CHAPTER ONE

1

# Understanding Fraud

## *What Is Fraud, and Why Does It Continue to Happen?*



What kind of society isn't structured on greed? The problem of social organization is how to set up an arrangement under which greed will do the least harm; capitalism is that kind of a system.

—*Milton Friedman, economist*

This chapter introduces you to fraud and helps you to understand why it happens so you can develop a proper foundation on which to learn how to prevent, deter, and detect it. Fraud is first and foremost a people problem, as discussed in the Introduction. Flawed processes may support its continued existence, but processes are only part of the environment in which fraud occurs. Processes do not commit fraud, people do. This chapter does not discuss common or traditional criminological studies but instead focuses on the human element involved

in analyzing fraud within an organization so we can determine what fraud is and why it continues to happen in today's organizations.

This chapter features the following:

- Fraud's many definitions.
- The value of informed skepticism.
- How to apply critical thinking when reviewing fraud.
- Discussions of confusion about responsibility and complexity.

---

TO BETTER UNDERSTAND THE MANY definitions of fraud, we begin our journey by learning what fraud looks like and why you need to ask many questions to gain a clear picture of the facts. You need to begin looking through a different set of eyes: not your own, but those of the fraudster.

## PEOPLE ARE GREEDY—HOW GREEDY ARE YOU?

Think about the people in your organization who have access to its financial resources and the value (money or otherwise) that is at risk with informed skepticism. Make sure the facts and findings support the organization's people in trusted positions. The value of informed skepticism lies in the level of details that support your findings. This will aid you in your fraud analysis. Think divergently and develop as many potential facts as possible. Always remain objective and independent in your thinking and apply sound principles. Remember to think *people*! People are at the heart of fraud, and critical thinking should be applied to the daily organizational processes from top to bottom.

The people in the organization are the front line of fraud defense. Fraud can begin and end with them. A fraud-conscious organization should have clearly defined roles and responsibilities for all economic activities down to specific individual tasks. People in the organization cannot be allowed to create confusion about responsibility. A fraudster generally creates confusion to deflect attention from the fraud he or she is committing. People who have access to the value of an organization need to understand their trusted responsibility in order to help detect, deter, and prevent fraud. Their responsibilities must be communicated effectively by management so they understand them. The organizational process often requires various skills in order to accomplish the desired results. The lack of a full understanding of the desired results is a breeding ground for potential fraud.

To understand the complexities that exist in an organization, start with the idea that no two people think alike. This in itself requires the development

of flexibility within the established principles and rules of an organization. Everything, including people, is constantly changing on a day-to-day basis. Organizations need to monitor and analyze the people in the processes on a daily basis.

This may not be practical, yet it is imperative that the organization create an environment in which its people know that monitoring and analysis is ever present. No one acknowledges the 800-pound friendly gorilla, but everyone feels its presence. The need for daily monitoring and analysis is too big a job for one person. This is why an organization needs to make sure that all of its people have the 800-pound friendly gorilla mind-set to create effective communication through a friendly rather than aggressive approach.

A successful organization needs to be firm and flexible at the same time. It is important for an organization to maintain enough strength to prevent fraud yet maintain enough flexibility to deal with its multiple complexities. The organization will need to confront the gray areas as well as conflicts that may arise on an ongoing basis by paying attention to questions such as the following:

- Has the organization set reasonable expectations and goals for the responsibilities of its people?
- Do the incentives communicated to the people in the organization maintain ethical behavior, or do they promote greed?
- Is there an opportunity for conflicts of interest to exist in the organizational process?

Management needs to maintain effective communication with its people and its processes to ensure that gray areas are addressed before they become fraud. It is important that the people in an organization understand the incentives and potential conflicts of interest in a proper context and act in accordance with the established organizational rules and principles—not their own rules and principles.



## ONE-MINUTE FRAUD MYSTERY: TRUST US INC.

This one-minute fraud mystery is designed to help you begin thinking divergently ("outside the box") so you learn how to develop solutions under less than ideal circumstances. Think about the situation presented here as you read the rest of the chapter.

You are the owner of Trust Us Inc. Betty Favor, one of the organization's most trusted employees, has worked there for 15 years. She socializes with

you on a regular basis. Recently, you hired a young new accountant who just graduated from college with honors in accounting. This new employee, John Asset, tells Betty that the bank statement does not reflect the same bank balance as the bank reconciliation that he just prepared.[1] Previously, Betty had taken care of all banking matters and prepared the bank reconciliations. Betty comes into your office and says it appears that John does not know what he is doing because there are errors on the bank reconciliation. She states that she redid the bank reconciliation to fix the error.

Do you think Trust Us Inc. is vulnerable to fraud? If so, where is the fraud, and how was it perpetrated? What is your approach to solving this mystery?

## DISTINGUISHING AMONG DETERRENCE, PREVENTION, AND DETECTION

In an Associated Press article about the sentencing of former attorney Mather Kluger for insider trading, Assistant U.S. Attorney Nolan Germano stated, "He had wealth, intelligence, and family support. He abused it all. Why? Because he could."[2]

Exhibit 1.1 illustrates this dynamic.

The theme of the dialogue in Exhibit 1.1 is that the strength of the 800-pound friendly gorilla in the room is not more effective than calm rationale in dealing with the club-wielding caveman. The theme of the dialogue in Exhibit 1.1 is a theme that is maintained throughout the book. The strength of the 800-pound gorilla needs to be friendly rather than imposing. The 800-pound friendly gorilla applies a relaxed, open, and transparent process, creating the necessary communication whether the fraud has already occurred or is in the process of being detected, deterred, and prevented. If the gorilla were to verbally attack the already defensive caveman, he would not get anywhere and would probably get clubbed. In this cartoon, there was no deterence and the 800-pound friendly gorilla was performing a postmortem analysis to understand the fraud. If an organization is to create 800-pound friendly gorillas, the objective is to make people feel comfortable in discussing the facts before the fraud occurs and not after the fact.

Frauds are typically simple. The role of the fraud investigator (I use fraud investigator, detector, or examiner interchangeably throughout the book) is to assist those who are determining the facts in reaching either a conclusion of fraud or no fraud. The 800-pound friendly gorilla fraud detectors can be internal auditors, external auditors, outside forensic consulatants, organizational management, boards of directors, audit committees, internal or external




**EXHIBIT 1.1** The 800-Pound Friendly Gorilla Interview

Gorilla: Please, Mr. Caveman, make yourself comfortable.
Caveman: Wow, you sure look strong! [*Reaches for club*].
Gorilla: That won't be necessary.
Caveman: Well, all right. [*Pulls hand back*].
Gorilla: Just want to have a conversation. I see you brought a club with you. I hope you don't intend on using it.
Caveman: Of course not.
Gorilla: So . . . how did you commit the fraud?
Caveman: I used my club.
Gorilla: So why did you commit the fraud?
Caveman: Because I could.

attorneys, or other specialzed consultants. A fraud investigator obtains sufficient and relevant information about the event or allegation to enable a judge and/or jury to reach a conclusion. The fraud investigator should not offer an opinion on whether fraud has been committed. Only a court of law may determine a person's guilt or innocence. If the fraud examiner offered an opinion that proved to be inaccurate, he or she would be vulnerable to a defamation suit.

Developing effective interview techniques is critical in creating open channels of communication in a fraud investigation. Contrary to what many may think, interviewing and interrogating are very different concepts. The mission of the 800-pound friendly gorilla is fact finding through interviewing techiques and not to make a determination of guilt. The interrogation is designed to make a deremination of guilt and is much more aggressive than our 800-pound friendly gorilla approach. What is key is to obtain the propeer facts. What kind of information is necessary to understand the facts that will establish supportable findings? Think about things like what happened, where it happened, when and why it happened (although intent is difficult to determine independently), how it happened, how much was taken, who had the opportunity, who helped it to happen, and what is necessary to enable the fact finder (judge or jury) to support a final conclusion about the fraud.



An organization's goal is to make a profit. When the organization hires people, the assumption is that they will have the organization's same goals and best interests at heart. This is the start of the need for controls as the goals and best interests between organization and employee often differ.

Much has been written about what fraud is, how it occurs, what the trends are among those committing or who are trying to commit fraud, and the importance of the "tone at the top" principle when attempting to prevent the flow of fraud. Tone at the top refers to the atmosphere created by the organization's leaders in terms of ethics. If the people at the top are unethical, then the people throughout the rest of the organization are likely to be unethical as well. Antifraud programs are typically defined as deterrence, prevention, or detection tasks, but what exactly do these mean, and how are they distinguishable?

**Fraud deterrence** refers to tasks or barriers designed to discourage those with a temptation to commit fraud from doing so. Example: the threat of imprisonment, job loss, and the fear of becoming a social outcast.

**Fraud prevention** refers to methods and strategies used to prevent those not deterred from succeeding in committing a fraud. Example: requiring two signatures on checks.

**Fraud detection** describes the methodologies deployed to investigate allegations of fraud. It is more reactive than proactive.

The goal of a fraud investigation is to obtain sufficient and relevant information about the event or allegation to enable the fact finder (judge or jury) to arrive at a credible conclusion of whether a fraud occurred, how it occurred, and who the potential perpetrator was. Throughout the book, I emphasize that the fraud investigator's role is not to proclaim the alleged perpetrator innocent or guilty but only to develop the facts to enable a court to determine whether fraud, in fact, exists and to help the organization develop an understanding of how to prevent fraud in the future. The AICPA Code of Professional Conduct, General Standards rule 201 states that "sufficient relevant data" may be obtained "to afford a reasonable basis for conclusions or recommendations in relation to any professional services performed." This requirement is not only necessary for compliance with many organizations' professional standards, but it also establishes acceptable practices within the industry standards.

Entities that rely on reactionary postures and wait for suspicions to arise are more susceptible to fraud. Sound fraud risk policy requires that ongoing standing procedures are in place to address deterrence, prevention, and detection simultaneously with the aid of our 800-pound friendly gorilla oversight.

Unfortunately, there are no systems, procedures, policies, or other mechanisms to deploy that provide a perfect guarantee against fraud. Both good and bad economies provide motivation for the potential fraudster. As long as there are people with access to money and other items of value that belong to someone else, there will always be a risk of fraud to manage. It is the vulnerable areas within an organization that need to be exposed and understood in order to deter, prevent, and detect fraud. Proactive rather than reactive fraud management is critical in the fight against organizational fraud.



## Defining Fraud

To understand the process of fraud prevention, deterrence, and detection, let's look at a sampling of relevant definitions of fraud:

- "Deceit, trickery; *specifically*: intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right. . . . An act of deceiving or misrepresenting."[3]

- "A deception deliberately practiced in order to secure unfair or unlawful gain."[4]
- "It usually consists of a misrepresentation, concealment . . . of a material fact, or at least misleading conduct. . . . It embraces all the multifarious means which human ingenuity can devise to get an advantage over another."[5]
- "Deception by misrepresentation of material facts, or silence when good faith requires expression, resulting in material damage to one who relies on it and has the right to rely on it. Simply stated, it is obtaining something of value from someone else through deceit."[6]
- "An intentional act that results in a material misstatement in financial statements that are the subject of an audit. . . . There are two types of fraud: misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets."[7]
- "Any intentional or deliberate act to deprive another of property or money by guile, deception or other means."[8]
- "Any illegal acts characterized by deceit, concealment or violation of trust . . . not dependent upon the application of threat of violence or of physical force . . . to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."[9]



The common theme of these definitions is that fraud occurs when there is an intentionally deceptive act that results in another party losing something of value. (The AICPA definition—the fifth one in the list—is remarkable, however, because unlike the other definitions, it is not contingent on another party's financial loss.) Intention is largely, but not exclusively, what distinguishes fraud from error. Intention needs to be aligned with motive. Fraudsters will avoid the appearance of intent by making the act appear to be an accident or a mistake. The 800-pound friendly gorilla understands the motivation driving the act.

Each of the above definitions states a necessary action to be performed. The 800-pound friendly gorilla studies the actions of the people in trusted positions in the organization to ensure proper ethical behavior. Fraud occurs when a material fact is intentionally misrepresented and a party who was known to be relying on that representation is harmed as a result. An acronym—discussed in more detail later in this chapter—that may help you to remember these elements is MIRD, which stands for *misrepresentation*, *intention*, *reliance*, and *damage*.

Fraud is instantly recognizable, yet it remains ambiguous because of the difficulty in proving intent and the underlying motive behind the action. A proactive approach to prevention and deterrence is necessary to mitigate fraud

risk. Only by getting ahead of potential fraud problems will an organization maximize its shareholder value.[10] Knowing the generally accepted definitions of fraud will not stop fraud. Awareness of popular theories that attempt to explain why individuals commit fraud will do only so much to prevent or deter fraud; having our 800-pound friendly gorilla monitoring the activities and actions of the people in the organization will be effective.

The only way to manage fraud risk effectively is by identifying value within an organization and protecting that value by using a methodology or an approach specific to the organization. There is no way to definitively predict who among an organization's stakeholders (anyone with an interest in the organization, current or future) is likely to try to commit fraud, and there is no one-size-fits-all method to prevent its occurrence. Organizations are unique in terms of structure and staffing, and individuals are unique as well, so there is no uniform system that can capture each fraud before it is committed. Each organization's situation needs to be examined on its own merits, and a solution must be tailored to meet the organization's needs based on its unique characteristics and the characters involved. Einstein said, "Human beings must have action; and they will make it if they cannot find it."[11] The 800-pound friendly gorilla makes sure that people in an organization have assigned responsibilities with assigned accountability.



## Classification Systems

Frauds are usually classified in terms of how they were committed. The ACFE has a model for categorizing known fraud schemes. This model is usually referred to as the "fraud tree," even though it resembles more of an organizational chart.[12] The methodology employed in Exhibit 1.2 classifies frauds primarily as involving corruption, asset misappropriation, and fraudulent statements and secondarily by the manner in which the plot is carried out.

The study of fraud—its causes and prevention—is still relatively new. ACFE's *2010 Report to the Nations* appears to be moving away from its traditional model, having refined and broadened the principal categories to include the following:

- Misrepresentation or concealment of material facts
- Bribery and extortion
- Forgery and theft (money, property, or trade secrets)
- Breaches of fiduciary duty
- Conflicts of interest
- Statutory offenses[13]

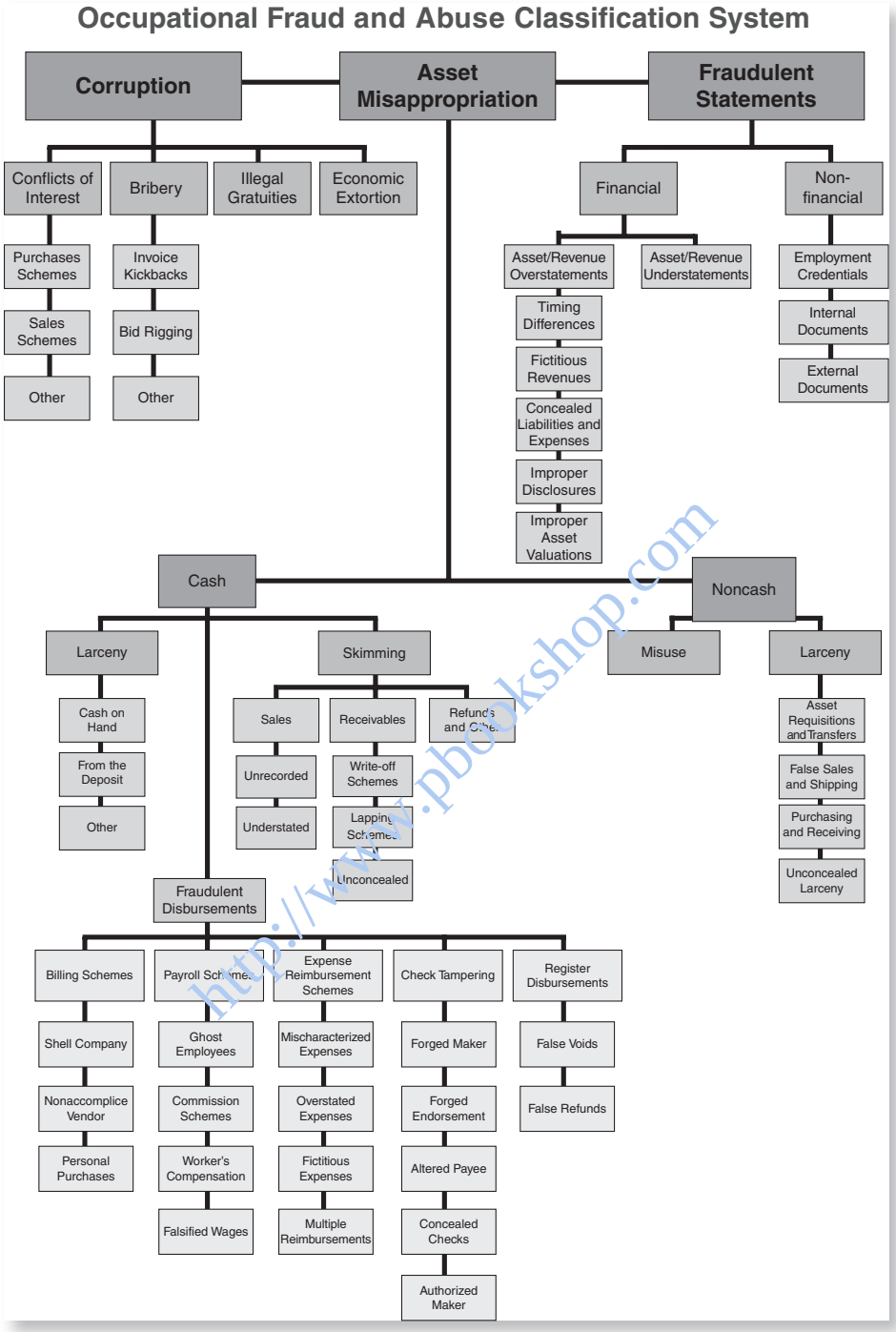




**EXHIBIT 1.2** ACFE's Fraud Tree

Source: Association of Certified Fraud Examiners, *2010 Report to the Nations*

The Institute of Internal Auditors analyzes fraud by the following types of risk:

- **Financial reporting risk.** Includes not just earnings management (like overstating assets or revenues and understating liabilities or expenses) but also financial misconduct by members of the board of directors or senior management.
- **Operational risk.** Addresses obtaining revenues and assets by fraudulent means in addition to using illicit tactics to avoid incurring expenses (such as committing tax fraud to reduce tax expenses).
- **Compliance risk.** Expenditures or liabilities are incurred for improper purposes (like corrupt practices) or asset misappropriation through embezzlement of funds or other company resources.

These various types of fraud use simple stealth measures that are like a small mosquito bite, and as long as there is no interest or outrage created, they often remain undetected. Most people perceive a mosquito bite as nothing more than a nuisance, but it can spread malaria (accounting for 2 to 3 million human deaths a year) and West Nile virus with its bite. Embezzlements, unless a large dollar amount is involved, often go undetected because the organization is not watching closely enough. Often it is not until the embezzlement significantly impacts the organization that the act is brought to light, much like the effect of a mosquito bite. An organization with an 800-pound friendly gorilla has a zero-tolerance policy for fraud, so the "mosquito bites" merely remain a nuisance and do not negatively affect the organization.

Organizations may avoid fraud if they have an eye toward preventing it, rather than merely dealing with fraud when it happens. Those who do not act to prevent fraud before it happens often think that they are not likely to be victims of fraud. They ignore the possibility that fraud can happen by mistakenly relying on their auditors to find fraud, believing that their people are trustworthy, and insisting that they have insurance. But even the smallest fraud left unattended can have a devastating effect on an organization.



## Why People Commit Fraud

There is no shortage of criminological studies that explain what causes individuals to choose to commit fraud. For the purposes of this book, an in-depth analysis of these theories is not necessary. Instead I offer some geometric analogies as a means of explaining fraud.

The *fraud triangle* was introduced in 1953 as part of a sociological study on embezzlement. It states that fraud is likely to occur when three elements are present:

1. **Pressure** or nonsharable need (generally financial in nature)
2. **Rationalization** (enabling an otherwise honest individual to commit a dishonest deed)
3. **Opportunity** (in terms of the skills to conduct the illicit act as well as the means or situational presence to effectuate the crime)[14]

In 2004, the *fraud diamond* expanded the triangle by maintaining the pressure and rationalization elements but separating the opportunity element into competence (or capability) and situation (weak internal controls).[15]

The *fraud pentagon* created a five-sided analysis by introducing arrogance as the fifth element of an environment at high risk for fraud. The pentagon is premised on the following:

> An employee's competence or power to perform and arrogance or lack of conscience [existing alongside] the conditions generally present when fraud occurs. Competence expands on [the] element of opportunity to include an individual's ability to override internal controls and to socially control the situation to his or her advantage. 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 personally apply.[16]



The existence of the five elements—pressure, rationalization, competence, situation, and arrogance—may lead to the commission of fraud if proper checks and balances are not in place. The main way in which an organization has direct control is by putting in place the necessary regulations and tools that the 800-pound friendly gorilla can use to detect a fraud structure. "Adept individuals with widespread access to corporate information, a mindset of entitlement, and the confidence to pull it off can compound the risk for fraud. Moreover, placing these individuals in a culturally lax environment with a poor tone at the top and weak internal controls is a recipe for disaster."[17]

These theories are by no means representative of the entire spectrum of explanations for why or how fraud occurs. They do, however, help to shape the framework for this chapter and for an analysis of the inherent vulnerabilities in business processes. From a people perspective, a *fraud tree* is more relevant

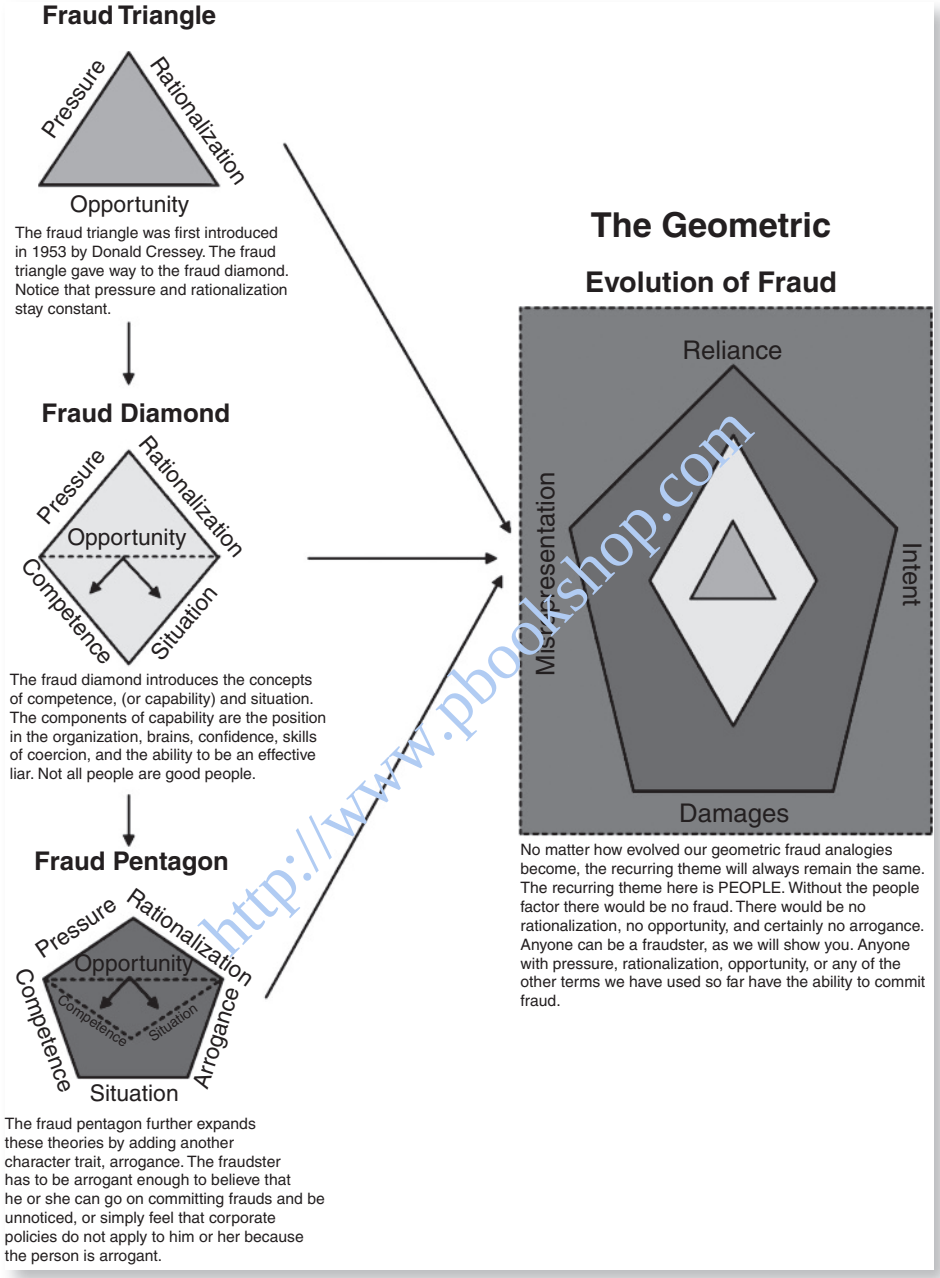




**EXHIBIT 1.3** The Geometric Evolution of Fraud

and useful to prevent, deter, and detect fraud than a schematic diagram that illustrates types of frauds.

Whether we use the industry-established fraud concepts listed earlier or the fraud triangle, diamond, or pentagon, there is one recurrent theme: people. Exhibit 1.3 combines the geometric theories and points toward elements that we need in order to prove fraud with supportable conclusions. The exhibit is just a guide. Each fraud is unique, and these guidelines are not intended to replace sound principles and practices acquired through experience and the continuing improvement of your skills.

Understanding what shapes the personalities of the people in your organization is a critical element in detecting, deterring, and preventing fraud. The 800-pound friendly gorilla looks at the personalities on display by the clothes people wear, the cars they drive, the jewelry they wear, and other things. Understanding the different personality traits of your people, from the board of directors to the mail clerks, will help you to shape your organization into one that is proactively addressing fraud risk. Exhibit 1.4 is an example of a fraud tree showing some of the potential perpetrators of fraud. This list is not exhaustive; anybody can be a fraudster. Exhibit 1.4 helps you think about the following questions:

- Who are the players initiating frauds?
- How are they doing it?
- What personality traits do they display?

The exhibit shows the tree's roots as the foundation (the organization) and the apples as the people creating the value through the organization's processes.

The roles and responsibilities of corporate executives should evolve with changes in the economy, technology, and the availability of information. Requiring C-suite signatures for financial statements and internal controls as a result of the Sarbanes-Oxley and Dodd-Frank legislation does not stop fraud.[18] The additional legislation and regulation typically creates more costly compliance and oversight and potential layers of distraction to the organization. The roles and interests of executives and legistors often conflict, which creates the opportuinity for fraud. Too much red tape handcuffs the organization's ability to operate and may create unethical rationalizations by the executives to meet these regulatory demands.

The money being spent on compliance with new legislation could be better invested in training the staff in an effective manner to develop and maintain fraud deterrence and prevention systems. Unfortunately, the increasing creation of external oversight acts is becoming the driving force in developing fraud risk

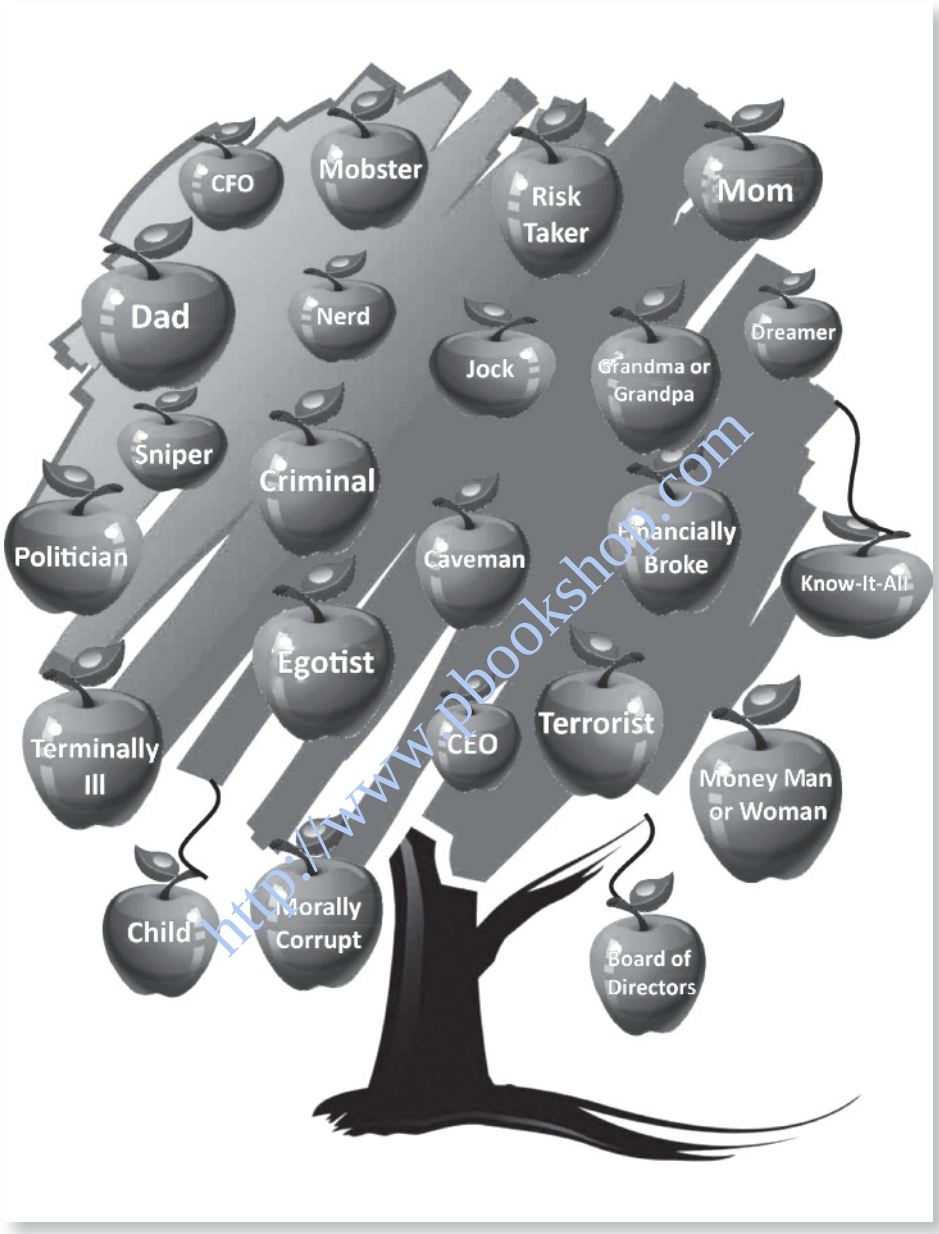


**EXHIBIT 1.4** The People of the Fraud Tree

management programs and is replacing the development of a strong ethical and moral culture or tone within organizations. Will the next 10 or 20 years of new laws and regulations guarantee the moral character of the organization and reduce or prevent fraud? It is highly unlikely. In this book, I will continue to refer to various perspectives, such as those of legislators, CEOs, managers, and employees. Inferences must also be made. For example, say a CEO wants to avoid fraud in his organization, but what if he is the fraudster? Legislation is an effective way to set the tone in an organization, but it is not the 800-pound friendly gorilla strategy. Each organization is different, and that means its strategies will differ as well. Maybe legislation should be the motivation for top management to develop 800-pound friendly gorillas and avoid fraud at all levels, but legislation should also avoid creating too much "one-size-fits-all" red tape.

The reason legislation designed to prevent fraud fails to be effective is that it does not take into account the myriad possible organizational structures and processes where fraud could exist. A one-size-fits-all approach might satisfy the legislatures' need for a reaction to public outcry, but the resulting legislation is never a comfortable fit for all organizations. Many organizations would be better off developing an 800-pound friendly gorilla strategy for their own unique circumstances.

Think about raising kids as an example. Most parents want to raise children with proper values and to do the right thing. We teach this by developing consequences for improper behavior. As a guardian, your choice is either to tell them how to act or to actually demonstrate the proper behavior and enforce the consequences of improper behavior. This applies to organizations as well. Will the presense of laws improve an organization, or should the ethical actions of the organization mold the ethical principles of the people? We assume that the punishments are mandated by law. What are the real consequences of the laws if the situation falls in a gray area? Today's organizations need to create accountability without the reliance on laws while still ensuring that proper interests are being served.

Leading by example is more powerful than simply reciting rules. It is better to lead by example than by the "Do as I say, not as I do" approach. During the years I worked with young kids, teaching them soccer skills, my longtime mentor, Spencer Rockman, taught me that telling a six-year-old how to kick a soccer ball like an adult is not as effective as showing him or her how to kick it like a six-year-old. Successful 800-pound friendly gorillas show their people the right way to act by leading with examples they can understand. The apple does not fall far from the organizational tree. Organizational leaders (tone at the top) need to implement proper controls that limit the opportunity and situational elements that develop into fraud; they should also lead by example to help deter, detect, and prevent fraud.

## THE INCREASED RISK OF FRAUD LOSS

There are common challenges in an organization that may inadvertently increase its risk of fraud loss. The hurdles an organization may face in trying to avoid fraud are innumerable, and this list is merely a starting point for dealing with such challenges, which include the following:

- The organization may not have clearly delineated markers for accountability and responsibility; therefore, it may not recognize its fiduciary obligation to reconcile line-organization responsibilities for safeguarding organizational assets with the people who have those duties.
- The organizational structure may harbor a needless complexity that fosters an environment conducive to fraud and thus creates a breeding ground for fraud.
- When facing suspicions of fraud, the organization may lack the necessary skill, education, and/or knowledge to ask the right questions and develop relevant facts in an objective manner.
- The organization may not apply divergent and critical thinking to analyze a potential fraud event when it manifests or when an allegation of fraud is presented.



Economic frauds may be committed for any number of reasons, but it always seems to come back to the individual and his or her capability and desire to commit fraud. The fraud triangle and its design speak to a perpetrator's need or ability to rationalize; however, it is not essential for fraud. Sam E. Antar, chief financial officer (CFO) of the now-defunct company Crazy Eddie Inc. and comastermind of a nearly 20-year fraud uncovered during the 1980s, openly admitted that neither he nor his coconspirators contemplated rationalizing the massive frauds that he, his uncle, and his cousin were perpetrating:

> We committed crime simply because we could. Criminologists like to analyze white collar crime in terms of the "fraud triangle"—incentive, opportunity, and rationalization. We had no rationalization. The incentive and opportunity was there, but the morality and excuses were lacking. We never had one conversation about morality during the 18 years that the fraud was going on.[19]

People are at the heart of fraud. This makes the situation more complex, because everyone is different and has different morals. There are people who are

prone to doing the wrong thing because they do the right thing only when it is in their self-interest (e.g., greedy people). Changes in circumstances can cause ethical people to make poor decisions. All individuals who are facing adversity will not commit fraud, but some will.

Fraudsters like Crazy Eddie's Sam Antar demonstrate one of the key points of this book: Unless we get to know the people in an organization and understand the general how and who within the business processes, we won't be able to proactively prevent or detect fraud. The most effective fraud prevention systems are continually communicated and reinforced. An effective fraud prevention system rewards ethical behavior and has clear and undesirable consequences for those who participate in unethical behavior.

## DIVERGENT AND CONVERGENT THINKING

Fraud does not occur in a silo or a vacuum, and neither should its deterrence, prevention, or detection. With a divergent approach you will be able to break down an event or an allegation into its various phases and gain insight into the many aspects of fraud risk within each business process.

Divergent thinking can occur only in a spontaneous, free-flowing environment in which ideas are typically generated in a random manner. The ideas and information are then organized by applying a convergent approach (critical thinking) in which all of the spontaneous, free-flowing ideas are gathered and grouped according to similar attributes or another typology and organized in a way that enables more meaningful analysis.

This is the first step in developing a fully supportable factual position and may need to be revisited once or several times during an investigation because of the iterative nature of fraud deterrence, prevention, and detection. Sometimes fraud will not be caught on the first go-round and will require patience, persistence, and continual review. In the process you will be dealing with a lot of information. Because of this it will be useful to think divergently. We do this by continually brainstorming, keeping case notes or a journal, writing down our observations, and painting a picture (figuratively or literally).



### Brainstorming

Brainstorming is a technique used to generate ideas on a particular topic or concept in an unstructured, unrestricted, and free-form manner. The goal is to generate as many ideas as possible in a short amount of time. In a successful

brainstorming session, each idea stimulates other ideas. Some ideas may follow a more logical progression while others appear more random. Ground rules should be established at the outset of a brainstorming session to ensure that all of the participating members feel uninhibited in contributing to the developing ideas.

This is when you develop your initial fraud theory. All thoughts, no matter how seemingly unrelated or inarticulate, are recorded. What may seem irrelevant at the onset may later prove to be insightful. The ideas or concepts proposed during a brainstorming session are to be categorized in a logical order based on the nature of the allegations involved in order to facilitate development of the initial scope of the work.

An easy way to hone one's brainstorming skills, in this context, is to practice. Brainstorming the information at the onset of a project, possibly with management's assistance and participation, will enable you to be insightful in developing interview plans. The next time you encounter a mystery (be it in a book, a television show, or a movie), consider these questions:

- Who are the characters? What are their roles? Identify all of them no matter how insignificant they seem.
- Identify each character's motive to commit a fraud.
- Who has the most to gain?
- Which of the characters has the situational opportunity to commit the act? Who is in a position to commit the act?
- Which character has the skill set needed to commit the act?
- Based on the situation, how could each of the characters have committed the act? What could he or she know about the act?
- Based on the situation, how could each of the characters plan to conceal the act?



The point of this real-life experiment is that we are all inquisitive by nature. We observe facts (in this case, story lines and characters) and then develop theories. Because each of us has different real-life experiences that shape our perceptions, each of us will observe the same scene differently. This is why it is so important to have multiple participants in a brainstorming session and to remain open-minded to alternative explanations for how things may have occurred.

Having multiple participants in a brainstorming session, however, does not necessarily mean that the same individuals should participate in the investigation. The brainstorming session may be composed of a peer group of otherwise

uninvolved professionals, and their ideas may be equally strong or even stronger precisely because of their lack of involvement in the investigation.

## Keeping a Journal or Writing It Down

Record your mental impressions contemporaneously with your fact-finding investigation to track the development of your theories and findings. Carry a small memo pad at all times, since thoughts may occur to you at any time. Record your formal observations while actively analyzing the facts or conducting inquiries as well as your informal stream-of-consciousness thoughts. Written observations are more easily organized and included in a report than observations that remain intangible and unspoken. The brainstorming exercise can also be used here. While reading a mystery book or watching a mystery show or a movie, keep a sheet of paper handy and make entries as you watch.

Write down whatever comes to mind about a fraud without constraint and without stopping to worry about grammar, organization, or convention. This will ensure that a divergent mind-set is being employed. A variety of thoughts about the fraud will develop relatively quickly. The concepts developed can later be organized and critiqued to develop a logical flow and to identify and close the gaps in facts and evidence necessary to create the big picture.

A similar exercise is to write about a situation without worrying about every detail. The details are important, but they can be filled in later when you formally write up the events. This exercise develops brainstorming skills, which generally focus on the big picture. Each time there is a fact of importance, write down everything that comes to mind.

Imagine, for example, witnessing a hit-and-run accident involving a man on a motorcycle and a pedestrian fruit kiosk. Picture why someone would drive through a fruit stand—upending the cart, its produce, and the person responsible for it—and not stop. Focus on the *person*, not the mess on the street. Was he late for an appointment? Was he sick? Was he intentionally targeting the cart's handler? Was the motivation rage? Did he want to circle back and steal as much fruit as he could? Put yourself in the driver's place.

The point of the exercise is to help you develop the ability to put yourself in the shoes of the person committing the fraud and to walk through the steps he or she took to commit the fraud.

## Painting a Picture

Paint the picture necessary to facilitate an understanding. Take what is in your mind about a fraud and the ideas you developed from brainstorming and

visualize them to create a picture. Transfer the picture in your mind to paper so you can see the people involved. See and appreciate the relationships among the ideas, people, and events to develop an understanding of where fraud can exist in organizational processes. Start with one central idea about the fraud or fraud risk, and then draw branches from the main idea to represent different parts or aspects of the main fraud.

Now you are creating a visual image or map of the fraud that others can use to further investigate or expose the fraud or fraud risk (see Exhibit 1.5). Fraud risk represents people in the organization who deliberately use deception to gain an advantage. In either an actual fraud or the risk of fraud, you are looking at specific events or allegations that can lead to the conclusion beyond reasonable doubt of their existence.

Divergent thinking identifies issues and ideas that are later converted into relevant and provable facts through the convergent, critical thinking process. Ideas generated by divergent thinking do not commit the creator or the group to a particular position or conclusion. Divergent thinking represents a means to an end, and it is but one tool in the toolbox. Any conclusion or position requires sufficient relevant evidentiary support.

Convergent, or critical, thinking leads to documented and/or provable conclusions, in contrast to the unconstrained and free-flowing ideas generated by divergent thinking. Convergent thinking takes the investigator to a possible




**EXHIBIT 1.5** Painting a Picture

conclusion and, by extension, helps him or her to identify the evidence to support that conclusion. When the evidence needed to support a fraud theory up front has been identified, an effective work plan may be developed to prove what did or did not occur. The more ideas generated, the greater the chance to resolve allegations and protect the organizational value.

An investigator cannot prove that fraud exists simply by applying divergent and convergent thinking to a situation or an allegation. The ideas generated have to be applied to the facts at hand, and a fraud theory, which is then tested, has to be developed.

Consider, for example, a hypothetical fraud that you are asked to investigate. Four of your coworkers may be involved in a potential fraud, and each of them may have several ways that he or she could have committed the fraud. Each coworker must be analyzed and asked to list related associations—such as spouses, kids, other family members, and significant others—who may have been involved. Each evaluation of a person of interest should include information about relationships and connections.

Leverage the ideas developed from brainstorming to picture the possibilities. This requires both divergent and convergent thinking. Generate as many ideas as you can in order to prevent, deter, and detect fraud in as short a time frame as possible. Did any of the four coworkers buy a new car or house recently? Did any of them go on an expensive vacation, purchase an expensive watch, or experience any life-changing events (major illness, bankruptcy, and/or divorce, etc.)? Keep your eyes open, because the signs will be there.



## CRITICAL THINKING REQUIRES CRITICAL QUESTIONS

What are the right critical questions? What types of questions do you think you should be asking while reading the one-minute fraud mystery and trying to work it out? The purpose of this exercise is to assist you in identifying questions to ask yourself and others as part of an antifraud project; it is not a primer on interviewing skills or even reading and interpreting body language.

There are two types of questions: general (open-ended) and specific (closed-ended). The lists below are not all-inclusive but are simply a starting point. Remember that each investigation will have different facts and require different questions. Maintaining a thinking pattern that is both divergent and convergent is necessary in developing effective questions.

## General (Open-Ended) Questions

We need questions to help us develop an understanding of the players involved in a potential fraud as well as an overview of the potential fraud itself. These open-ended questions are designed to give the illusion of control to the respondent. In general, people feel more comfortable when they have the illusion of control over a situation. Therefore, a respondent who feels in control of the situation is more likely to reveal pertinent information.

The interviewer never truly releases control, however, because the inquiries that the interviewer makes will be geared to reveal specific information about a specific situation. The interviewer wants the subject of each interview to think, reflect, and give us his or her opinion. These opinions can be long, especially in response to open-ended questions. The interviewer should never interrupt. A respondent who feels comfortable will generally let his or her guard down. If there is a question about a response, or a point needs to be clarified, the interviewer should make a note and come back to it. Whether that happens immediately after the answer is provided or after all preplanned questions have been asked depends on the tone of the interview.

When possible, conduct interviews in teams of two, with one asking the questions and the other observing and recording the responses. Transcribe these notes as soon after the interview as possible to preserve the responses and memories. If the subject seems overwhelmed by having more than one interviewer, either mitigate that response in advance (i.e., explain why there are two people present) or, if the interviewer is unable to remove the discomfort, consider abandoning the team approach altogether.

In place of the team approach. you can consider using a recording device, but be sure to make the respondent aware of the fact that the interview is being recorded for reasons of accuracy, legal protection, and the avoidance of any future misinterpretations. It should be noted that in some states it is illegal to tape-record someone without his or her knowledge, so make sure you follow the applicable laws. It is important that the subject not be overwhelmed, because this can inhibit his or her responses.

The open-ended questions will often generate emotions that lead to more uninhibited information, which is the goal. This information cannot be elicited with hostile words or attitudes, so it is important that the interviewer's posture remain supportive of the subject, unbiased, and empathetic. Generally, people want to help when they are asked for help, and they may also confess to an empathetic ear when guilt sets in.

Open-ended questions have the following characteristics:

- They ask people to think and reflect.
- They often make people give their opinions and feelings.
- They hand control of the conversation over to the person being interviewed.

Open-ended questions for people with knowledge of an organization are usually asked at the onset of an investigation and include the following:

- What does the organization do?
- How does the organization treat you and your coworkers?
- Do you know why I'm here at your company talking to you?
- Do you know what's missing (e.g., cash, accounts receivable, inventory, equipment)?
- What type of problems could exist?
- Where do you think your organization is vulnerable to loss?
- Does your organization have an expectation for employee conduct? What is it?
- How do people in the organization spend their time? Are there any laggards?
- What are the employees' activities on a normal day?
- What do *you* think I should know about the organization's leaders?
- What areas of expertise are needed to perform the organizational process?
- What do *you* think I am looking for?
- What are the involved parties' hobbies?
- What are their interests?
- What bothers them?
- What do you think needs to be changed in the organization?
- What are the people in the organization's strongest beliefs, values, and philosophies?
- Who has the influence or sense of entitlement to do it? (*It* can be making changes in the company policy, committing fraud, or whatever fits into the particular situation.)
- Who do you think could have made the money or asset disappear, and why? How could he or she have done it?
- What else do you think I need to know about this problem?

Information-seeking questions are one type of open-ended question, and their purpose is self-explanatory. These are usually posed to people with information at the outset of an investigation. Here are some examples:

- What prompted you or your company to look into this?
- What are your expectations or requirements for this matter?
- What process did you go through to determine that this is necessary?
- How do you see this happening?
- What is it that you'd like to see accomplished?
- Whom have you had success with in the past?
- Whom have you had difficulties with in the past?
- Can you help me understand this situation a little better?
- What does this answer mean?
- How does the process work now?
- What challenges does the process create?
- What challenges has the process created in the past?
- What are the best things about the process?
- What other items should we discuss?

Another subset of open-ended questions is qualifying questions. These include the following:

- What do you think are the next steps?
- What is your time line for implementing the investigation?
- What other data points should we know before moving forward?
- What budget has been established for this?
- What are your thoughts?
- Who else is involved in this decision?
- What could make this no longer a priority?
- What's changed since we last talked?
- What concerns do you have?



## Specific (Closed-Ended) Questions

Close-ended types of questions are used to narrow and refine the information that has been acquired through open-ended questions and other means, to form a persistent, tenacious focus.

Most interviewers prefer to develop a rapport with the subject before getting into the details with them. This portion of an interview is also used to establish credibility—both on the subject's part (why he or she is important to talk to) and the interviewer (why he or she was asked to speak to the subject). Here are some examples:

- How did you get involved in XYZ?
- What kind of challenges are you facing?
- What's the most important priority to you in this matter? Why?
- What other issues are important to you?
- What would you like to see improved?
- How do you measure that?

Closed-ended questions have the following characteristics:

- People generally find them easier to answer (yes or no).
- The interviewer controls the conversation, often utilizing a generic questionnaire.

Both open-ended and closed-ended questions are designed to yield facts. Information-seeking questions are generally open-ended, whereas confirmatory questions are usually closed-ended. Closed-ended questions are usually answered yes or no or with short answers. Interviewers typically know the answers to the questions before they ask them. Be sure to substitute the word *event* for *fraud* in all the questions.

Keep in mind that an event refers to the facts, transactions (such as source documents), and people who may be involved. Take one element at a time in the development of your supportable fact patterns and later put them together to tell the story. Additional closed-ended questions include the following:

- How would you describe the event? (This is an example of using the word *event* for *fraud*.)
- Did you see it or just hear about it?
- What are the potential causes of the event?
- What are the potential effects of the event on the organization?
- What are the most important (smoking-gun) issues about the event?
- What are the smaller issues (distractions) that caused the event?
- Has the event changed? Why are those changes important?
- What is known and unknown about the event?
- What should have been known?
- How does the event make you feel?
- What category of ideas or documents do you have about the event?
- How often do these events occur in your organization? Why?
- What suggestions or recommendations would you make about these events?

- What are the different aspects of the events that you can think of?
- Are the sales supported?
- Are there multiple bank accounts?
- Are there commission-based employees?
- Are checks ever issued to the wrong payee?
- Are there fictitious vendors (payees)?

## THE PERSONALITY TRAITS OF A FRAUDSTER

Develop and identify the personality traits of potential fraudsters as you ask the questions in the preceding section. Exhibit 1.6 presents some of the personalities you may encounter as you develop your ideas to prevent, deter, and detect fraud in your organization.

A list of common traits of fraudsters with sample questions and brainstorming activities follows.




**EXHIBIT 1.6** Fraud Human Traits

**They are deal makers** (wheeler-dealers). Do you feel like every time you speak with these people, it is like being on a game show? What is in it for the deal makers?

**It's their way or the highway** (dominating and controlling). Do you feel pushed or intimidated into making or supporting a bad decision? Why are the controllers so closed-minded?

**They hate people reviewing their work** (no oversight required!). Do you feel like you are treading on forbidden ground when you ask a relevant question about these people's work? Why are they so defensive? Are they hiding something?

**Everything has to go through them** (control freaks). Do you feel like these people require control over the system, or do they engage in the overrides to the controls? Why do they have a burning need to control? Are they hiding something?

**Their sole desire is for personal gain** (self-motivated). Do you feel like they always put themselves first at the expense of others? Is it organizational or personal gain? Are they greedy?

**They are always trying to get around the system** (noncompliant work-arounders). Do you sense that these people are always trying to avoid you? Whose self-interest is being served, theirs or the organization's?

**They have an extended lifestyle or something else** (extenders). Do you get the feeling that your colleagues who make the same salary as you have another source of income? Do they purchase a new car every year, take exotic vacations, send their kids to expensive colleges, and live in the upscale section of town? Lifestyle itself is not indicative of inappropriate conduct, but it may provide insight into someone's need for supplemental income. Legitimate explanations for the apparent excesses include inheritance, frugal lifestyle up to that point, or even generous relatives and friends. When was the last time the organization updated its background checks? Updated background checks should be performed for all employees and key contractors on a routine basis. Is this one of the most trusted employees?

**They have very close relationships with customers or vendors** (chummy buddies). Do you think that a particular relationship with a business associate or two is creating vulnerability for the organization? Is the relationship based on business interests, personal interests, or both? How is the value in the organization vulnerable because of such relationships? Collusion-based frauds, which involve more than one person, are likely to occur when there is a close personal relationship

with vendors and clients or customers. These schemes typically include overbilling (with the refund to the inside person at the payer organization), kickbacks for influence used in obtaining business, and inventory abuse or theft.

**They have close relationships with the boss** (boss's pets). Do you think that these individuals have personal relationships with their immediate (or higher-level) supervisors, and do these relationship put the organization at risk? What are the relationships based on, and do they create a conflict of interest?

**They can never relax or sit still** (antsy). Do you think that people who cannot sit still or relax may be under undue pressure? Is it work-related or personal in nature? What is the reason?

**Their work performance is off the charts** (chart breakers). Do you think that there is a credible reason that these people are chronic outperformers? Is it skill based, effort based, or something else?

**They are the first in and the last out** (FILOs). Do you think there is a credible reason that these people are consistently the first to show and the last to go? Is it because they are overworked (and thus entitled to more), inefficient (and covering up), or conscientious? What could they be hiding?

**They spend excessive time on the job** (clock burners). Do you think that the jobs performed by these individuals warrant the overtime, or is there possibly an ulterior motive? Are they unsupervised, with unfettered access? Is the work product generated worth the cost?

**There are frequent, dramatic changes in their behavior personalities** (seesaws). Do you sense a particular trigger to these people's behavioral and personality changes (instability, substance abuse, or addictions)? Would these mood swings put the company at risk for financial loss? (Any insight derived from this line of questioning is not a substitute for consultation with a trained psychologist, when indicated.)

**They appear to be completely trustworthy** (trustworthy). Do you think that these people are as trustworthy outside the organization as they want you to believe they are internally? Are they too good to be believed? When was the last time you ran any background checks? As noted earlier, background checks should be performed and updated on a regular basis.

**They take little or no time off** (workaholics). Do you think that these people are too protective of their responsibilities (without obvious justification)? Why haven't they taken any substantial leave during

their tenure? When was the last time others performed these people's duties? Many employers discover irregular activities when a "dedicated" employee is forced to take an unscheduled leave. Interdepartmental cross-training with unscheduled and periodic rotation can avoid this problem. An unavoidable consequence of that, however, is that the employees will learn extra tasks that can facilitate inappropriate conduct.

## THE MORAL COMPASS

This section discusses examining your moral compass (a counterpart to the misrepresentations represented by the *M* in the MIRD acronym, which will be explained in the following section). Does your moral compass zigzag into what we call the Z pattern, or does it follow a straight line? Do you have a Z pattern in your organization? Are the people following the organization's mission and direction, or do they stray from the straight line as though forming the letter Z?

If the pattern is left unexposed, the subtle changes in people can have a significant impact on an organization. A simple example is taking home a ream of copy paper without permission. Now apply that thinking to the one-minute fraud mystery at the beginning of this chapter. Where is Betty Favor in the organizational structure? Does she have the ability to zig and zag, or does she appear to following a straight line of good moral character? Does she have control? Whom does she report to? What type of lifestyle does she have? What questions are you thinking should be asked? This is making good use of divergent thinking.

People can be shiny and are just as capable of stinging as jellyfish are (Exhibit 1.8).



## THE ELEMENTS OF FRAUD: MIRD

As mentioned earlier, MIRD is a useful acronym, not just to remember the important elements of fraud's definition (*misrepresentation*, *intention*, *reliance*, and *damage*) but also to implement a divergent way of thinking. You can use it to understand where people and value meet in an organization and to expose the potential for fraud. Again, these are elements to help define fraud and not nessarily the ingredients needed for fraud to occur.

To analyze fraud through this acronym, start by considering what is the *misrepresentation*. How much would the facts have to be misrepresented to be

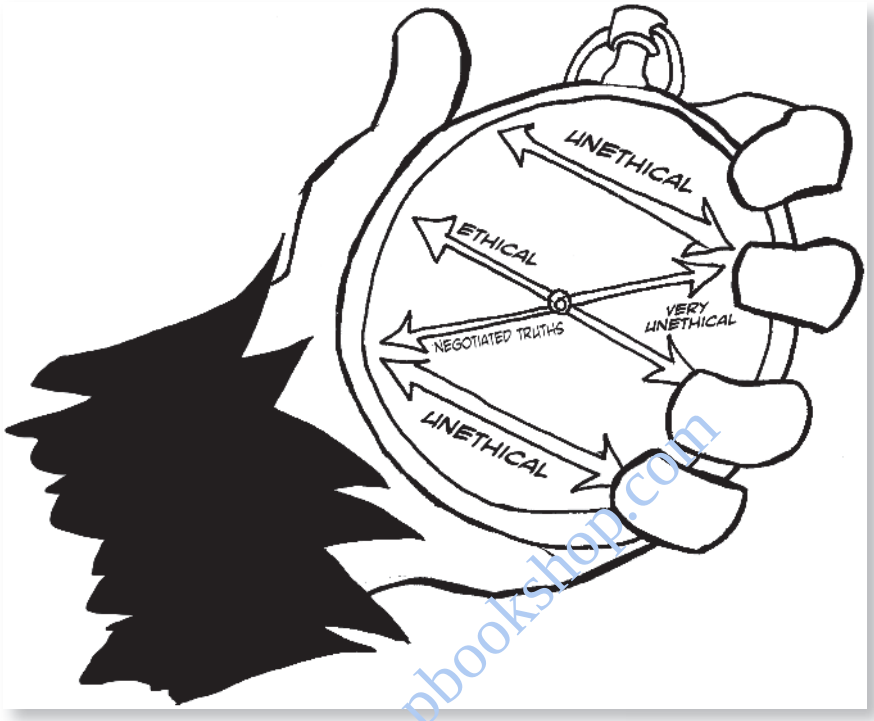


**EXHIBIT 1.7** The Z Pattern





considered material?[20] The answer is clearly more qualitative than quantitative. This is not something that can be assigned a percentage of a larger item or expressed numerically. The key to materiality is the ability of a false statement about a fact to cause action or inaction on the part of an individual who is relying on the statement's accuracy to define his or her action. This does not mean that an immaterial misrepresentation is not fraud. For instance, say someone tries to steal inventory and is caught before the goods are removed. There is no dollar loss since the goods were not lost, a quantitative measure. However, when that person tried to steal the goods, he or she broke the law, a qualitative measure. The 800-pound friendly gorilla looks at the motives behind the actions rather than just at the numeric values when addressing a misrepresentation.

Next, examine the *intentions* of the people in the organization. Intention is an important concept to understand when discussing fraud; it is critical to


**EXHIBIT 1.8** The Jellyfish Analogy





understanding someone's actions. Intent is necessary to prove fraud—either beyond a reasonable doubt (99 percent convinced), in a criminal matter, or by preponderance of the evidence (more than 50 percent belief), in a civil matter. Remember that fraud analysts serve as fact finders only and do not supplant the judge or jury in declaring guilt or innocence. Intention is a state of mind and can be very difficult to prove. The utilization of open-ended questions and other effective communication is the key to determining intention, because it is less accusatory and more proactive.

Apply some divergent thinking with the facts in our one-minute fraud mystery to develop what the intention is. What is John Asset's intent in raising the issue of the discrepancy? What is Betty Favor's intent in rebuffing him? What is the owner's intent? It may be easier to soothe ruffled feathers and overlook

the fraud, but is that the best answer for the organization in the long run if the goal is to establish the correct ethical tone? Whose interests are being served? What controls are in place? What questions do you think should be asked?

Necessary or unavoidable *reliance* creates situations that are vulnerable to fraud or the exploitation of value. The world is governed by people. The same people who create the laws, regulations, and other oversight mechanisms generally provide the direct or indirect oversight of compliance with these measures. It is important not to assume that people will automatically observe or follow the same rules they create or enforce.

Furthermore, organizational leaders rely on others (employees) to be sufficiently trained and educated to perform the tasks they are hired to perform. The leaders of an organization often believe that their people are not so covetous of what is not theirs, that they would not overtly commit fraud or covertly engage in the exploitation of another's assets or value for personal gain. Leaders need to take pause and ask the following of themselves and their subordinates: Do we and our people have the necessary skills to perform the required tasks? Do we and our people know what fraud looks like?

In terms of our mystery, does Betty Favor or John Asset have the trust of the owner? Whom do you give more credibility to? Who is more qualified? Who has more to lose: John, by pointing out the discrepancy, or Betty, for telling her boss that his newest employee is incompetent? What questions do you think should be asked? We rely on people in the organizational structure, and we need to make sure that these people have good moral character and fully understand their role in the organization.

Finish your examination of the MIRD acronym by thinking of *damage* in terms of value. After all, the financial damage comes from the value taken inappropriately (directly or exploitatively) from the organization. Think about the item of value within the organization that was lost as a result of the reliance on an intentional misrepresentation. The value can be as simple as having check-signing authority, writing off uncollectible accounts, making deposits, or ordering inventory.

Apply the concept of damage to our one-minute fraud mystery. Who has access to the value: Betty Favor? John Asset? The owner? What questions should be asked?

In applying the divergent thinking process to the mystery, we have not yet asked to see any documentation, such as the bank reconciliation or the bank statements, nor have we contacted the bank. Yet a fraud theory or plot has emerged, which will be useful to draw a final conclusion about the one-minute fraud mystery by the end of the chapter.

## EDUCATION ABOUT FRAUD

Educating people about what fraud looks like and where the value and people meet in an organization is the first step in preventing, deterring, and detecting fraud. Many organizations rely on the assumption that people in particular roles understand their responsibilities and have the necessary education and skill sets to competently meet their obligations. Yet there is an 80-20 rule for a typical organizational structure: 80 percent of the process is controlled by only 20 percent of the individuals.

Organizational values and beliefs play a role that transcends an obligation to follow the rules. Does the organization's culture emphasize building for the company's future or for the C-suite's retirement? The moral of Dr. Seuss's children's story *The Lorax* is that destroying the environment in the name of growth and profiteering destroys the future.[21] This is a concept that even young children can grasp, yet many corporate leaders fail to see it. An organization should maintain an environment that does not succumb to pressures that have the potential to jeopardize the company's long-term existence. Unfortunately, this is not a universal statement. When an organization believes in the maximization of shareholder value, it often can mean the sale of all or part of the organization, without any regard for the interests of the people working there. Such a situation could be rife with fraud possibilities since the employees may feel betrayed.

One way to gauge the relative moral compass of an organization is to consider whether executive salaries or staff training and education are likely to be the chosen victim of a budgetary contraction. In an economic environment where people are being asked to do more with less because of downsizing and other cost-cutting measures, training and continuous improvement may not be a top priority. The fraudster is aware of these cuts, and it allows him or her to perpetrate a fraud.

Consider the organizational impact of reducing annual training budgets. The staff members, which may or may not experience changes (up or down) in their salaries, are being asked to expand their responsibilities, perhaps into new territory where some individuals have little or no experience. Yet they may not be given the appropriate tools to do the job. How will this affect morale? Does this give the employees an incentive to work harder? Are the employees who are being asked to do more still willing to protect the organization's value?

An organizational process is only improved by the continual education and reeducation of the people involved in it. What does the education in a typical organization generally consist of? It is true that there are those who do a job and those who have a career. Continuous improvement and job training are not on

the radar for all organizations or individuals. Fraud develops in organizations with leaders who believe there is no need to stay current with the trends and techniques in their chosen field.

Most antifraud professionals, if they belong to credible professional organizations, are required to constantly manage their personal knowledge base and maintain and improve their skill sets. Some are required to annually attend professional ethics training. A well-trained staff represents the front line of an organization's fraud fighters, and failing to prepare the personnel with the best tools to meet their duties in protecting their organization from loss is preparing the organization to fail. Create a "neighborhood watch" in your organization by keeping your employees trained and educated. Develop a proactive approach to fraud by having all people in the organization fully trained and ready to combat fraud.

The Public Company Accounting Oversight Board was created by the Sarbanes-Oxley Act of 2002 to provide independent and external oversight to public company financial audits in the form of informative, accurate, and independent audit reports. Its purpose was to protect investors and the public interest.[22] Senator Paul Sarbanes (D-MD) and Representative Michael Oxley (R-OH) cosponsored this legislation to establish new and enhanced oversight standards for U.S. public companies. Sarbanes is a Harvard-educated attorney, and Oxley is a lawyer from Ohio State University. Neither had formal or practical training in financial auditing, internal control, or risk assessment.[23] Their views were limited and were based on the assumption that people will follow rules. Fraud is unique and is still occurring despite these new standards.

Oscar Wilde once said, "Education is an admirable thing, but it is well to remember, from time to time, that nothing that is worth knowing can be taught."[24] Gaining knowledge is worthwhile, but nothing replaces learning from past experiences and actually applying what you have been taught. More involvement in the unique organizational processes through hands-on experience is lacking in the development of these laws. The only true way to avoid fraud is through understanding the people who are being asked to comply with these laws by analyzing their application of them.

Fraud risk evolves from the intersection of people and value, and fraud is mitigated by the introduction of appropriate education and training. Checks and balances can be, and are, circumvented when the scale of self-interest tips in the direction of unchecked greed. The mere presence of financial audits and systemic checks and balances will not alone prevent or deter fraud. The use of random data selection to screen for errors and irregularities is a flawed approach to managing fraud risk, because it is impossible to replicate

or automate the human factor. There is often an assumption (which may or may not be true) that the individuals charged with the responsibility of protecting organizational value are properly trained and understand how fraud may occur.

The solution to the issue of organizational fraud is to develop people in the organization who have a shared vision of the company's goals and who are invested in the organization and its success. These people should be trained so that they can properly apply divergent and convergent thinking to identify the fulcrum where value and peope meet and whether or not fraud exists there. An organization has to have value, or it would not exist. The same people who create or maintain value can also destroy it. To protect the value in an organization, we need to understand the people who have control over it and the inherent process-based vulnerabilities of the organization.

Three things must be present to allow fraud to exist and remain undetected in your organization: distraction, deception, and divison.

Add the human element to the three *D*s, and you have the formula for fraud to exist in your organization. People are easily distracted, and that distraction leads to the opportunity for deception. The great promise of increasing one's net worth and obtaining a thing of value with minimal relative effort leads some to take the risk of enduring unpleasant consequences. There is a line separating those who would be willing to take that risk from those who would not. Throughout history fraudsters have added creativity to deceptions.

In your defense against fraud, you must examine the people who distract others in the process and the means by which these distractions are formulated. Do the distractions allow the fraudster to deceive the people involved in the process so that he or she can access the value and remain undetected? By the time we get to the third *D*, division, these distractions and deceptions have created a division among the people in the process that exposes the value to the fraudster.

These distractions may appear to be from sources beyond the people in the organization, such as a speculation created by a negotiated truth (white lie) that creates unreasonable expectations as a result of leaked misinformation by the fraudster. The organization must train people in the process to look for the distractions that create the opportunity to camouflage the deception and create the necessary division for the fraud to exist.

We are a society of tangibles, so it is often difficult to stimulate interest in the intangibles. Value is an intangible concept. For example, a car loses significant value when it is driven off the showroom floor, yet people continue to purchase it, because the car can be touched and value can be assigned to it. The concept that its value will almost certainly decline is conveniently ignored by

most people because it is something that cannot be identified by the five senses. It is important that the fraud investigator pay attention to the intangibles.

Let's examine the one-minute fraud mystery by considering the following questions:

- How do we begin our divergent thinking process?
- Where is the organization's value?
- Who has access to the cash?
- Is the organization's value exposed?
- Are the parties involved educated, and do they understand what fraud looks like?

The fraudster knows what fraud looks like. In our mystery, Betty clearly has the authority, since she has directly gone to the owner. Betty also oversees the functions concerned with banking; John went to her upon discovering the discrepancy. John is a new accountant—could he have made a mistake? Who is lying, and how do you know? Is this situation simply an error and John and Betty are both protecting their jobs, or is it there an ongoing fraud?

What questions should you continue developing to educate people on what fraud looks like? How do we balance the idea that an 800-pound friendly gorilla is watching that creates enough consequence, yet maintains open communication and rewards ethical behavior?



## CONFUSION ABOUT RESPONSIBILITY

Responsibility and fraud prevention, deterrence, and detection go hand in hand. Exposure to fraud risk arises when there are ambiguities related to operational and oversight responsibilities or when there is conflict between the responsible party and the benefiting party. The proverbial fox cannot be allowed to guard the henhouse. You cannot have the controlling party guarding the value in the organization without developing the proper oversight and checks and balances.

Who are the people with knowledge? Who has the most to gain (or lose)? In our one-minute fraud mystery, is it Betty, John, and/or the owner? Which people manage any part of the revenue stream or asset structure, and do they have relevant practical knowledge (no technological malarkey)? Who makes the decisions? In our mystery it appears to be Betty.

Who are the customers, investors, and bankers? Who is the organization's audience? What level of understanding can you establish? Is it simple, or can

you start at an advanced level? In our mystery, we know that cash is involved, and we know the three parties involved. What documentation is available? Who is the intended user of the documents? In our mystery, it appears that we have bank statements and reconciliations. What other documents and information should we or could we expect to find?

People provide answers to questions, or they provide guidance on where the answers may be found. This is why we often find ourselves unwittingly playing the "he said, she said" game when tracking down key answers to critical questions. Your best friend in determining responsibility is often a disgruntled employee, a former spouse, a competitor, law enforcement or governmental agencies, credit collectors, and others who are often not part of the organizational culture at the time.

So how do you manage concerns about confusion of responsibility? By introducing an 800-pound friendly gorilla to the organization to develop open channels of communication.

The 800-pound friendly gorilla represents the oversight necessary to continuously monitor both systemic controls and the human factor (reliance on personnel to do the right thing for the right reasons), and it also provides the appropriate consequence systems to address ethical lapses or poor judgment. Think of the organization fraud risk management process as a movie script. Who is the cast? What is the plot? Unfortunately, these scripts do not always have happy endings when organizations are not monitored. An organization left unexamined will have fraud.



## COMPLEXITY

Is fraud complex or simple? Our caveman in Exhibit 1.1 states that he used a club to commit fraud, similar to the rationale offered by Willie Sutton, the infamous American bank robber of the early twentieth century. According to legend, when asked why he robbed banks, Sutton said, "Because that's where the money is." Frauds do not have to be complex, but in some instances the complexity is necessary to circumvent the controls that are in place or to discourage questions from the 800-pound friendly gorilla.

A good exercise is to think about how you would design a fraud. Which people have full control of the value, and how would you circumvent their controls? Continual exercises should develop potential fraud schemes and plans to deter, prevent, and detect fraud. The best defense is developed through past experiences, such as an analysis of prior frauds to see how they occurred and how they could have been prevented. You need to think like a fraudster to catch a fraudster.

GAAP and/or IFRS (the use of GAAP and/or IFRS depends on where the organization does business and where geographically its customers are) establish the best practices for recording the value in an organization. Proper accounting will assist in detecting fraud, but too often organizations focus only on the results of the reporting protocols to foster the comparibility of entities, and they ignore or do not understand how accounting records can serve to deter, detect, and prevent fraud. What communications about fraud risk are relied on, and where are they represented in the financial statements? Generally accepted accounting principles (GAAP) or international financial reporting standards (IFRS) are not intended to deter, detect, and prevent fraud. Intent does not matter from a financial reporting prespective since fraud is clearly a departure from these established standards.

Balance sheets are purportedly accurate for one day, although companies are not static and their performance changes constantly. Financial statements are developed by people and are easily manipulated by knowledgeable individuals. The income statement references a specific time period and, because it too is developed by people, is accurate only if the underlying records are complete and accurate. The cash-flow statements, supplemental disclosures, and notes to the financial statements are all subject to the same risks of misstatement, error, or fraud. The fraud that occurs is in the development of these documents and is subject to people and the judgments that are made. The fraudulent reports are a symptom of the disease (fraud), which is characterized by unchecked greed.

You have both corporate and individual greed to consider in your pursuit of fraud. You might like to think that all disease could be eliminated, but this is not a reality, and the same is true of fraud. Developing, maintaining, and rewarding people with the correct ethical tone is the best medicine for fighting fraud in your organization.

Fraudsters typically know how to manipulate the traditional pathways to communicate organizational results because they understand the organizational process. The methodologies are innumerable but generally include some variant on fictitious revenues, deferred or false revenues, and conspiracies with other greedy people in the organization's process. Fraudsters often know how to manipulate others. People are often implicated by association. Therefore, it is important to have 800-pound friendly gorillas that know when they are being implicated by other's actions.

Having a working knowledge of an organization's performance communication system enables the fraud to occur and in some cases continue for an extended period before being detected. Any successful fraud plan requires an understanding of the inner workings and a knowledge of what people want. Nothing will destroy an organization's value faster than a well-planned fraud. Knowing who

is able to influence these communications and circumvent these processes is critical in preventing, deterring, and detecting fraud in an organization.

Typically, the board of directors and management leaders make the accounting decisions. What training and education do they have, collectively, that make them the *right* team to generate decisions? Are their decisions chained to organizational transparency by the rules, or are individual performance bonuses factored into the decisions they make? Does the organization's decision-making team consult with its independent accountants for major reporting or accounting policy decisions?

Accountants, particularly certified public accountants (CPAs), are expected to uphold the public trust. Although their fees are paid by the organization that engages them for financial statement preparation, the accountants' duties extend to those who are reasonably expected to rely on their work. It is critical that oversight include management of the gatekeepers and their responsibilities, as well as any apparent or perceived conflict of interest that may be present (e.g., an accountant's permissiveness because the client generates substantial annual revenues).

According to the economic entity assumption principle, entities are legally separate from their owners and should therefore account for their activities separate from that of their owners. This is the flip side of what is known as *piercing the corporate veil*, when a court deems that the owners of organizations are not distinguished separately from the entity because of the commingling of business transactions with personal transactions. Because of limited liability, most business owners are generally not personally liable for the debts, losses, and liabilities of the business itself. The business is considered an artificial person.

However, if the owners act in a manner that does not distinguish between themselves and the entity, a court may determine that the entity should be set aside formally since its form of business was not respected by its owners. If this occurs, and the court decides that the business is merely an alter ego of the owners (i.e., the owners are not considered separate from the organization and are therefore subject to personal liability due to the commingling of business and personal transactions), then those owners will generally not be able to avail themselves of the protections from liability normally enjoyed by businesses. Business law and the intricacies involved in the formation of business entities are beyond the scope of this book, but most businesses are organized in such a manner that the owners are afforded protection from any liability resulting from the business.

There are many things that a court will look at in determining whether alter ego liability should be applied. Typical factors include (but are not limited to) the following: whether the company was adequately capitalized; whether

the company kept its own records; whether shares (for a corporation) or units (for a limited liability company, or LLC) were actually issued; whether the owners commingled their finances with the business entity; whether there were corporate directors or LLC managers running the business; how the legal formalities were followed; and whether the owners used the business for personal purposes. It is always a case-by-case situation. An organization should take every precaution to run its business in full compliance with the legally required formalities and use the business in a proper way in order to avoid alter ego liability and remove the complexities it can cause.

Truly great leaders have learned how to leave their egos at the door and create a tone for their organization based on principles. They make sure that the right questions are asked so that when the people meet the value, the people perceive that oversight exists (regardless of the actual oversight in place). This holds true for governmental bodies, Fortune 500 companies, or a simple corner grocery store.

An organization's internal control model should maintain zero tolerance for any violations of these controls. It's the risk-reward concept at its best: the risk must always be greater than the reward. Even the 800-pound friendly gorilla cannot argue against that in preventing fraud. Yet, ironically, people often circumvent internal controls for their own benefit. Regardless of the organizational structure, if there is not a perceived consequence, then deceptive behavior will exist. Even a deterrent like death will not stop fraud from existing if the reward is perceived as being greater than the risk.

In this chapter's mystery, the owner and Betty are the two people in the organization who appear to have the power to override the control. John, as an employee, appears to be the least likely to override the control since he does not have access to the bank and is not involved in the receiving of funds. Other parties that should be considered are the bank, the independent accountant, the attorney, and other organizational personnel. Who has the greatest opportunity to commit fraud against the organization?

In this scenario, the owner does not appear to have access to the cash control. In most companies, the owners trust their employees with this. Remember that Betty has worked for the company for 15 years. Betty can speak for Trust Us Inc. and does so with apparent authority. She appears, in the eyes of a reasonable person, to have the authority to act on behalf of the organization. Her apparent authority is vested in her status as its most trusted and longest-tenured employee.

However, one would do well to remember that *apparent* authority is not the same as *actual* authority. Where are the bylaws, minutes, organizational charts, and so on that give her the authority she has assumed? One of the problems

with apparent authority is that by providing the appearance of such authority to outsiders, the company may become responsible for that person's actions and be bound accordingly to any agreements.

Does your organization have a proactive approach to deterring, preventing, and detecting fraud? Is the organizational code of conduct clearly communicated? Are there needless complexities perpetuated, and do they enable or invite fraud? Consider the message being sent internally and externally. Is it okay to have an alter ego that mixes business with personal matters? Is it okay for employees to act with apparent authority? Ostrich management, in which one's head is buried in the sand, at great risk, is not workable, and it promotes a culture in which these very pitfalls arise. We can no longer be like the three monkeys that "see no evil, hear no evil, speak no evil."

"Healthy greed" is an oxymoron, since *greed* is defined by *Merriam-Webster*'s as "a selfish and excessive desire for more of something than is needed." That is, the essence of greed is *the selfishness and the excess*, not the mere desire to have more than one needs. Milton Friedman's view of greed, which was quoted at the beginning of the chapter, does not necessarily contradict the dictionary definition; it probably just accepts Ayn Rand's principle that selfishness is a virtue. Most for-profit corporations are not content with simply surviving or breaking even; they look to prosper by continuously providing a return on investment to their shareholders. This would be an example of healthy greed. Healthy greed should exist to create competitive and thriving markets, and it should not be driven merely by one's own self-interest but instead be intended for everyone involved in the process. We need more "we the people" thinking and less "what's in it for me?" mentalities. Remember, everyone is greedy, but just how greedy are they? Make sure the 800-pound friendly gorilla is ensuring that any greed present in the organization is healthy greed.



## SUMMARY

Simple embezzlement can lead to significant losses in an organization. The party embezzling faces jail time and can be charged with more than embezzlement alone. Typically, wire fraud, mail fraud, and tax evasion (since embezzlement income is taxable even though illegal) can also be added. An organization can be put out of business by this type of fraud because of the cost of lawyers, the time necessary to investigate, and the missing value (if not recovered).

It's like comparing death from a mosquito bite to death from a shark attack. Everyone's much more afraid of the shark. However, your chances of being

attacked by a shark are just one in 11.5 million, according to the University of Florida. Meanwhile, the mosquito bite is more dangerous, in terms of worldwide death rates, from malaria, West Nile virus, and other diseases.

Similarly, an organization often positions itself to protect against the occurrence of the big fraud (a shark attack), which is less likely to occur, and ignores the small frauds (mosquito bites), even though the mosquito bites are much more likely to occur.

An organization seldom even prosecutes embezzlement because of the way it makes the organization look. The organization figures it has insurance, prosecution is costly and time-consuming, restitution may be made, and the ethical tone is not moral and breeds more fraud. Without a fear of fraud, organizations often ignore the small frauds. Instead, an organization must follow through and publicize the behavior to send a message that it will not be tolerated. Organizations should not be reactive in their approach but should rather be



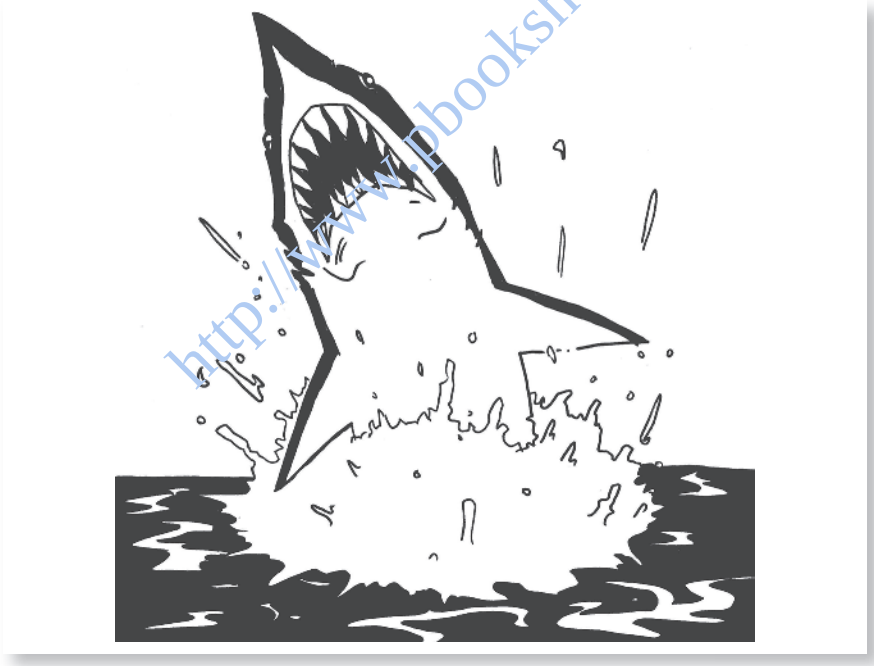

**EXHIBIT 1.9** Shark Attack

proactive by creating the correct moral ethical tone and having the 800-pound friendly gorilla watching from the start.

Outrage equals interest; without it, no one is watching. Typically, if the event or transaction does not create outrage, no actions will be taken. This is one of the reasons most frauds remain unreported and continue to exist in today's organizations. A wrongdoing should not need media attention or have to be selective to cause the proper actions to be taken. In small cases of fraud, the fraudsters are often forced to quietly resign in order for the organization to avoid the lengthy and public process of prosecution. All fraud, whether outrageous or not, needs to be addressed by today's organizations to set the proper ethical tone. In Chapter 2, we discuss the fact that even when someone is watching, fraud will continue. We will see why enhanced legislative, regulatory, and professional oversight is not helping auditors in the fight to combat fraud, and how through this understanding the nonauditor can grasp the necessary organizational tone to proactively establish the fight against fraud.

Regardless of outrage, the most successful fraud defense is interest.

## ONE-MINUTE FRAUD MYSTERY ANALYSIS

After reading this chapter, are you able to establish where the value exists in the process at Trust Us Inc.? Can you determine which people had access to the value, and where the company was vulnerable to fraud? Remember, you are the fact finder and need to apply divergent thinking. Here are some thoughts on this chapter's mystery based on my experience in the field:

- **Allegation.** The bank reconciliation and bank statement records do not match.
- **Probable cause.** At this point, you know that something has occurred. Either Favor or Trust could have been mistaken in their reconciliation, or they could have committed fraud. If Asset had discovered fraud, then it would appear that Favor was trying to cover her trail. It is also interesting that Favor went straight to the company's owner with her findings and did not address them with Asset.
- **Action.** Further questioning is necessary. A cautious approach is necessary for this situation. While you want to treat Betty Favor as a person of interest, you need to use the 800-pound friendly gorilla approach when investigating her. You need to understand the level of socialization and relationships that exist between the parties. Make note of the 15-year

relationship between the owner and Favor. Who else may be involved (the owner)? Is the relationship between them limited to this transaction or is it ongoing? Favor clearly has an understanding of the organizational business process and may be the potential ring leader. John Asset brought the problem to his direct supervisor (Favor), which appears to be the typical process. However, remember that Asset's involvement can only be dismissed after a proper investigation is complete. Do not rule out victims or parties that bring the problem to light. Rule them out only after the proper due diligence has been completed. Examine where the greed exists that enables the fraudster to start rationalizing his or her thinking. Are there external influences? Look for lifestyle changes. Look for conflicts of interest. Know your answers before you ask critical questions by having a well-thought-out and planned approach.

- **Preparation.** Get bank records directly from the bank (third-party documents are the best source) and start within the house records. Caution should be used; you may need to get the records without Favor's knowledge. Develop open-ended questions for brainstorming. Are the books audited by independent auditors? Develop a nonaccusatory theme when asking employees questions as to avoid raising their defenses. If the preparation phase gets too involved or complicated, bring in a high-level investigator with good communication skills to help. Questions to ask include the following:
  - Are the entries in the books and records being altered?
  - Are there overdrafts?
  - What is the financial condition of the organization and the parties involved?
  - How do the canceled checks compare to the general ledger?
- **People of interest.** Betty has knowledge of the process and the ability to override control, and her background has not been checked in 15 years. She is a trusted employee and is in the right position to succeed in perpetrating a fraud.
- **People-with-knowledge interview plan.** Interview John Asset first (least likely to commit fraud; he has no signing authority and reports to Favor), Betty Favor second (owner's "pet"; everything goes through her; enjoys personal gain), and the owner last (never assume the owner is not in on the fraud). Also, is it possible for any other parties to have knowledge of the potential fraud?
- **Documentary evidence.** Collect bank statements and all supporting documentation, including bank reconciliations, tax returns, general ledgers (organized or messy?), financial statements, and loan applications.

- **Formulate opinion.** Embezzlement. Greed. Long-standing relationship situation, with a well-established level of trust bestowed on one individual. Owner is involved directly or indirectly, since there is a lack of 800-pound friendly gorilla oversight in Trust Us Inc. See if the company documents conflict, because there is the potential of embezzlement. The difference between larceny and embezzlement is that in the latter, employees and owners have authorized access to the funds. You need to develop proof. An example could be outstanding checks that never seemed to clear.

## 800-Pound Friendly Gorilla Suggestions for Trust Us Inc.

Trust Us Inc. was in need of a better control system to protect itself from fraud. It had no controls in place to deter, detect, and prevent fraud, and its systems could be overriden. The fraud was discovered inadvertently when a new employee was hired. Trust Us Inc. needs to establish a new level of thinking to protect itself from further fraud. It needs an 800-pound friendly gorilla solution. Too much trust in any one person can lead to fraud. The following actions are needed to reduce the risk of fraud in the organization, and it is a good starting point to begin by developing the 800-pound friendly gorilla protection needed to safeguard the organization and implement the following tactics to reduce the risk of fraud:

- Separate the authorization of the transactions from their recording.
- Monitor the responsibilities given to people with access to the organization's value.
- Require multiple signatures.
- Perform background checks initially and annually.
- Institute a policy of job rotation.
- Have employees bonded with the proper insurance policies (to reduce risk exposure).
- Institute a mandatory vacation policy.
- Create annual financial disclosure policies for the people in the organizational process.
- Define the trust levels with the appropriate checks and balances as needed.



## A Simple Picture

As I mentioned earlier, I gave the facts of this chapter's one-minute fraud mystery to my cousin's daughter Lindsay, a 16-year-old sophomore in high school, and asked her to draw her perspective of what happened based on the facts at

the start of this chapter. Where does the greed exist in Exhibit 1.10? Lindsay's drawing clearly indicates who has access to the money and organizational value. It also shows the reporting functions. In this one image, you can see where the organization is susceptible to fraud through the fact that Betty has direct access to the cash. In the end, we need to articulate the evidence and

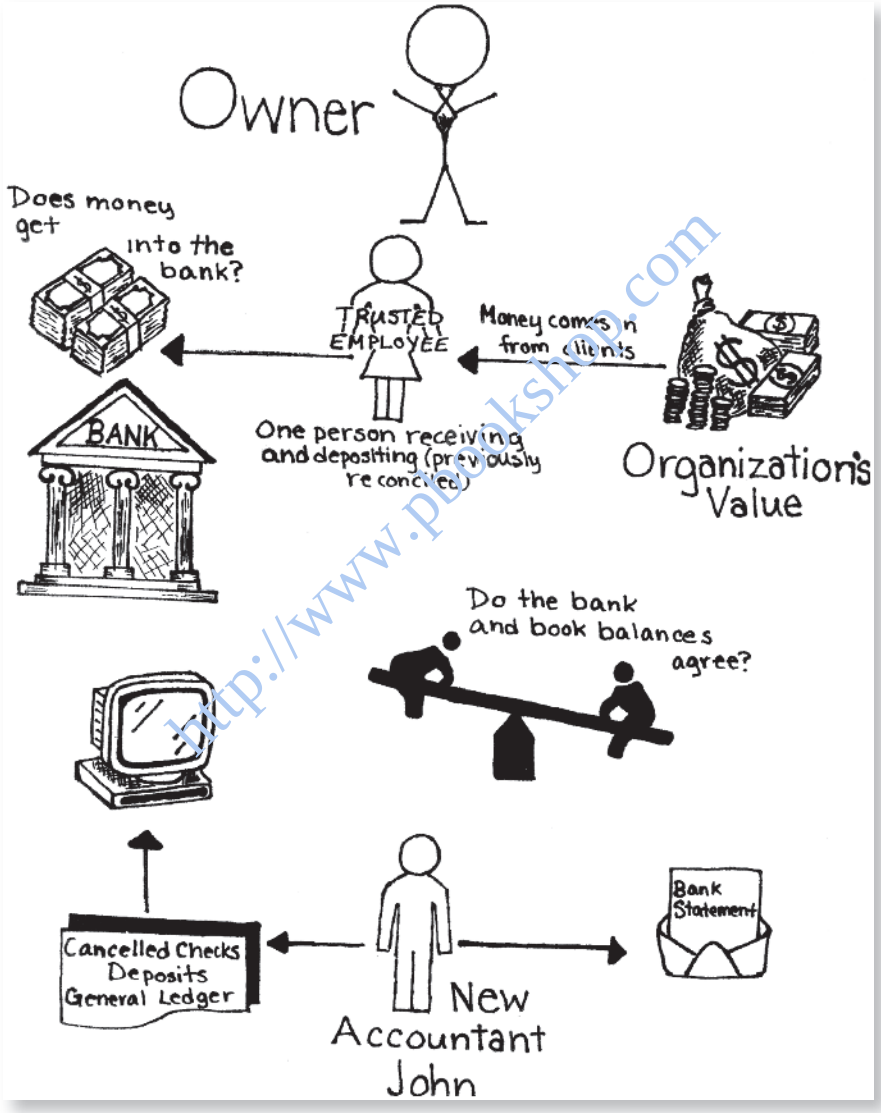




**EXHIBIT 1.10** Trust Us Inc. Drawing

supports in the same simplistic manner that Lindsay has in this drawing by focusing on the relevant facts. The simpler the approach that the organization utilizes to expose where people and value meet in a process, the greater the chances are for deterring, detecting, and preventing organizational fraud.

## NOTES

1. A bank reconciliation is a critical fraud review process that ensures the transactions on the books are consistent with the bank. The bank statement is a third-party source document. Third-party source documents are able to be obtained independently, which aids you in your fraud investigation since the person of interest may not know that he or she is being investigated. Third-party information is the most reliable source when obtained directly from the third party, assuming that the third party is not involved in the fraud and has not altered the document.
2. David Porter, "Ex-Lawyer Gets Longest Insider Trading Sentence Ever, Associated Press, June 5, 2012, http://www.dailyfinance.com/2012/06/05/ex-lawyer-gets-longest-insider-trading-sentence-ever.
3. *Merriam-Webster's Collegiate Dictionary*, 11th ed., http://www.merriam-webster.com/dictionary/fraud?show=0&t=1322278715.
4. The Free Dictionary by Farlex. *Fraud. The American Heritage Dictionary of the English Language*, 4th ed. (Boston, MA: Houghton Mifflin, 2001), http://www.thefreedictionary.com/fraud.
5. Stephen H. Gifis, "Fraud," *Law Dictionary* (Hauppauge, NY: Barron's, 1984).
6. Internal Revenue Service, "Definition of Fraud," *Internal Revenue Manual*, Sec. 25.1.1.2, July 18, 2008, http://www.irs.gov/irm/part25/irm_25-001-001.html.
7. American Institute of Certified Public Accountants (AICPA), Codification of Auditing Standards AU Section 316 (formerly Statement on Auditing Standards [SAS] 99). AICPA's definition neither contemplates corruption (e.g., kickbacks or bid rigging) nor requires financial injury.
8. Association of Certified Fraud Examiners, *2010 Fraud Examiners' Manual* (Austin, TX: ACFE, 2010), 2.201.
9. The Institute of Internal Auditors, *Glossary*, http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/full-standards/?i=8317.
10. According to Association of Certified Fraud Examiners, *2012 Report to the Nations*, entities, on the average, lose 5 to 7 percent of their revenues to fraud annually.
11. Albert Einstein and Sonja Bargmann, *Ideas and Opinions* (New York: Crown Publishers, 1982).
12. This classification system was first introduced in Association of Certified Fraud Examiners, *1996 Report to the Nations* and *2010 Report to the Nations.*

13. Association of Certified Fraud Examiners, *2010 Fraud Examiners' Manual*, Sec. 2.201. Frauds classified as "statutory offenses" include those resulting from the violation of federal or state laws. Some of the more significant federal laws are the Sarbanes-Oxley Act, the Dodd-Frank Act, the False Claims Act (as modified), the Honest Services Fraud Act, and the Foreign Corrupt Practices Act.
14. Donald R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement* (New York: Free Press, 1953).
15. David T. Wolfe and Dana R. Hermanson, "The Fraud Diamond: Considering the Four Elements of Fraud," *The CPA Journal* (December 2004), http://www.nyscpa.org/printversions/cpaj/2004/1204/p38htm.
16. Jonathan Marks, "Playing Offense in a High-risk Environment," Crowe Horwath International, http://www.crowehorwath.com/folio-pdf/RISK8115_PlayingOffenseWP_lo.pdf.
17. Ibid.
18. The Sarbanes–Oxley Act, enacted July 30, 2002, created the Public Company Accounting Oversight Board and the Investor Protection Act. It is commonly referred to as Sarbanes–Oxley, Sarbox, or SOX. The Wall Street Reform and Consumer Protection Act, commonly referred to as the Dodd–Frank Act, is a federal statute that implements financial regulatory reform; it was signed into law by President Barack Obama on July 21, 2010.
19. Herb Greenberg, "Making a Strong Case for Sarbanes-Oxley: A Former Crook Argues against Watering Down Securities Laws" *Market Watch*, October 11, 2006, http://www.marketwatch.com/story/a-reformed-crooks-view-of-sarbanes-oxley. A detailed discussion of the Crazy Eddie Inc. fraud can be found on Sam Antar's website, http://www.whitecollarfraud.com.
20. The Securities and Exchange Commission suggests a 5 percent starting point in developing a materiality threshold. Similarly, there is no absolute definition of *materiality* for Internal Revenue Service purposes. Generally, if something has the ability to influence another's actions, it is material.
21. Dr. Seuss, *The Lorax* (New York: Random House, 1971).
22. The Public Company Accounting Oversight Board's website, http://www.pcaobus.org, contains a wealth of information about the group's mission as well as the oversight it provides, including inspections and enforcement and its liaison with the Securities and Exchange Commission.
23. We presume that Senator Sarbanes and Representative Oxley had qualified personnel advising them on relevant matters. The point is that lawyers are again proposing to fix a potentially broken system by creating additional layers of oversight (which potentially divert the resources available to address the matter directly) and not by enhancing education and awareness.
24. "The Objective of Education is Learning, Not Teaching," Knowledge Wharton. University of Pennsylvania. August 20, 2008, http://knowledge.wharton.upenn.edu/article.cfm?articleid=2032.