CHAPTER 1

The Fraud Problem

After reading this chapter, you will be able to

- Understand the results of fraud prevention efforts over the last several years.
- Identify the three main components of any fraud scheme, traditionally known as the fraud triangle.
- Discuss the various actions companies take against those who perpetrate fraud and the reasons why they do not initiate criminal prosecutions.

Internal fraud at companies is a big enough problem to be considered an industry unto itself. It is estimated that organizations lose an average of 5% of revenue annually to internal fraud, which equates to $652 billion in losses each year just in the United States.[1]

People often wonder why so much fraud occurs and why it is not caught sooner, thereby limiting the losses. The answer is simple. Companies have systems in place to help ensure that accounting transactions are recorded accurately and that proper procedures are followed. Companies have policies to guide the behavior of people who would generally strive to act in an ethical manner, but occasionally need rules to dictate their behavior. Those systems, procedures, and policies often work to catch errors and honest mistakes in the accounting process.

However, when an employee is committing fraud, he or she is deliberately trying to thwart those systems and policies. The person is purposely circumventing the system, while at the same time attempting to conceal his or her actions. While systems, policies, and procedures may be reasonably good at bringing errors to light, they typically cannot and do not expose fraud. Fraud constitutes a purposeful disregard for the system and a deliberate attempt to violate that system for personal gain, and most companies' systems aren't designed to stop this.

There are also the companies that have inadequate or nonexistent systems to ensure accurate accounting records and financial statements. Those companies can barely keep adequate and reliable records, even with honest employees. But if they can't even ensure a basic level of accuracy, management will hardly be able to prevent, detect, and stop fraud from within.

Internal fraud itself is troubling. Companies entrust their employees with assets, information, and customers. Business cannot be done unless companies put trust in people to sell their products or services, deliver them, collect the money, and keep accurate records.

Employees must be charged with growing and managing the business, as well as doing what is in the best interest of the owners and the rest of the company. When those trusted people steal, it can be disheartening. Maybe even more troubling is the fact that so little of the proceeds of fraud are ever recovered.

A 2006 fraud survey by KPMG[2] found that in 42% of major frauds, none of the stolen goods or money was recovered. None. The Association of Certified Fraud Examiners (ACFE) found equally disappointing results in its 2006 survey of fraud examiners. In 42% of internal fraud cases, there was no recovery of money or assets, and in 23% of cases, the recovery amounted to 25% or less of what was stolen.[3] As both of these studies show, close to half of internal fraud victims cannot count on recovering any of the proceeds of fraud, and another one-fourth will recover only a fraction of what was stolen. Clearly, companies cannot and should not expect to recover fraud proceeds.

Progress?

With the focus on fraud since the big cases of Enron, WorldCom, and Tyco, an important question is whether or not companies are making any progress in the fight against fraud. Has the focus on the fraud issue caused them to tighten controls and take swift action against perpetrators, or have companies remained largely complacent in fighting fraud?

The general consensus seems to be that companies have made some progress in protecting themselves against fraud, but still there has not been a noticeable decrease in fraud overall. Some might argue that the progress has not been swift enough, and that is why no real results have been seen. It also may be that companies have been so focused on compliance with Sarbanes–Oxley, that most of the measures taken are merely for the sake of compliance and not designed for true fraud prevention. Companies may think that they have improved in terms of fraud prevention and detection, but that self-assessment can often be overly optimistic. Until a marked decrease in fraud is seen worldwide, the idea that companies have been effective at reducing fraud is dubious.

The ACFE conducted studies on fraud detection, investigation, and prevention in 1996, 2002, 2004, and 2006. In each of these studies, Certified Fraud Examiners were asked to estimate the amount of revenue companies lose each year to internal fraud. In the 1996, 2002, and 2004 reports, Certified Fraud Examiners estimated that 6% of revenues would be lost by companies as a result of occupational fraud and abuse. When applied to the U.S. gross domestic product, that would total $600 billion in 2002[4] and $660 billion in 2003.[5]

Five percent of revenues were estimated to be lost to internal fraud in 2006,[6] a 1% decrease from previous estimates. When applied to the 2005 U.S. gross domestic product, this is an estimated $652 billion lost to occupational fraud. It's important to remember that these particular figures are all estimates and there is much room for error. The most important conclusion we can draw from these surveys is that professional fraud investigators don't think the instance of employee fraud has decreased to any great extent during the past several years.

And let us not forget that any estimate of the total cost of fraud is just that—an estimate. There is no way for anyone to know the exact total impact of fraud, because we know that a lot of fraud goes undetected. All we are left to do is make educated guesses about the total cost of fraud by assessing the frauds that were discovered and making assumptions about the frauds that were not discovered.

How Companies See Themselves

The results of the 2006 KPMG fraud study suggest that fraud risk management is becoming more important to companies, and it is of increased importance when companies engage in strategic planning. Companies recognize the importance of image and reputation, and this may be fueling a focus on reducing fraud scandals.[7]

The study further indicates that companies are devoting more time and resources to fraud management, with the focus generally on fraud detection and reporting. Less emphasis is being placed on fraud prevention and responses to the discovery of fraud. Survey participants reported an overall decrease in the average time it took to detect a fraud as a result of this greater focus on fraud detection.[8]

While the increased focus on fraud detection is a good thing, the lack of attention to fraud prevention and management's response to fraud is troubling. As we will see later, a swift response to fraud is necessary to deter other employees from committing fraud. And clearly, fraud prevention efforts can pay dividends if only management would value such activities.

A 2006 global survey by Ernst & Young had findings similar to those of the KPMG study. The firm's survey of more than 500 corporate leaders found that companies had increased their spending on assessing and improving internal controls. As a result, the corporate leaders believed they had made significant progress in detecting and preventing internal fraud.[9]

Although survey participants felt better positioned to detect and prevent fraud, there was little hard evidence to prove that fraud has been reduced. One out of five companies surveyed by Ernst & Young reported "significant fraudulent activity" within the past two years.

These surveys seem to have one common theme: Corporate executives think their companies are doing better now than in the recent past when it comes to preventing fraud, but none of the hard data supports that assertion. That's dangerous. Executives and management may very well be caught off guard by a fraud while they hold onto this false sense of security. Unless management can come to grips with the true effectiveness (or lack of effectiveness) of a company's fraud detection and prevention efforts, marked improvement cannot be made.

Tips and Techniques

How Companies See Themselves

Overall, companies see themselves as having made significant improvements in fraud prevention and detection during the past several years. However, fraud does not appear to have been reduced, according to studies by anti-fraud professionals. There is clearly a disconnect between actual performance and the executives' perception of their performance.

Defining Fraud

Occupational fraud and abuse goes by many other names, including internal fraud, employee fraud, employee theft, and embezzlement. The phrases "occupational fraud" or "internal fraud" are often preferable when discussing corporate fraud, because they apply to a range of employee misconduct while the other terms are a bit more restrictive.

In lay person's terms, occupational fraud is something that

- Violates a person's fiduciary duties to the organization.
- Is done in secret and concealed.
- Is done for a direct or indirect benefit to the perpetrator.
- Costs the employer assets, revenue, or opportunities.

Legally speaking, fraud is generally defined as an intentionally false representation about a material point, which causes a victim to suffer harm. Essentially, when someone purposely lies about an important fact and someone else loses money because of that lie, a fraud has been committed. Most of the instances of fraud are fairly straightforward to prove. After all, it's usually pretty clear when something is false, and whether it was material and there was a loss to a victim.

TIPS AND TECHNIQUES

Legal Elements of Fraud

- Intentional
- False
- Representation
- Material point
- Victim suffers harm

It is not always so easy to prove intent. One of the first defenses that often surfaces in a fraud case is that the perpetrator simply made a mistake or error and there was no intent to defraud. In some situations, that may truly be the case. Plenty of errors are made daily in business, so that defense can't immediately be ruled out.

Fraud investigators, therefore, look for evidence of intent to defraud in the documents and actions of the accused. Manipulation of documents and evidence is often indicative of such intent. Innocent parties don't normally alter documents and conceal or destroy evidence. Although there may be times when these actions are taken to cover up a mistake due to fear of discipline, these things are usually perpetrated by those who had an active part in the fraud and its cover-up.

Obstruction of an investigation can also signal criminal intent on the part of a participant in a fraud scheme. Innocent parties don't usually lie or conceal information when being questioned relative to an occupational fraud. Naturally, employees are sometimes nervous or hesitant about providing information and evidence when fraud is being investigated. They may be reluctant to participate in an interview because of the fear of implicating others in the fraud. But again, innocent parties are, for the most part, not inclined to cover up evidence or lie about the situation. Therefore, false statements and other obstruction of an investigation can be another factor that points to the intent to defraud.

Finally, two additional factors to consider when determining the intent of an involved party are past behavior and the benefits obtained from the fraud. Employees, managers, and executives who have a prior history of engaging in unacceptable behavior or being involved in inappropriate transactions should be eyed carefully. Although past behavior doesn't prove fraud in a current investigation, a pattern of unethical behavior certainly indicates something about the character and tendencies of the accused.

It is important to determine whether an individual obtained any benefits from a suspected fraud. Typically, errors are exactly that—errors that don't personally benefit the person responsible. However, a transaction that creates a direct or indirect benefit for the person involved should be viewed as suspicious. Fraud is meant to give illegitimate benefits to the parties involved, and those benefits may be indicators of a participant's intent to defraud.

None of these factors alone can prove intent to defraud beyond all doubt. In the absence of a confession from the accused, intent may need to be established by compiling a list of behaviors that signal the intent. The more factors identified in the commission of a fraud, the closer we come to proving that a fraudster intended to commit the crime.

Fraud Triangle

One of the most basic concepts in the field of fraud examination originated with the famous criminologist, Donald R. Cressey. While doing research for his doctoral thesis in the 1950s, Cressey developed the following hypothesis about fraud:

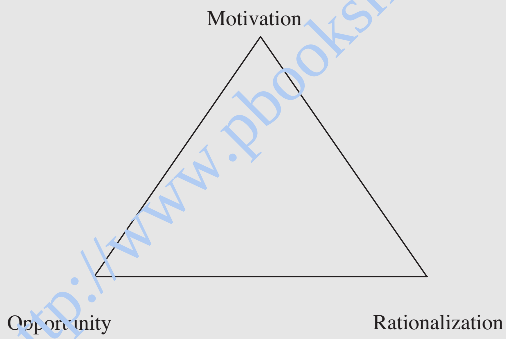
> Trusted persons become trust violators when they conceive of themselves as having a financial problem which is nonsharable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted

persons with their conceptions of themselves as users of the entrusted funds or property.[10]

Quite simply put, Cressey's hypothesis states that three key elements are present in every internal fraud: motivation, opportunity, and rationalization. These three elements have become known as the "fraud triangle." Contemporary academics and investigators have added their own ideas to modify this concept, but the fraud triangle is still the most widely recognized basic framework of fraud.

TIPS AND TECHNIQUES

Fraud Triangle



Motivation

The motivation component of fraud or embezzlement is the pressure or "need" that a person feels. It could be a true financial need, such as the need to replace belongings after a house fire. Other real needs may include financial distress from a lost job, high medical bills, child support payments, investment losses, or heavy personal debt.

The motivation could also be a *perceived* financial need, whereby a person strongly desires material goods but doesn't have the money or means to acquire them. A person may also have an addiction such as gambling or drugs, and that could be a motivator. Nonfinancial pressures and motivators may be in play as well, and these could include such things as the expectation for good results at work, the imposition of unachievable goals, or the need to cover up a poorly performed job. Any pressure in one's business or personal life could conceivably motivate someone to commit occupational fraud.

IN THE REAL WORLD

Gambling as a Motivation for Fraud

Looking back over the past 10 or 20 years, it may have been unusual to hear about a fraud scheme in which the perpetrator had a gambling addiction. Today, anecdotal evidence suggests that this is occurring more and more often.

Opportunities for gambling are increasing as casinos open across the country. Gambling is now recognized as an addiction that is not too different from alcohol or drugs. It can be a strong motivator to commit fraud, as casinos are clearly set up in order to make the gamblers lose. It's a habit that gets expensive very quickly.

Further complicating the problem is the belief on the part of many problem gamblers that one day they will win big and will pay back the theft from the company. This makes it much easier for an employee to justify the theft in her or his mind.

Opportunity

The opportunity to commit fraud includes the access to assets, people, information, and computer systems that enables the person not only to commit the fraud but to conceal it. Employees are given all sorts of access to assets and records in order to carry out their job duties, and that access is one of the key components of fraud. This is why it is so important to limit employees' access to only the assets, systems, and information that are necessary for them to properly perform their jobs.

As corporate structures have become more complex and managers have become responsible for a wider range of employees and functions, individual employees have been given more access and control. Increased access to resources and data, along with increased control over functional areas of companies, has created a situation in which it may be easier than ever to commit occupational fraud. Obviously, these increased opportunities to commit fraud involve risk, but in many ways they are unavoidable in the modern business world.

Rationalization

The third and final piece of the fraud triangle is rationalization. This is the process by which an employee determines that the fraudulent behavior is "okay" in her or his mind. For those with deficient moral codes, the process of rationalization is easy. For those with higher moral standards, it may not be quite so easy; they may have to convince themselves that a fraud is okay by creating "excuses" in their minds. A thief may convince himself that his theft just makes up for the bonus or raise that he should have received but did not. An embezzler may tell herself that she is just "borrowing" money from the company and that she will eventually pay it back. Maybe the rationalization is that no one will "miss" the funds or assets, or that the company "deserves" the theft because of lax supervision and security.

Management has the most control over the opportunity portion of the fraud triangle. It can limit access to assets and put controls in place that ensure monitoring of systems and people. Motivation can be constrained by management as well, although not to the degree that opportunity can be limited. The best way to reduce "needs" is by paying employees fairly (to reduce perceived financial burdens) and by creating performance systems that are reasonable (not requiring job performance beyond what is realistic).

Rationalization is probably the most dangerous piece of the fraud triangle because it is the one that companies have the least control over. It is nearly impossible for management to eliminate the rationalization piece because they can't control the minds of employees. Management has no way of knowing what lies an employee may tell himself in order to justify fraud in his mind, so there is virtually no way of counteracting the lies.

Characteristics of Internal Fraud

Employee fraud falls into at least one of three widely recognized general categories:

1. Asset misappropriation
2. Bribery and corruption
3. Financial statement fraud

Many fraud schemes include components from more than one of these three categories.

On average, an internal fraud scheme lasts 18 months and costs a company $159,000.[11] Almost one-fourth of the cases studied in the ACFE's 2006 *Report to the Nation* caused losses over $1 million.[12]

When two or more employees collude to commit an internal fraud, the losses to the company are more than four times higher than the losses from a single-person fraud.[13] The losses are dramatically higher when employees collude, because they are able to jointly cover up the fraud. A company with good supervision of employees and cross-checking of work may still fall victim to a fraud scheme if the right employees collude to cover one another's tracks. This collusion also increases the length of time a fraud scheme may continue without being detected.

Smaller companies are generally hit harder by fraud than larger companies. Their median dollar loss per fraud scheme is higher than in larger companies, and naturally, smaller companies have smaller budgets, which consequently feel an even greater impact from fraud.[14]

Detecting Internal Fraud

According to the 2006 study by the ACFE, 34% of frauds are detected through a tip from an employee, vendor, customer, or anonymous person.[15] This supports the idea of having anonymous hotlines available for people to report fraud, which will be discussed further on. If people are willing to report suspected fraud to the company, it makes sense to make it as easy as possible to report the suspicious behavior.

TIPS AND TECHNIQUES

How Fraud Is Discovered[a]

Tip: 34.2%

By Accident: 25.4%

Internal Audit: 20.2%

Internal Controls: 19.2%

External Audit: 12.0%

Notified by Police: 3.8%

Note: Some frauds had more than one reported method of discovery, causing the percentages here to exceed 100%.

[a]2006 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.

The next most common way to detect internal fraud is by accident. About 25% of frauds are detected this way.[16] An accidental detection may include a phone call routed to the wrong person, who then uncovers the fraud, or a piece of mail that is inadvertently intercepted, or some other chance event that causes an outside party to become aware of fraudulent activities. This statistic about accidental detection is very disturbing to fraud prevention professionals. In spite of all of the anti-fraud resources available to companies and the increased fraud prevention efforts management says are being undertaken, one-fourth of frauds are still discovered by accident.

Following closely behind in the fraud detection spectrum are internal audits and internal controls. Some may be surprised that these methods of detecting fraud end up in third and fourth place, given that they are often considered highly effective methods of preventing fraud. It is quite possible that companies still haven't developed internal controls sufficiently to make them as effective as they might be.

Tips and Techniques

Fraud Tips by Source[a]

Tips about internal fraud don't come only from employees. Outside parties can be a valuable source of credible fraud tips.

Employee: 64.1% of tips

Anonymous: 18.1% of tips

Customer: 10.7% of tips

Vendor: 7.1% of tips

[a]2006 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.

Why Audits Don't Find More Fraud

Users of financial statements often mistakenly believe that independent auditors are charged with finding fraud. If the auditors signed off on the financial statements, there must not be fraud. That couldn't be further from the truth, and boards of directors, investors, banks, and executives need to understand the real purpose of audits.

Audits by independent auditors are not designed to detect fraud, and most often they do not detect fraud that may be present. Instead, an audit is aimed only at determining whether the financial statements are free from material misstatements. That is, are the financial statements fairly presented, and do they give an accurate picture of the known financial condition of the company? The auditors test only a small number of transactions in this quest to audit the financial statements, and they will direct management to correct any material errors that are found during that testing.

In no way are auditors required to look for fraud in a company. They are required to be aware of the potential for fraud, to discuss ways fraud could be committed, and to exercise professional skepticism when auditing the books and records. If they come across evidence that may suggest that fraud is occurring, the auditors have some responsibility to look into those matters and report their findings to management or the board of directors. This is a fairly low level of responsibility, so outside auditors cannot be relied on to find fraud in companies.

Taking Action

Companies that fall victim to occupational fraud have several choices to make after the fraud has been discovered. First, the company must decide how much to investigate and who should do the investigating. But once the investigation results are in, the important choices need to be made.

Something has to be done about the employee or employees involved in the fraud. If no action is taken, it sets a bad precedent for other employees. Studies have found that when employees perceive that fraud is being detected and corrective action is taken, there can be a general deterrent effect. For this reason, employees need to know that there are fair and swift consequences for those who commit fraud.

If the company decides to punish the fraud perpetrator, the question remains how far to take the punishment. On one end of the spectrum is discipline, with the perpetrator remaining employed by the company. The discipline may be formal or informal and may include some agreement to repay the fraud proceeds.

Somewhere in the middle of the spectrum, the employee is terminated from the company. On the far end of the spectrum is legal action, either civil or criminal or both. Of course, litigation is expensive, and we've already seen that the likelihood of recovering the proceeds of fraud is low.

Criminal prosecution is many times difficult to initiate, inasmuch as local, state, and federal law enforcement agencies are always busy and seem to want to pursue only the largest or most egregious cases. Companies can often increase the likelihood of a criminal prosecution if they are willing to do a lot of the hard work at their own expense. A fully investigated case with well-organized evidence is much more appealing to law enforcement agencies than a case with many allegations but little substantive evidence uncovered.

Failing to Take Action

Plenty of companies take little or no legal action against perpetrators of occupational fraud. The ACFE asked why companies didn't refer their fraud cases to law enforcement. The most common reason was the fear of bad publicity, which accounted for 43% of cases. Thirty-three percent of cases were not pursued because management believed that internal discipline was sufficient. Thirty percent of cases were not pursued because a private settlement was reached, and 21% of cases were deemed too costly to pursue. Note also that some cases had more than one reason reported, causing the sum of the percentages to exceed 100%.[17]

Often companies just want to move forward and put the fraud in the past, particularly if it involved highly visible employees. Taking action against those who commit occupational fraud prolongs the pain and is an ongoing reminder of the fraud. That prospect is not appealing to many corporate managers and likely accounts for many of the companies that don't pursue employees who have stolen from them.

Why It Is Easy to Commit Fraud

Fraud can often be fairly easy to commit. Why is that so? One of the major reasons is that employers must put trust in their employees and give them access to data and assets. It's also important to remember that employers give responsibility to people who are trusted. If someone wasn't deemed trustworthy enough to take money to the bank, she or he wouldn't be handed the bank deposit. That trust inherently means that opportunities to commit fraud are handed to employees each day.

IN THE REAL WORLD

Trusting Employees

A family-owned manufacturing firm with a 15-year history of success was interested in growing significantly. One important strategic

In the Real World (continued)

step was the hiring of a chief financial officer (CFO). Up until that point, the finance function was managed with a combination of an in-house bookkeeper, an outside accounting firm, and the financial knowledge of the owner, who was an engineer.

Immediately after being hired, the new CFO began making changes to the finance procedures. The owners went along with all of it, believing that he had the best interest of the company at heart. Besides, he came highly recommended and was hired for his expertise in finance. He knew what he was doing!

The truth is that all of the CFO's changes were done to take information and control away from the owners while he was stealing everything the company owned. Any objection to new procedures or lack of information was met with an ''I'm the finance professional'' response.

In less than three years, the CFO succeeded at bankrupting the company while lining his own pockets with enough money to retire and live comfortably for the rest of his life.

The way modern business is conducted can contribute to the fraud problem. Managers are supervising many people and can't possibly watch over all of them. Some employees work offsite or telecommute, making supervision of them more difficult. Lack of real loyalty in the business world may contribute to the fraud problem because employees may have an easier time rationalizing bad acts.

Employees naturally become well educated on the inner workings of a company. They analyze portions of the company's business process day after day. They know where the gaps and weaknesses are.

They often know what will be reviewed by management and what will not. They are so close to their work that they are able to devise methods for concealing fraud. They see the details of their work each day and become intimately familiar with their part of the business. It is not difficult to find a way to exploit the system.

The fact that fraud is easy to commit is no excuse for employees to scam their employers. But executives and managers must become aware of the potential for fraud and must acknowledge the risk of fraud and the ease with which it may be committed.

Fraud-Fighting Lessons

As you will learn throughout the rest of this book, there is much work to be done by companies that want to reduce opportunities for fraud. Although the concept of internal controls goes back many years, management still has a lot of room for improvement. Specifically, internal controls at many companies need to be adjusted so that they better address fraud risks. Whereas internal controls at one time may have been primarily directed at preventing errors in the accounting system, in today's world those controls should focus on preventing fraud.

Companies that have anti-fraud programs in place also have room for improvement. The anti-fraud programs need to be more wide reaching and comprehensive. Comprehensive fraud prevention programs involve all levels of employees and should integrate internal controls with anti-fraud education and a formal ethics policy. It is clear that the current fraud prevention efforts of companies have not been effective, and this book aims to assist executives, attorneys, and auditors in learning the critical facts about fraud detection, investigation, and prevention.

Notes

1. 2006 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.
2. 2006 Fraud Survey by KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative.
3. 2006 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.
4. 2002 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.
5. 2004 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.
6. 2006 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.
7. 2006 Fraud Survey by KPMG.
8. Ibid.
9. 9th Global Fraud Survey: Fraud Risk in Emerging Markets, Ernst & Young, completed in 2006.
10. Cressey, Donald R., Other People's Money: A Study in the Social Psychology of Embezzlement, 1953 Edition. Boston: Wadsworth Publishing Co., 1972.
11. 2006 Report to the Nation, Association of Certified Fraud Examiners, Austin, TX.

12. Ibid.
13. Ibid.
14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.