

# CHAPTER 1

---

## Finding Fraud

There are two different ways that a reactive fraud investigation starts. One type of investigation begins when an actual fraud has been identified, and maybe one or more perpetrators are identified, too. The other type of investigation starts with a strong suspicion of fraud, but no real proof of theft.

Both types of investigations are important to any organization that takes fraud prevention and control seriously. Companies with good fraud prevention controls actively monitor their systems and follow up on questionable data and unusual relationships between numbers. The investigation that starts this way should not be viewed as any less important than the one that begins with a definitive instance of fraud.

### Signs of Fraud

---

Numerous signs can point to the possibility of fraud. Literally hundreds of different types of fraud schemes exist, so the number of possible red flags of fraud is huge. It would be impossible to cover them all in their entirety here, but some general signs of fraud can apply across all types of businesses and fraud schemes.

It is important to educate management and employees on these warning signs of fraud. Study after study indicates that tips from employees are one of the most common ways that corporate fraud is

detected. Therefore, it makes sense to educate employees about symptoms of fraud so they can report red flags when they see them.

### Accounting Irregularities

Irregularities that point to the possibility of fraud can range from simple things like unreconciled accounts and unusual account balances to more complex problems like “on-top entries,” which are made after the books are closed in order to manipulate the numbers ultimately reported on the financial statements.

An auto dealership had a controller who had not reconciled the bank accounts for nearly a year, despite management’s insistence that it be done. Management did not insist enough, and the problem persisted; the accounts remained unreconciled month after month. Unreconciled bank accounts usually signal one of two problems: The accounting staff is incompetent or understaffed, or there is a fraud-in-progress that will likely be exposed through a bank reconciliation. Both of these problems need to be corrected quickly.

In this case, it turned out that the controller simply couldn’t handle all of the responsibilities of her job. She was out of her league and was not doing the reconciliations because she did not have time and was likely afraid that the reconciliations would expose her incompetence. The reconciliations would have shown that she didn’t have a good handle on the company’s finances.

The auto dealership was lucky in this case. They simply dismissed the controller and hired someone more experienced and more competent. But there was a period of time during which management was afraid a fraud had occurred. They should have recognized early on that the unreconciled accounts were a sign of a big problem.

Cynthia Cooper, head of internal audit at WorldCom, recounts the on-top entries problem that she and her team discovered was part of a massive fraud scheme at the company. Executives were directing employees to make journal entries *on top* of the regular general ledger activity to make the financial statements conform to a predetermined template. Lower-level employees did not see these entries, because they

occurred outside the regular system of recording accounting details, so the practice went on for a long time before it was discovered.

To further confuse anyone who might look at the on-top entries, executives directed a web of confusing entries to be made. They were not a handful of simple debits and credits. There were hundreds of entries, with figures divided and bounced between many different accounts, apparently in an attempt to confuse and discourage anyone who might try to dig into these entries. The existence of these entries was discovered because of some irregular numbers and account names by the internal audit team. This demonstrates the importance of being on the lookout for unusual accounts, numbers, and descriptions within the accounting system.

It's not always easy to spot accounting irregularities. After all, an employee or executive who engages in fraud is often aware of what others are expecting their work or their numbers to look like. In many companies, management knows that revenue and expenses are expected to fall within certain parameters. Numbers outside of those expectations might raise suspicions. So a good fraudster will ensure that the numbers do not appear unusual in that regard. It's only when someone digs deeper that the irregularities start to surface. An examination of a public company's Securities and Exchange Commission (SEC) filings might reveal some notes or disclosures that do not make sense in light of the numbers reported. Small clues like these will be necessary to point to irregularities.

For example, suppose a company reports in the notes to the year-end financial statements that the raw materials used to make its products have become significantly more expensive. An examination of the company's gross profit margin, however, shows that the percentage is stable. The only legitimate way for the gross profit percentage to remain unchanged during a period in which raw material prices increase significantly is for the sales price of the goods to rise proportionately. The sales prices at this company did not change, however, so that immediately raises a red flag about that unchanged gross profit margin. The numbers reported don't make sense in light of the information provided in the notes. This should definitely be examined further.

It is clear that the accounting irregularities giving rise to a fraud investigation may not be easily identifiable. Those committing financial statement fraud are often adept at covering their tracks, so the red flags are not always obvious. The investigator often relies on intuition when examining the numbers and explanations for possible irregularities.

### Apparent Control Weaknesses

When readily apparent major deficiencies in a company's control procedures are identified, they should be considered warning signs that fraud could be occurring. All companies have some things that are not as secure as they should be. However, when the controls over a company's assets and data are severely deficient, that is cause for alarm.

Some of the most common characteristics that might be considered severe deficiencies include:

- *Complete lack of segregation of critical duties*, giving one or more persons almost complete control over a financial area of a company and offering many opportunities to commit fraud and easily conceal it. For example, if the same person receives customer payments, records the payments to the customer's accounts, makes the bank deposits, and reconciles the bank statement, there are many opportunities to commit and conceal fraud. The employee could steal a customer payment, record the payment on the customer's account so the customer doesn't know the funds have been stolen, and later adjust the accounting records while doing the bank reconciliation in order to cover the theft. If these duties are segregated among two or three employees, the risk of theft of a customer payment and subsequent acts to cover the theft are much less likely.
- *Ability to override controls and limits of authority easily*, either with no oversight of the process or with lax enforcement of it. For example, an area supervisor regularly exceeds his authority for vendor payments. His approval limit is capped at \$20,000. He commonly requests that vendors issue multiple invoices for work, so that no individual invoice exceeds the \$20,000 threshold. Upper management is aware of this situation, but does not enforce the policy or regularly monitor this

supervisor's activities. By failing to enforce the policy, management may be effectively encouraging the employee to continue to break rules, which could create opportunities for fraud.

- *Failure to reconcile accounts regularly.* Account reconciliation is important for accurate record keeping, even in the absence of fraud. Obviously, without reconciliations, management cannot know whether the books and records are accurate. Failure to reconcile also can encourage theft by employees who are aware that reconciliations are not done, and a theft could go unnoticed for a long time. In the example cited earlier in this chapter, management did not enforce its policy requiring monthly reconciliation of accounts, which led to a significant problem in the accounting function.
- *Poor accounting records in general.* This problem is often faced by smaller companies, but can also affect large companies, particularly ones that have done many acquisitions and have failed to integrate. Disjointed accounting systems make things difficult to monitor and reconcile, and offer opportunities for duplicate accounting entries to go unnoticed. Poor records also make it difficult for management to get an accurate financial picture of the company, and that could contribute to a fraud going unnoticed for a period of time.

It makes sense that the existence of major deficiencies in preventing fraud might be the precursor to fraud actually occurring at a company. If a company is lucky, it will catch the weaknesses before something happens. But many companies are not so lucky, and the identification of these types of problems should lead to further examination of the company to determine whether, in fact, fraud may have occurred under these serious circumstances.

If a company is not diligent about implementing good control procedures over its accounting function, it's also likely that management will not be interested in looking for the fraud that might result from the poor controls. Hopefully, internal or external fraud experts can encourage management to identify and examine the weaknesses and their results.

Another problem is that, when serious problems are found, a company often either ignores the problems or fixes them without looking

into whether a defalcation is associated with the control weaknesses. As difficult as it may be for management to admit that weaknesses like this may have led to fraud, it is important to find out for sure what the fraud status is.

### **Lack of Information**

When information and documentation is unavailable, it can raise questions about honesty or dishonesty. In the regular course of business, documents are sometimes lost or things cannot be explained. However, there comes a time when too many items are missing or the missing information is too suspicious to ignore.

For example, the bookkeeper of a nonprofit organization frequently had difficulty locating canceled checks that were requested by the auditors as part of their annual financial statement audits. The auditors instead relied on the information on the carbon copies in conjunction with the general ledger detail. Unfortunately, the payees noted on the carbon copies were not accurate, and the checks in question were actually issued to the bookkeeper. She destroyed these canceled checks as soon as the bank statement arrived, and hoped that the auditors wouldn't request copies of those specific checks.

When an occasional document is missing, it is usually not cause for alarm. But if a pattern of missing documentation emerges, it can be a warning sign of fraud. Look for missing information of a grouped or patterned nature: blocks of time, for a particular customer or vendor, for a certain type of transaction, or relating to a certain employee. A missing document or two is not all that disturbing, but ten missing documents, all related to one vendor—and all being questioned by management—are bothersome.

### **Apparent Deception**

When people seem to be going out of their way to conceal information, alter documentation, or otherwise engage in behavior designed to deceive those looking for facts (auditors, superiors, investigators, etc.), it raises suspicions about fraud.

For example, a disability insurance claimant fills out all paperwork, but does not mention her ownership interest in a business that is closely related to the job that she is currently unable to perform. A fraud investigator discovers the business ownership independently and becomes suspicious that the claimant may actually be working in this business, even though she claims she cannot work at her regular job due to disability. This ownership interest merits additional scrutiny. People often don't hide things like this without good reason. It is possible that the claimant wanted to hide this ownership interest because it might lead to the investigator finding out she was working there. If she was not working there, and there was truly nothing to hide, why conceal it?

The same goes for deceptions in any type of fraud investigation or audit. It is presumed that if people are not honest about their involvement in situations, ownership of assets, professional licensing, or other material facts, they may have something to hide. Investigators should take clues like this very seriously. Lying is usually not compartmentalized. A deception in one area of life or a business is not usually an isolated incident. Take deception—either with outright lies or through the deliberate omission of critical information—as a likely sign of other problems.

### **Tips about Fraud**

Companies rely heavily on reports about questionable behavior from employees, customers, vendors, or other outside parties. Tips are one of the most common ways that fraud is detected by companies, so any credible tip should be taken very seriously.

How does a company evaluate the credibility of a tip? It does not generally matter whether the tipster is anonymous, although it's reasonable to believe that those willing to put their names behind information do bring some measure of credibility to the information they are providing. Reliable tips usually have a sufficient amount of detail as to be believable. The more vague the tip is, the less reliable it is likely to be. The information provided by the tipster should also make sense in light of known circumstances surrounding the company's operation and the accused.

For example, a tip that merely states that Joe in the shipping department is acting like something unusual is going on is probably not very credible. In contrast, a report that Joe in shipping was seen in the shipping area several hours after his shift was over is a more specific tip that may be more reliable. If Joe was reported to be in the shipping and receiving area at a time when he is normally not working, and the door of the loading dock is open, this level of detail adds credibility to the report.

People do sometimes report false information in order to cause trouble for an enemy, an ex-spouse, or a disliked coworker, however. It is important to assess the potential motivation of a tipster when evaluating the information.

### Change in Behavior or Lifestyle

When an employee exhibits significant changes in behavior, this is a potential sign of fraud. Drug and alcohol problems could be precursors to fraud because of the expense of addiction, or they could be the result of fraud as a person tries to hide a guilty conscience.

Behavioral changes, such as becoming uncooperative, argumentative, or defensive, can be signs of problems as well. These behaviors may be signs of dissatisfaction at work, which could be a reason for an employee to commit fraud. Or they could be an outward sign of an employee's stress as she or he engages in on-the-job fraud.

Newfound wealth is often difficult for a person to hide. Despite an employee's best efforts to keep a fraud under wraps, buying a new car or fancy jewelry may be too much to resist. Spending beyond one's apparent means should be a warning sign that a fraud may be occurring.

Management at a small company was surprised when the bookkeeper arrived at work one day on a brand-new Harley-Davidson motorcycle. Employees knew this was an expensive bike, and there was a general feeling that the bookkeeper and her husband weren't in a position to afford this luxury item. No one voiced their concerns to anyone else, because they did not want to seem judgmental about the bookkeeper's financial choices. They thought they ought to mind their own business.

Less than a year later, management discovered that the bookkeeper had been engaged in a long-term scheme to defraud the company. This fraud scheme was apparently the source of funds used to buy the Harley-Davidson. Had management investigated this unusual situation immediately, the company might have saved tens of thousands of dollars lost to theft after that luxury purchase.

None of these lifestyle changes alone is a definite indicator that fraud is occurring. Even several of these characteristics identified in one employee may not mean that a fraud is in progress. However, these signs are small pieces of a puzzle, and they should be watched carefully, because they are sometimes related to an occupational fraud.

### **Investigative Intuition**

The least scientific of all the signs that fraud could be occurring may be the gut feeling that something is not right. Seasoned fraud investigators often refer to a “sixth sense” they get when examining situations and documents. This intuition is important in identifying instances of fraud and in looking for avenues to investigate in a suspected fraud scheme. Look for facts and relationships that don’t make sense. Analyze relationships between people and between facts that seem unusual or counter-intuitive. Find behavior that seems suspicious or out-of-the-ordinary.

A hunch, suspicion, feeling, or intuition requires further information and examination of data. When an investigator has developed her or his intuition related to fraud investigations, she or he cannot ignore the signs and fail to gather further information. Investigative intuition is a skill that can be developed over time and can be invaluable in fraud investigations.

### **Looking for Suspects**

---

Those aware of fraud risks might think they should be on the lookout for likely fraud suspects. That is not a bad idea, and there are many potential personal red flags of fraud, but it is difficult to put those who commit fraud into one little box. Many different types of people commit

fraud; it is difficult to pinpoint a few types who are more likely to steal from their employers.

It's important to recognize that there are inherently bad people who look for situations in which to take advantage of others. Companies try to avoid hiring these people but do not always weed them out because they may be good actors who are able to cover their evil intent. More likely, a company is a victim of a situational fraudster—someone who has a particular reason to commit a fraud at a certain time. This person would not normally be considered a bad or unethical person, but circumstances at home or work may motivate the employee to commit fraud.

A wide range of factors could cause a person to turn to fraud, including a legitimate financial need, a plan to get revenge on someone, a house going into foreclosure, a child support or alimony burden, an expensive addiction to drugs, a desire to engage in risky behavior for a thrill, or a feeling of power desired by the employee.

The motivators don't necessarily have to be evil-sounding. They can be everyday stresses and burdens that people find themselves susceptible to. Whatever the reasons or personal characteristics of a person who commits fraud, management will often be surprised by the identity of the dishonest employee. It is most often someone who was trusted and widely regarded as a good employee. It is only logical that the trusted employees would have access and opportunity to commit fraud. Managers typically do not provide access to information and assets for employees they don't trust. Only the trusted employees can access the bank accounts and look at confidential information—exactly the type of access that is needed to commit fraud.

When a doctor finds that her longtime bookkeeper has been stealing from her medical practice, she is often shocked. This was the woman she trusted for years to make the bank deposits, send out the bills, and generally handle the finances. How and why did fraud happen? Most often, that trust created between a business owner and an employee is exploited for financial gain. The bookkeeper knows the doctor is not looking at the bank statements, and therefore will not identify improper payments. The doctor does not have a good feel for the volume that is billed each month, and will not notice if the bookkeeper steals some cash

payments from patients. The doctor trusted the bookkeeper to handle the money, and the employee was probably loyal and worthy of trust for years. But the combination of little oversight by the doctor and a personal financial need could cause an honest bookkeeper to turn to fraud.

A situation like this illustrates just how easy it is for an owner or executive to be defrauded by the least likely suspect. It is important to be aware of red flags that fraud may be occurring, and it is even more important to implement controls and oversights to prevent even the most seemingly honest employees from committing fraud.

### **Evaluating Fraud Tips**

---

One of the most common ways that an internal fraud is detected is through a tip, from either an employee, a customer, a vendor, or an outside party. Anonymous hotlines are excellent tools for reporting fraud, but management must have a plan for evaluating these tips.

Some tipsters are okay with revealing their identities from the start. Others fear retribution or damage to their own reputations, so they prefer anonymous reporting. Just because a tip is anonymous, that does not mean it is any less credible than an allegation made by someone who is open about her or his identity. However, if someone is willing to reveal her or his identity when providing a tip, it may lend additional credibility to the information. Employees are sometimes worried that a hotline or other anonymous reporting mechanism might lead people to make false reports about others. While this does happen sometimes, those reports usually appear suspicious and are quickly identified as meritless.

Legitimate tips usually have specific (rather than general) allegations, sufficient information as to be believable, and a fact pattern that seems to fit with known variables in the workplace (the facts make sense). For example, a tip that indicates Janet in accounting is stealing customer payments would seem unreliable if Janet's job duties are such that she never comes into contact with customer payments. Management may want to verify that Janet does not have unintended access to those funds. If it can be verified that she does not have any access (authorized or unauthorized), the tip can likely be ruled out as bogus.

In contrast, if a report comes in that William in accounting is issuing payments to a fake company, and he is the employee who regularly generates accounts payable checks, that tip seems to make sense. The details will have to be investigated, but it is immediately clear that this fraud is possible given William's job duties.

How does management handle a tip? It is not wise to immediately dismiss the allegations, even if they seem completely baseless or are likely a hoax. In those cases, management should do some preliminary verification of facts. If this initial work completely debunks what was reported, it is probably okay to not investigate further. If the fact-checking finds that some or all of the representations in the tip are true, however, then further investigation is definitely warranted. The more facts that check out and the more serious the allegations, the more management should consider a formal investigation.

Suppose that a tip comes in about Amy, a commissioned salesperson, creating bogus sales at the end of the month to increase her monthly commissions. Management has noticed that commission payouts have been a bit higher than normal, and that the number of canceled orders has been unusually high. If Amy was causing false orders to be entered into the system, that would cause the commission payouts to be higher than they should. Higher-than-normal order cancellations could be related to Amy canceling orders after the month is closed and the commissions are calculated.

Management could then take the additional step of querying the accounting system to see whose customer orders are being canceled. If Amy's cancellations seem unusually high compared to everyone else's, this is another indicator that the tip may be credible. There is enough information backing up the allegations from the tipster, such that management should continue to look into the potential that a fraud is occurring.

### **Should You Investigate?**

---

When an internal fraud occurs at a company, the natural reaction is to assume that an investigation must be started immediately. After all, it is important to determine who was involved, exactly how the fraud was committed and covered, and what evidence exists to prove the fraud.

Intuitively, that makes sense. In reality, it's not always the way things go. Whether a fraud is fully investigated often depends on the estimated size of the fraud and the size of the company in question. It does not always make sense for a company to investigate a fraud because of the cost involved.

For a public company, an internal fraud is probably always going to be investigated to some degree, and the larger the fraud, the larger the investigation. Many regulations must be followed, and it's imperative that financial statements be restated if necessary. To determine the amount of the fraud, the effect on the financial statements, and whether the financial statements need to be restated, an in-depth investigation is usually required.

But for private companies, it is not so certain that an investigation must be done. There are a variety of reasons why. It is important to first understand that the recovery of the proceeds of fraud is typically very small. The Association of Certified Fraud Examiners (ACFE) reports that in more than 65% of cases, 25% or less of the amount stolen is recovered.<sup>1</sup> So to undertake an investigation with the intention of recovering significant money from the thief is probably misguided. If a victim company is fortunate enough to have insurance coverage for the fraud, an investigation must be initiated to help compile a proper insurance claim with supporting documentation.

Yet there are times when an investigation should be done, even if money is unlikely to be recovered. Management may conduct an investigation because they are not sure who was involved in the fraud and need to identify all responsible parties. They may also be unsure of the exact methods used in the commission of the fraud, and an investigation will help nail down this aspect. Fraud investigations play an important part in fraud prevention efforts; finding out exactly how a fraud was perpetrated and who was involved can go a long way toward preventing future frauds.

## **Confronting Suspects**

---

When management suspects a fraud has occurred, it is often difficult to decide whether to confront the suspect. Those who decide in favor

of confrontation immediately start questioning the suspect. They usually have good intentions, but the situation can go wrong very quickly. Usually the goal is to gather information about the suspected fraud, and it is believed that confronting the suspect will accomplish this goal. That is the thinking of someone who is not experienced in fraud investigation.

Often there is only *one* chance to speak with a suspect about the situation, so it must be done carefully. Once management reveals its suspicions, the suspect often will not agree to future meetings, so no more information will be gathered from her or him. There is an art to interviewing suspects, as will be discussed in Chapter 6. It is best to leave these tenuous situations to the experts, or at the very least to someone who has some training in the field of interviewing.

Interviews with suspects are usually best done after the bulk of available information and evidence has been gathered and examined. Although human nature may cause us to want to start asking questions immediately, the better practice in most cases is to wait.

### Skills of a Fraud Investigator

---

The educational background of a good fraud investigator can fall into a wide range of disciplines. Fraud investigators have degrees in accounting, finance, police science, law, or criminal justice. There is no widely accepted course of study for fraud investigators, although those degree programs that offer a strong foundation in accounting and finance seem to prepare students well for the numerical component of fraud investigations.

Many excellent fraud examiners have a work history that is far more important than their educational background. On-the-job experience as a police detective, federal agent, insurance claims analyst, financial statement auditor, or financial analyst can lend itself well to a career in fraud investigations. It's not unusual for practical experience in the field to play a much bigger part in the fraud investigator's skills than any type of classroom training. The field of fraud examinations has an extremely varied range of educational and work experience. Other careers often have a few well-defined career paths, but the road to success as a fraud investigator can lead in many directions.

A strong financial background includes a working knowledge of financial statements and possibly a good grasp of the accounting process. Many successful investigators come from a background that did not necessarily focus on the process of accounting, so it is obviously still possible to be a great investigator without these skills, but any accounting knowledge will enhance a fraud investigation.

A highly regarded forensic accountant or fraud investigator is able to go beyond the investigation and excels in presenting the findings both in writing and orally. The investigator obviously has to be able to communicate the findings in a way that laypeople will be able to understand. Most cases have a possibility of going to court, so the ability to testify well is important.

How does a fraud investigator know whether she or he will do well testifying in a deposition or trial? It is difficult to say until she or he has actually done it. However, if a person is afraid of speaking in public, it is probably not a good fit. Think of testifying as speaking in public with members of the audience heckling you. It is the opposing attorney's job to poke holes in your work and opinions, and it can often get contentious. If you fluster easily or have a hard time making yourself understood, you will likely have a hard time testifying.

In anticipation of testifying as an expert witness, a fraud investigator must be willing to build a strong curriculum vitae (CV). The CV is often the first thing by which an expert will be judged, so making a good impression here is helpful. That good impression is made by offering up proof of your expertise, including degrees, certifications, employment history, continuing professional education, memberships in professional organizations, and articles and books written. Each piece of information on the CV should be aimed at proving that you are a well-qualified expert in your field.

Good fraud investigators are able to combine technical expertise with creativity and a knack for finding key pieces of evidence. The creativity component becomes crucial when you are trying to devise ways of verifying information or finding new evidence. The fraud investigator has to have multiple ways to find information, and the information is not always found where ordinary people would expect it. A good fraud investigator can locate a publicly available database or government agency

that might be able to verify a fact. She or he might find a new witness to a situation by carefully examining some unusual documents.

Authoritative accounting and auditing literature often refers to the “professional skepticism” required of financial statement auditors. It’s important that auditors be critical when examining the numbers and evaluating information provided by management. The auditor should constantly be asking whether the information makes intuitive sense, whether the explanations are reasonable, whether other explanations are possible, and whether the information presented is in fact true.

A fraud investigator takes this professional skepticism to a higher level. Some investigators are even accused of being too suspicious or of being negative in general. More likely, fraud investigators are so used to looking for what is wrong or inappropriate, that they are more prone to be skeptical of explanations, alleged evidence, and the facts as they have been presented.

### **Differences between Audits and Investigations**

Many forensic accountants and fraud investigators come from a traditional auditing background. It makes sense for an auditor to use her or his accounting and financial expertise in this way, because that foundation is absolutely critical for a high-quality financial investigation. It can be a natural fit for the person who is comfortable with numbers to move into a financial investigator position.

As already discussed, additional skills go into a fraud examination, including investigative techniques, interviewing techniques, financial data reconstruction, and much more. But a position as an outside auditor can be one of the best foundations for success in forensic accounting, because it offers the professional an opportunity to see financial statements and accounting departments in action.

Audits have never been designed to find fraud, and they likely will never be. They are designed to find errors and improper applications of accounting rules. Fraud, by its nature, is difficult to find during an audit, because steps have been taken by the actors in the fraud to conceal it. Fraudsters try to conceal a fraud from not only the company’s

management and owners but also the auditors. Familiarity with the company's operations and the auditing procedures will help an employee successfully conceal the fraud.

There are a handful of obvious differences between an audit and a fraud investigation. The process of performing an audit versus an investigation is quite different. Audits are often very standard, with the examination of certain financial statement items done on a routine basis. Certain procedures, such as inventory test counts and accounts receivable confirmation, are standard and do not vary a lot from engagement to engagement. The auditors are essentially looking for documentation that supports the accounting entries, but are not usually trying to verify the authenticity of the documentation or determine whether the transactions under examination are suspicious.

In contrast, fraud examinations are anything but routine, and this materially affects the planning and execution of the engagement. The most obvious difference between an audit and a fraud investigation is the lack of standard work programs for fraud investigations.

Audits are done largely based on standard work programs that outline areas of testing and examination. There are some differences in these work programs from audit to audit, based on client circumstances. Work is done on a test basis, with auditors selecting a sample of transactions within their predetermined scope. If those transactions pass the auditors' tests, it is essentially assumed that other transactions would pass the tests as well.

There is no such standardized process during a fraud examination. Checklists and investigation guides can help to some extent, but the investigative procedures are often determined based on the results of work just completed. Work is usually not done on a test basis. An area of suspicion is isolated, and the fraud investigator will usually examine all transactions within that area.

Audits rely heavily on the concept of materiality. Auditors regularly consider whether an item or transaction would make a difference in the eyes of the user of financial statements. Materiality is often defined largely in terms of dollars, but also involves circumstantial considerations that a financial statement user might consider important.

The SEC defines *materiality* as:

The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.<sup>2</sup>

For example, in a company with annual sales of \$10 billion, an improperly recorded sale of \$25,000 likely would not make a difference to someone looking at the financial statements. It is just too small of a dollar amount to even matter when compared to total sales of \$10 billion. In contrast, a theft of \$25,000 at the same company committed by the CFO might be considered material, even though the dollar amount is equally as small as the first situation. In this case, the relative amount is small, but the theft could very well be considered material because it was perpetrated by the top finance official in the company. That executive is essentially in charge of the money at the company, and if he is stealing, that circumstance may be material.

Materiality is not relied on in fraud investigations to dismiss irregularities. Any size fraud may be important to the organization regardless of the dollar figure. Small thefts can easily be significant, because they might indicate larger problems within the company. They may also tip investigators off to other larger frauds. It is not as simple to dismiss small items in a fraud investigation as it is in a financial statement audit.

The other major difference between audits and investigations relates to the opinions expressed. Audits are aimed at giving negative assurance: The auditors are not aware of anything that would make the financial statements incorrect. Fraud examinations give positive assurance: We found X, Y, and Z during our examination, and here is the evidence.

Fraud investigations are regularly referred to as *fraud audits*, although that term really should be avoided because of the confusion it can cause. An *audit* is a specific type of service offered by accountants, and a fraud investigation is quite different from an audit. It is more appropriate to refer to the project as a *fraud investigation*, *fraud examination*,

or *forensic accounting project*. While the terms used to describe this type of engagement seem like an insignificant matter, the most precise language possible should be used to describe your work.

## Conducting a Fraud Investigation

---

The focus of this book is the actual performance of a fraud investigation. The challenge in educating the reader about investigations is the wide variety of cases that can be handled by fraud investigators. This book attempts to instruct readers on some of the most common fraud schemes, controls that can help prevent them, and techniques for detecting them.

We will talk at length about the many signs of financial fraud and techniques that fraud investigators can use to further examine a company's finances to determine whether a fraud has occurred. Remember that because there are so many different types of fraud schemes and continuously evolving technology, which creates new opportunities for fraud, no book could ever cover all possible situations. This book covers some of the most common schemes and investigative techniques.

The information in this book is for general and educational purposes only, and should not be construed as legal or accounting advice or opinion. The material in this book may or may not be applicable or suitable for your specific circumstances or needs. Fraud investigations should be conducted by professionals with sufficient competence and experience in the field. The information in this book should not be considered a substitute for work experience or supervision by management. Please consult with a qualified fraud investigation professional before taking any action based on the information in this book.

## Notes

---

1. 2006 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, Austin, TX.
2. SEC Staff Accounting Bulletin: No. 99—Materiality; [www.sec.gov/interps/account/sab99.htm](http://www.sec.gov/interps/account/sab99.htm).

<http://www.pbookshop.com>