Outstanding Achievement Award; 2009 American Accounting Association Innovations in Accounting Education Award; The 2013 Max Block Award from the CPA Journal; the 2013 American Accounting Association FIA Section Outstanding Research Manuscript. In 2013, the West Virginia University Foundation recognized him for his outstanding teaching, the highest recognition for teaching at WVU. In 2014, Dr. Riley was recognized by the WV Society of CPAs as Educator of the Year and by Wheeling Jesuit University for his service to the institution. In 2015, WVU College of Business & Economics presented him with the Dean's Special Recognition for the Coursera MOOC and 21,600

participating students (with Richard Dull). Dr. Riley is a CPA, CFE, CFF, CVA, forensic accountant, and fraud examiner who has developed and implemented fraud and forensic accounting education programs for the United States National Institute of Justice and the Internal Revenue Service. Dr. Riley possesses an undergraduate degree in accounting from Wheeling Jesuit University, a Masters of Professional Accountancy from West Virginia University, and Doctor of Philosophy Degree from the University of Tennessee. In spring 2017, WV Governor Justice appointed Dr. Riley to the WV State Board of Accountancy.