ANSWERS TO EXERCISES

Chapter 1

Review Questions

1-1 (Learning objective 1-1) What is fraud examination?

Answer: Fraud examination is a process for resolving allegations of fraud from inception to disposition. Fraud examinations involve not only financial analysis, but also interviewing witnesses, taking statements, writing reports, testifying to findings, and assisting in the prevention and detection of fraud.

1-2 (Learning objective 1-2) What is the fraud theory approach?

Answer: The fraud theory approach is the methodology used for resolving allegations of fraud by developing a worst-case scenario of what could have occurred, then attempting to confirm or refute that theory.

1-3 (Learning objective 1-3) Occupational fraud and abuse includes any personal enrichment that results from misuse or misapplication of the employing organization's resources or assets. There are four key elements to this activity. What are they?

Answer: The four key elements to occupational fraud abuse are that it (1) is clandestine, (2) violates the employee's fiduciary duties to the organization, (3) is committed for the purpose of direct or indirect financial benefit to the employee, and (4) costs the employing organization assets, revenues, or reserves.

1-4 (Learning objective 1-4) Under the common law, fraud generally consists of four elements, all of which must be present. List them.

Answer: The four legal elements of fraud are (1) a material false statement, (2) knowledge that the statement was false when it was uttered, (3) reliance on the false statement by the victim, and (4) damages as a result.

1-5 (Learning objectives 1-4 and 1-5) What is the difference between occupational fraud and occupational abuse? Give examples.

Answer: Occupational fraud tends to be more costly and less common than abuse. Occupational fraud consists of such actions as asset misappropriations, corruption, and fraudulent financial statements. Occupational abuse consists of petty offenses such as taking extended lunch periods or breaks, showing up late for work or leaving early, and doing slow or sloppy work.

1-6 (Learning objective 1-7) Edwin H. Sutherland, a criminologist, coined the phrase "white-collar crime." What did he mean by this term? How has the meaning of this phrase changed over time?
Answer: Sutherland coined the term "white-collar crime" to describe criminal acts of corporations and individuals acting in their corporate capacity (e.g., crime in the executive suite). Over time, the term has come to encompass almost any financial or economic crime, from the mailroom to the boardroom.

1-7 (Learning objective 1-7) Sutherland developed what is known as the "theory of differential association." What is the principal tenet of his theory?
Answer: The theory of differential association's principal tenet is that crime is learned. Sutherland believed that this learning typically occurred in intimate personal groups.

1-8 (Learning objective 1-8) Cressey interviewed nearly 200 embezzlers in order to develop his theory on the causation of fraud. As a result of his research, what was Cressey's final hypothesis?
Answer: "Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, 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 property."

1-9 (Learning objective 1-9) Cressey believed that non-shareable problems provided the motivation for employees to commit occupational fraud. What did he mean by "non-shareable"?
Answer: Cressey meant that the problems, at least in the eyes of the potential offenders, must be kept secret from others, so as to avoid embarrassment or, more importantly, a loss of status.

1-10 (Learning objective 1-9) Cressey divided the non-shareable problems of the subjects in his research into six different subtypes. What are they?
Answer: The subtypes are (1) violation of ascribed obligations, (2) problems resulting from personal failure, (3) business reversals, (4) physical isolation, (5) status gaining, and (6) employer–employee relations.

1-11 (Learning objective 1-11) Albrecht concluded that there were three factors that led to occupational fraud. What are they?
Answer: Albrecht's list is very similar to the fraud triangle. The three factors he identified are (1) situational pressures, (2) opportunities, and (3) personal integrity.

1-12 (Learning objective 1-12) What factor did Hollinger and Clark identify as the primary cause of employee deviance?
Answer: The research of Hollinger and Clark strongly suggests that job dissatisfaction among employees—across all age groups but especially younger workers—is the most likely cause of counterproductive or illegal behavior in the workplace.

1-13 (Learning objective 1-13) The *2009 Global Fraud Survey* covered a number of factors that are related to occupational fraud. List these factors.
Answer: The 2009 Global Fraud Survey *gathered data on occupational fraud and abuse relating to (1) the cost of fraud and abuse, (2) position, gender, tenure, and criminal history of the perpetrator, (3) size of the victim organization, (4) actions taken against occupational fraudsters by their victims, (5) methods by which occupational frauds were detected, (6) commonness of schemes, and (7) costs associated with various schemes.*

Discussion Issues
1-1 (Learning objective 1-1) How does "fraud examination" differ from "forensic accounting"?
Answer: Fraud examination is a process used to resolve allegations of fraud from inception to disposition. Forensic accounting is any accounting work done in anticipation of litigation.

1-2 (Learning objective 1-2) There are several steps involved in the fraud theory approach. What are they?
Answer: The fraud theory approach involves analyzing the available evidence, developing a theory of what fraud could have occurred based on a worst-case scenario, testing the theory, revising it or amending it as necessary, then proving the theory through additional investigative work.

1-3 (Learning objectives 1-3 through 1-6) How does occupational fraud and abuse differ from other kinds of fraud? Give examples of other fraud types.

Answer: Typically, any crime that uses deceit as its principal modus operandi is considered fraud. Occupational fraud involves those frauds that are committed against organizations by individuals who work for those organizations. Other fraud types include but are not limited to: insurance frauds committed by customers and policyholders, Internet frauds and scams perpetrated by individuals, frauds against governmental organizations committed by companies and individuals, frauds against banks committed by outsiders, and credit card frauds perpetrated against businesses.

1-4 (Learning objectives 1-7 and 1-8) How does the study of criminology relate to the detection or deterrence of fraud? How does it differ from the study of accounting or auditing?

Answer: Criminals commit frauds. Accounting relates to the classification of assets, liabilities, income, expenses, and equity. Auditing involves the verification of books and records. While accounting and auditing give us information on how fraud is committed, the study of criminology helps us understand why fraud is committed. The simple fact is that books don't commit fraud, people do. Understanding both how and why fraud is committed helps us better detect and deter it.

1-5 (Learning objective 1-7) Sutherland's contribution to criminology, in addition to giving us the term "white-collar crime," involved developing the theory of differential - association. What are the implications of this theory with respect to occupational fraud?

Answer: Sutherland's main point was that the tendency to commit crime is learned, not inherited. He believed that criminals learned both the techniques of committing crimes and the value systems of criminals in small, intimate groups. This explains, in part, why prisoners frequently return to crime after they are let out of confinement. While behind bars, they talk to other inmates and learn the specifics of how to better commit their crimes. They also are taught the unique values that "street" criminals hold, such as "getting something for nothing" and "society owes me a good living."

Occupational fraudsters, on the other hand, learn their techniques by working with books, records, inventory, and other assets. They frequently hear about other employees who were not successful in their crimes. Rather than being discouraged by someone being caught, the potential criminal often learns a different lesson: that the method the other person used to commit fraud was faulty and that a different one must be devised in order to succeed. They also learn the value systems that some businesses have: Profit is everything, and the end justifies the means. Such values obviously send the wrong message.

1-6 (Learning objective 1-8) Cressey's "fraud triangle" states that three factors—non-shareable financial need, perceived opportunity, and rationalization—are present in cases of occupational fraud. Which of these three factors, if any, is the most important in causing executives, managers, and employees to commit occupational fraud?
Answer: All three are equally important. A fire cannot exist without fuel, oxygen, and heat; a fraud cannot exist without motive, opportunity, and rationalization. If a person has unlimited motive but no opportunity, he or she cannot commit fraud. If a person has opportunity but doesn't need the money, the fraud is unlikely to occur. Should an individual have both motive and opportunity but cannot salve his or her conscience through rationalization, the crime will most likely not be committed.

1-7 (Learning objectives 1-8 and 1-9) Cressey described a number of non-shareable financial problems that he uncovered during his research. Which of these, if any, apply to modern-day executives who are responsible for large financial statement frauds? In the 50-plus years since Cressey did his study, are the factors he described still valid? Why or why not?
Answer: Three non-shareable financial problems seem to be at the root of today's financial frauds: violation of ascribed obligations, problems resulting from personal failure, and business reversals. Many modern-day businesses begin "cooking the books" when executives realize that they will not be able to meet their financial obligations. Similarly, some executives are too ashamed to admit that they don't have the talent or wherewithal to steer an enterprise through rough economic conditions. And sometimes, business reversals—from loss of a major client or contract, recessions, high costs of capital, and the like—are at the root of these so-called non-shareable financial problems.

One could argue that these factors are as valid today as they were over half a century ago. What motivates people to act changes little over time, although the methods that they use to accomplish their illegal goals (e.g., computer frauds) may.

1-8 (Learning objectives 1-8 through 1-11) Albrecht, in his research, developed the "fraud scale" and furnished a list of the reasons employees and executives commit occupational fraud. How are Albrecht's conclusions similar to Cressey's? How are they different?
Answer: Cressey's three factors were a non-shareable financial need, perceived opportunity, and rationalization. Albrecht's consisted of financial pressure, perceived opportunity, and personal integrity. One of the factors, perceived opportunity, was

named by both researchers. Cressey's non-shareable financial need is similar to Albrecht's financial pressure; however, Cressey's is more specific. Nearly everyone suffers financial pressures of some kind, but most do not turn to fraud in order to alleviate them. The ability to rationalize illegal conduct and personal integrity could be viewed as one and the same. However, personal integrity is difficult to measure, while specific rationalizations are easier to identify.

1-9 (Learning objective 1-13) The ACFE's *2009 Global Fraud Survey* found, among other things, that the frauds committed by women had smaller median losses than those by men. What are some possible explanations for this finding?
Answer: The sizes of losses due to occupational fraud are almost always determined by the employee's access to assets. This explains why executives account for the largest losses. Women, because of the so-called "glass ceiling" (where they are not promoted into jobs equal to their male counterparts'), typically occupy lower-level positions.

Chapter 2

Review Questions

2-1 (Learning objective 2-1) How is "skimming" defined?
Answer: Skimming is the theft of cash from a victim organization prior to its entry in the organization's accounting system.

2-2 (Learning objective 2-2) What are the two principal categories of skimming?
Answer: Skimming schemes can be subdivided based on whether they target sales or receivables. The character of the incoming funds has an effect on how the frauds are concealed, and concealment is the crucial element of most occupational fraud schemes.

2-3 (Learning objective 2-3) How do sales skimming schemes leave a victim organization's books in balance, despite the theft of funds?
Answer: When an employee skims money by making off-book sales of merchandise, neither the sales transaction nor the incoming cash is ever recorded. For example, suppose a cash register clerk skims $500 in receipts from one sale of goods. At the end of the day, his cash drawer will be short by $500—the amount of money that was stolen. But because the sale was never recorded, the sales records will be understated by $500. Therefore, the books will remain in balance.

2-4 (Learning objective 2-3) Under what circumstances are incoming checks received through the mail typically stolen?
Answer: Checks are normally stolen when a single employee is in charge of opening the mail and preparing the deposit. The employee simply removes the check from the incoming mail and forges the endorsement of the employer, then endorses it with his or her own name and cashes or deposits it.

2-5 (Learning objective 2-4) How do "understated sales" schemes differ from "unrecorded sales"?
Answer: Unrecorded sales schemes are purely off-book transactions. Understated sales, on the other hand, are posted to the victim organization's books, but for a lower amount than what the perpetrator collected from the customer. Typically, the perpetrator will understate a sale by recording a lower sales price for a particular item, or by recording the sale of fewer items of merchandise than the customer actually purchased.

2-6 (Learning objective 2-5) How is the cash register manipulated to conceal skimming?
Answer: There are two common methods. The first is to ring "no sale" on the register and omit giving the customer a receipt for the purchase. The second and less common method is for the cashier to alter the tape itself so that it does not show the sale. This is impossible to accomplish with cash registers that also record the transaction electronically.

2-7 (Learning objective 2-6) Give examples of skimming during nonbusiness hours and skimming of off-site sales.
Answer: Certain categories of employees usually commit these schemes. Managers of department stores or employees opening or closing the store have been known to open early or close late and skim all or part of the sales during those periods. Apartment rental employees, parking lot attendants, and independent salespeople are at a higher risk of skimming funds from off-site sales.

2-8 (Learning objective 2-8) What are the six principal methods used to conceal receivables skimming?
Answer: The six concealment techniques identified in this chapter are: lapping, force balancing, stealing customer statements, recording fraudulent write-offs or discounts, debiting the wrong account, and document destruction.

2-9 (Learning objective 2-9) What is "lapping" and how is it used to conceal receivables skimming?
Answer: Lapping is the crediting of one account through the abstraction of money from another account. Lapping customer payments is one of the most common methods of concealing receivables skimming. Suppose a company has three customers, A, B, and C. When A's payment is received, the fraudster takes it for himself instead of posting it to A's account. When B's check arrives, the fraudster posts it as a payment to A's account. Likewise, when C's payment is received, the perpetrator applies it to B's account. This process continues indefinitely until one of three things happens: (1) someone discovers the scheme, (2) restitution is made to the accounts, or (3) some concealing entry is made to adjust the accounts receivable balances.

2-10 (Learning objective 2-10) List four types of false entries a fraudster can make in the victim organization's books to conceal receivables skimming.
Answer: The fraudster can lap the payments, as discussed in the previous question. He can also engage in force balancing by posting a payment to a customer's account even though the payment was stolen. A third false entry that can be made is to fraudulently write off a customer's account as uncollectible. A fourth technique is to credit the targeted account with a fraudulent "discount" in the amount of the stolen funds. Also, some fraudsters conceal receivables skimming by debiting existing or fictitious accounts receivable.

Discussion Issues
2-1 (Learning objective 2-3) Sales skimming is called an "off-book" fraud. Why?
Answer: Simply because the fraud occurs outside the books and records. There is no direct audit trail to uncover; the proof of the fraud must be determined by indirect methods, such as ratio analysis or other comparisons.

2-2 (Learning objective 2-3) In the case study of Brian Lee, the plastic surgeon, what kind of skimming scheme did he commit?
Answer: Dr. Lee committed a sales (revenue) skimming scheme. In this fraud, Dr. Lee's clinic was a partnership with several other doctors, and all of the revenue derived from his services was supposed to go to the partnership. Because of a lack of controls and periodic reconciliations by the clinic, Dr. Lee simply instructed his patients to pay him directly. His scheme was uncovered by accident, as are many frauds.

2-3 (Learning objectives 2-5 and 2-12) If you suspected skimming of sales at the cash register, what is one of the first things you would check?
Answer: The cash register tape is one of the first things you should check. In a typical cash register skimming scheme, the crooked employee will ring up "no sale" on the register when a sale is made and pocket the money. The customer is not given a receipt. If you notice an excessive amount of "no sales" entered on the cash register, it could mean that the drawer is being opened and no money is being put in.

2-4 (Learning objective 2-3) Assume a client who owns a small apartment complex in a different city than where he lives has discovered that the apartment manager has been skimming rental receipts, which are usually paid by check. The manager endorsed the checks with the apartment rental stamp, then endorsed her own name and deposited the proceeds into her own checking account. Because of the size of the operation, hiring a separate employee to keep the books is not practical. How could a scheme like this be prevented in the future?
Answer: Two simple, separate control measures might help prevent such future occurrences. Although it might not be practical for the owner to reconcile the rental receipts himself since he lives in a different city, he could obtain a restrictive endorsement stamps that states "for deposit only." Second, the owner could have rental payments directed to a bank lockbox, where they would be less likely to be stolen.

2-5 (Learning objectives 2-8 and 2-11) What is the most effective control to prevent receivables skimming?
Answer: In almost all cases of receivables skimming, the person handling the cash and the person keeping the books are one and the same. An employee who opens incoming mail or handles cash should not be permitted to post the transactions.

2-6 (Learning objectives 2-3 and 2-7) In many cases involving skimming, employees steal checks from the incoming mail. What are some of the controls that can prevent such occurrences?
Answer: Here are some of the basic controls over incoming checks:

- *The person opening the mail should be independent of the cashier, accounts receivable clerk, or employees who are authorized to initiate or post journal entries.*
- *Unopened mail should not be delivered to employees having access to accounting records.*

- *The employee who opens the mail should (1) place restrictive endorsements on the incoming checks; (2) prepare a list of checks received; (3) forward all remittances to the person responsible for preparing and making the bank deposit; and (4) forward the list of checks to a person who can check to see if it agrees with the bank deposit.*

2-7 (Learning objectives 2-7 and 2-11) In the case study of Stefan Winkler, who was the chief financial officer for a beverage company in Florida, how did he conceal his skimming scheme? How could the scheme have been prevented or discovered?
Answer: Winkler's scheme is a classic example of too much trust placed in one employee. The beverage company received money from two different sources: route deposits (cash sales) and office deposits (accounts receivable). The route salespeople prepared their own deposit slips showing the cash and currency collected. The office personnel listed and accounted for the checks received through the mail. Winkler removed currency from the route deposits and replaced it with a check for the same amount from office deposits. Although office personnel listed the checks, they did not prepare the deposit slips—Winkler did that. As a result, he would ensure that the bank deposits agreed with the amount of money going into the bank.

To cover his tracks with the credit customers, Winkler would lap payments made by one customer to cover thefts from another customer. He would also give unauthorized discounts to credit customers. When Winkler was fired for other reasons, he made a general ledger adjustment of over $300,000 in a vain attempt to cover the shortages.

There were many clues: The internal control deficiencies were glaring. All of the cash made a stop at Winkler's desk on its way to the bank. Had there been adequate division of responsibilities, Winkler's scheme would have been much more difficult to accomplish. There were excessive false discounts to customers. The cost of sales would have been out of line with sales. And, like so many other fraudsters, Winkler lived beyond his means. Had his fellow employees been properly educated about fraud, they would have easily seen the fact that Winkler was driving a $75,000 car as a red flag. Also, had they been to his home, they would have noticed that their chief financial officer lived in an excessively expensive residence.

Chapter 3

Review Questions

3-1 (Learning objective 3-1) What is cash larceny?

Answer: Cash larceny involves the intentional taking away of an employer's cash without the consent, and against the will, of the employer. Cash larceny schemes involve the theft of money that has already appeared on the victim company's books.

3-2 (Learning objective 3-2) How do cash larceny schemes differ from fraudulent disbursements?
Answer: Cash larceny schemes generally target receipts, not disbursements. Furthermore, larceny schemes usually involve the physical misappropriation of cash by the perpetrator. The method of extraction—for instance, a perpetrator putting cash in his pocket—is itself improper. Fraudulent disbursements, on the other hand, typically rely on the submission of phony documents or the forging of signatures in order to make a fraudulent distribution of funds appear to be legitimate. The manner by which funds are disbursed is the same as in any legitimate disbursement, but the purpose of the distribution is fraudulent.

3-3 (Learning objective 3-3) What is the difference between cash larceny and skimming?
Answer: Both cash larceny and cash skimming schemes involve theft of the victim company's funds. However, cash larceny involves the removal of money after it has been recorded in the company's books, whereas skimming involves the removal of cash before the funds appear on the books. In other words, cash larceny is an on-book fraud, whereas skimming is an off-book fraud.

3-4 (Learning objective 3-4) Where do cash larceny schemes rank among cash misappropriations in terms of frequency? In terms of median loss?
Answer: In the 2009 Global Fraud Survey, *cash larceny schemes were less common than both skimming and fraudulent disbursements schemes. This is to be expected, as cash larceny is an on-book form of fraud that leaves an imbalance on the victim organization's books. This makes cash larceny more difficult to conceal than other forms of cash misappropriation. The median loss for cash larceny schemes was greater than that for skimming schemes, but lower than that for fraudulent disbursements schemes.*

3-5 (Learning objective 3-5) What are the main weaknesses in an internal control system that permit fraudsters the opportunity to commit cash larceny schemes?
Answer: Cash larceny schemes can take place under any circumstances in which an employee has access to cash; therefore, regular supervision and surveillance controls may prevent the opportunity for theft to occur. The lack of, or inadequate, separation of

duties for receiving, recording, depositing, and disbursing cash permit cash larceny schemes to occur.

3-6 (Learning objective 3-6) What are the five methods discussed in this chapter that are used to conceal cash larceny that occurs at the point of sale? Explain how each works.
Answer: In the cash larceny schemes reviewed, there were five methods that were identified as being used to conceal larceny at the point of sale. The first was thefts from other registers, in which an employee steals cash from another person's cash register. This does not conceal the crime, but it may help conceal the perpetrator's identity. The second method was death by a thousand cuts, in which an employee repeatedly steals very small amounts of cash over an extended period of time, hoping that the thefts are small enough to avoid triggering an investigation. The third method is the use of reversing transactions. After the perpetrator has stolen cash, he processes fraudulent refunds or voids sales in order to bring sales records back into balance with cash on hand. The fourth method is to alter cash counts or cash register tapes. Totals are misreported to create a fictitious balance between cash on hand and sales. The fifth method is to destroy sales records, which makes it difficult for the victim organization to discover an imbalance caused by larceny.

3-7 (Learning objective 3-8) How do employees commit cash larceny of incoming receivables? How are the schemes concealed?
Answer: Fraudsters may post the customer's payment to the accounting system but steal the cash, which causes an imbalance in the cash account. This imbalance can be concealed if the perpetrator has control over the recording function for ledger accounts. The fraudster makes unsubstantiated entries, which produce fictitious balances. Other ways to conceal cash larceny include using reversing transactions, creating unauthorized discounts, charging the theft to bad debts, or adjusting the inventory account. Alternately, the perpetrator simply may destroy all records of the transaction.

3-8 (Learning objective 3-8) What is force balancing and how is it used to conceal cash larceny?
Answer: Force balancing involves the making of unsupported entries in an organization's books and records to produce a fictitious balance. For example, if an employee steals an incoming receivables payment after it has been posted to the appropriate customer account, this will create a shortage in the cash account because the amount of receipts posted will exceed the amount of receipts on hand. If the employee is

able to make one or more unsubstantiated entries to cash in the amount of the stolen payment, he or she can eliminate the imbalance.

3-9 (Learning objective 3-9) How do fraudsters commit cash larceny from the bank deposit?
Answer: Fraudsters steal all or part of the deposit and conceal the scheme by destroying the bank statement, or by showing the deposits as "in transit." This type of scheme is usually effective when there is a poor internal control system over cash collections and deposits, in which the same employee may be responsible for cash collections, preparing deposit slips, making deposits, and reconciling bank statements. The fraudster may also alter the deposit slip after it has been returned in the bank statement.

3-10 (Learning objectives 3-5, 3-7, and 3-10) What are some basic internal control procedures to deter and detect cash larceny schemes?
Answer: The separation of duties related to cash receipts, deposits, and recording is a basic internal control to deter and detect cash larceny schemes. This includes segregation of authorization, recording, and custody functions for cash and related transactions. Assignment rotation, mandatory vacations, surprise cash counts, and physical security of cash can also assist in deterring and detecting cash larceny schemes.

Discussion Issues
3-1 (Learning objectives 3-1, 3-6, 3-8, and 3-9) Briefly describe some common types of cash larceny schemes.
Answer: Cash larceny, which involves the theft of an organization's cash after it has been recorded, can take place in any circumstance in which an employee has access to cash. Several different types of cash larceny schemes were described in this chapter. Most of these schemes involve larceny that either occurs at the point of sale, involves incoming receivables payments, or targets the victim organization's bank deposits. Within these three groups, there were several unique methods that were identified based on the steps taken to conceal the thefts. Employees generally conceal larceny at the point of sale by stealing from another person's cash register, stealing very small amounts over an extended period, processing fraudulent reversing transactions, altering cash counts or sales records, or destroying sales records. Larceny of receivables is generally concealed through force balancing, fraudulent reversing entries, or record destruction. Cash larceny from the deposit may be concealed by deposit lapping or by fraudulently recording stolen funds as deposits in transit. Larceny also frequently occurs because

there is a breakdown of controls such that one person has solitary access to an organization's books and records. In these cases, it may not be necessary for the perpetrator to use any concealment technique; he simply steals money without trying to hide the crime.

3-2 (Learning objective 3-3) Why is it generally more difficult to detect skimming than cash larceny?

Answer: The benefit of a skimming scheme is that the transaction is unrecorded and the stolen funds are never entered on company books. This makes the skimming scheme difficult to detect because sales records do not reflect the presence of the funds that have been taken. In a larceny scheme, on the other hand, the funds that the perpetrator steals are already reflected on the victim organization's books. As a result, an imbalance results between the sales records and cash on hand. This imbalance should be a signal that alerts a victim organization to the theft.

3-3 (Learning objectives 3-2 and 3-3) In the case study of bank teller Laura Grove, what type of fraud did she commit?

Answer: Laura perpetrated a cash larceny scheme. In order to classify the scheme, we first look to the fact that she took cash, which means her scheme was a form of cash misappropriation. To further classify the scheme, we look to the method by which she took the cash. Remember, there are three categories of cash misappropriation: fraudulent disbursements, skimming, and cash larceny. Laura Grove's scheme involved the physical misappropriation of cash without the use of fraudulent documents or forged signatures. She made no attempt to record or justify the removal of cash as a legitimate disbursement of funds. Therefore, her scheme could not have been a fraudulent disbursement.

The only two other categories of cash misappropriation are skimming and cash larceny. The difference between these two types of fraud lies in whether the stolen funds had been recorded on the victim organization's books at the time they were stolen. In this case, the money Laura Grove stole had already been recorded on the bank's books and records; therefore the scheme must be classified as a cash larceny.

3-4 (Learning objective 3-5) What are the internal control weaknesses that failed to deter and detect the fraud in Laura Grove's case?

Answer: Various weaknesses that may have contributed to the scheme include shutting off the surveillance camera on the vault during nonbusiness hours, not maintaining the security of the vault combination, not rotating employees periodically, and not checking employees' belongings when they left the bank.

3-5 (Learning objectives 3-6 and 3-7) Other than falsifying a company's records of cash receipts, how might an employee conceal larceny from a cash register?
Answer: An employee might discard or destroy cash register tapes. Missing or defaced backup documentation should indicate a red flag for fraud. Altering the cash count for his or her register is another way to conceal a fraud. Proper internal control procedures would prohibit an employee from performing a reconciling cash count of his or her own register.

3-6 (Learning objectives 3-10 and 3-11) What steps might an organization take to protect outgoing bank deposits from cash larceny schemes?
Answer: One form of cash larceny is for an employee to steal from the bank deposits. Usually, it is perpetrated by the employee who is in charge of making the deposit. Some internal control procedures that might assist in the deterrence of such frauds are: (1) separating the duties of receiving and opening of the mail and preparing the deposit slip, (2) segregating the functions for taking deposits to the bank and recording the transactions, (3) maintaining more than one copy of the deposit slip to be matched and reconciled with the bank's receipts of deposits, (4) examining the bank deposit slip for alterations, and (5) reconciling the bank statement with the book balance by a person who is not also involved with the custody function for cash.

3-7 (Learning objective 3-8) How is the larceny of receivables often detected?
Answer: Many times, receivables schemes involve skimming—the perpetrator steals the payment but never records it. This type of scheme might be detected by the delay between the time the payment is received and when it is posted to the books. Customer complaints of incorrect account balances are often a clue to a receivables skimming scheme.

If the theft occurs after the payment has been recorded, then it is classified as cash larceny. In order for an employee to succeed at a cash larceny scheme, she must be able to hide the imbalances in the accounts caused by the fraud. Larceny of receivables is generally concealed through force balancing, reversing entries, or destroying records. Looking for inappropriate journal entries and examining supporting documentation may help to uncover a larceny of receivables.

3-8 (Learning objective 3-11) In the case study "The Ol' Fake Surprise Audit Gets 'Em Every Time," how did Newfund's accounting and management controls contribute to the detection of Gurado's fraud scheme? How did the resulting actions of management help to deter future frauds?

Answer: Newfund's internal control procedure of conducting organized and effective surprise audits induced Gurado, a well-respected branch manager, to "come clean" at the prospect of his fraud being discovered during a prospective, imminent surprise audit. In this case, the threat of detection served the same goal as detection through an actual audit. Gurado was immediately fired for his misdeeds, which reinforced the importance of following proper procedures to other employees.

3-9 (Learning objective 3-11) Among the proactive audit techniques suggested in this chapter are the following: (1) a summary, by employee, of discrepancies between cash receipt reports and the sales register system; and (2) a summary, by employee, of discounts, returns, cash receipt adjustments, accounts receivable write-offs, and voids processed. Why would these two tests be effective in detecting cash larceny?

Answer: Because cash larceny involves the theft of on-book funds, it creates an imbalance on the victim organization's books. For example, if a cash register clerk steals $100 from his register, then the cash receipt report from that register will be $100 lower than the total recorded in the register sales system (unless a fraudulent entry is made to correct the imbalance). The first test suggested above would identify employees who tend to have these imbalances, which could signal larceny. This test would be particularly helpful in identifying employees who have multiple, small imbalances that individually are too small to be investigated, but collectively can become quite large.

In order to conceal imbalances caused by cash larceny, employees often process fraudulent adjusting entries to bring their cash receipt reports and register sales totals back into balance. The second audit test suggested above would test for this kind of activity by identifying employees who process an inordinate number of adjusting entries, which could be a result of efforts to hide cash larceny schemes.

Chapter 4

Review Questions

4-1 (Learning objective 4-1) What are the five categories of fraudulent disbursements, and where did billing schemes rank in terms of frequency and cost in the *2009 Global Fraud Survey*?

Answer: The five categories of fraudulent disbursements are: billing schemes, check-tampering schemes, payroll schemes, expense reimbursement schemes, and register disbursement schemes. Among these categories, billing schemes were most commonly reported. Fifty-two percent of fraudulent disbursements in the survey involved billing fraud. Billing schemes were the second most costly form of fraudulent disbursement, with a reported median loss of $128,000.

4-2 (Learning objectives 4-2 and 4-3) How is the term "billing schemes" defined, and what are the three categories of billing schemes covered in this chapter?
Answer: Billing schemes are frauds in which a perpetrator causes the victim organization to issue a fraudulent payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases. The three categories of billing schemes are: shell company schemes, non-accomplice vendor schemes, and personal-purchases schemes.

4-3 (Learning objective 4-4) What is the purpose of a shell company and how is it normally formed?
Answer: A shell company is a fictitious entity established for the purpose of committing fraud. It may be nothing more than a fictitious name and a post office box that the employee uses to collect disbursements from false billings. Since checks received will be payable to the shell company, the fraudster will normally set up a bank account in the name of the fictitious company, listing himself as the authorized signer on the account.

4-4 (Learning objective 4-5) There are four ways in which fraudulent invoices are approved for payment. What are they?
Answer: Fraudulent invoices are approved for payment by self-approval, by a rubber stamp supervisor, or through the normal internal control system by reliance on the authenticity of the false voucher the fraudster creates. In addition, collusion among several employees can overcome even well-designed internal controls and can enable fraudsters to obtain approval on bogus invoices.

4-5 (Learning objective 4-5) Why does collusion among employees in the purchasing process make it very difficult to detect billing schemes?

Answer: One of the main purposes of a well-defined internal control system is to separate the duties of individuals who are involved in the purchasing process in order to prevent any one person from having too much control over a particular business function. It provides a built-in monitoring mechanism in which each person's actions are verified by another person. But, if everyone in this process works together to create fraudulent voucher documents, then billing schemes will be very difficult to detect.

4-6 (Learning objective 4-6) Why do most shell company schemes involve the purchase of services rather than goods?

Answer: Services are intangible, which makes it more difficult for the victimized company to verify whether they were ever actually delivered by a vendor. If a billing scheme involves fictitious goods, the defrauded company may be able to detect the fraud by comparing its purchases to inventory levels, but this comparison will not identify the purchase of nonexistent services.

4-7 (Learning objective 4-7) What is a pass-through scheme and how does it differ from a typical shell company billing scheme?

Answer: In a typical shell company scheme, the perpetrator bills the victim organization for fictitious goods and services. In a pass-through scheme, on the other hand, the perpetrator actually provides real goods and services.

Pass-through schemes are usually undertaken by employees in charge of purchasing on behalf of the victim company. Instead of buying merchandise directly from a vendor, the employee sets up a shell company and purchases the merchandise through that fictitious entity. He then resells the merchandise to his employer from the shell company at an inflated price, thereby making an unauthorized profit on the transaction.

4-8 (Learning objective 4-9) What is a pay-and-return scheme? List three examples of how this type of fraud can be committed.

Answer: In a pay-and-return scheme, an employee intentionally mishandles payments to a vendor and then steals the excess payment when it is returned by the vendor. Generally, the perpetrator either double-pays an invoice, intentionally makes a vendor payment for an excess amount, or sends a payment to the wrong vendor. In all cases, the perpetrator then contacts the non-accomplice vendor, explains that a "mistake" was made, and asks the vendor to return the excess payment to her attention. When the overpayment is returned, the fraudster steals it.

4-9 (Learning objective 4-10) How does an employee use a non-accomplice vendor's invoice to generate a fraudulent payment?

Answer: Typically, the fraudster either prepares a fake vendor invoice and submits it to his company for payment or reruns an invoice that already has been paid. After his company prepares a check for payment, the perpetrator intercepts the check before it is sent out or has an accomplice do the same after the check arrives at the vendor's place of business. Alternatively, he could alter the vendor's address or electronic payment information in the payables and online banking system so that the check is delivered to the fraudster or an accomplice.

In addition to the preceding examples, an employee can generate fraudulent payments using a non-accomplice vendor invoice by committing a pay-and-return scheme, as was discussed in the preceding question.

4-10 (Learning objective 4-12) How does an employee make personal purchases on company credit cards, purchasing cards, or running charge accounts?

Answer: Instead of running false invoices through accounts payable, some employees make personal purchases on company credit cards, purchasing cards, or running charge accounts with vendors. An employee with a company credit card or purchasing card can buy an item merely by signing his name (or forging someone else's) at the time of purchase. Some companies keep open charge accounts with vendors with whom they do regular business. Office supply companies are a good example of this kind of vendor. Purchases on charge accounts may require a signature or other form of authorization from a designated company representative. Obviously, that representative is in a position to buy personal items on the company account. Other employees might do the same by forging the signature of an authorized person at the time of a fraudulent purchase. In some informal settings, purchases can be verified by as little as a phone call.

Discussion Issues

4-1 (Learning objectives 4-3 and 4-4) In the case study of Cheryl Brown, the administrative assistant at a Southeastern medical school, what type of billing scheme did she commit?

Answer: Cheryl committed a shell company scheme. She and an outside accomplice created a shell company and bilked her employer out of thousands of dollars through the use of fake invoices.

4-2 (Learning objectives 4-8, 4-11, and 4-13) Explain how separation of duties contributes to the prevention and detection of billing schemes.
Answer: By enforcing a rigid separation of duties in the purchasing process, an organization can significantly limit its exposure to billing schemes. Segregating the purchasing process into four basic functions—purchasing, approval of purchase, receipt of goods, and cash disbursement—can prevent most forms of billing fraud. This is because most billing schemes succeed only when an individual has control over two or more of these functions. If these duties are strictly segregated, it will be very difficult for an employee to commit most forms of billing fraud.

4-3 (Learning objectives 4-8 and 4-14) List and explain at least four proactive audit tests that could be performed to help detect a shell company scheme.
Answer: Examples of tests that can be used to detect a shell company scheme include the following. Vendors lacking certain identifying information such as a telephone number or tax ID can be extracted from the vendor master file for investigation. Similarly, the vendor master file can be matched to the employee master file for duplicate telephone numbers, addresses, and so on. The invoice payment file can be searched for vendors who had multiple invoices just below established review limits—a possible sign of an attempt to circumvent management review of bogus invoices. The vendor master file can also be matched to the invoice payment file to identify payments to any unapproved vendors. There are several other tests identified in this chapter that could also be used.

4-4 (Learning objectives 4-4, 4-5, and 4-8) What are some of the ways shell company invoices can be identified?
Answer: Auditors, accounting personnel, and other employees should be trained to identify red flags relating to fraudulent invoices. One common red flag is a lack of details such as a telephone, fax, tax identification, or invoice number. Another common red flag is an invoice that lacks detailed descriptions of items ordered. Lastly, using a mail drop or residential address may also indicate a billing fraud scheme. All of these red flags should be investigated.

4-5 (Learning objectives 4-4 and 4-7) Sharon Forsyth worked in the purchasing department of a retail store. She was in charge of ordering merchandise inventory and various supplies for the organization. She purchased merchandise through a fictitious shell company and then resold it to her employer at an inflated price. What is the name of this type of fraud?

Answer: This type of fraud is called a pass-through billing scheme and is a subcategory of shell company schemes in which actual goods or services are sold to the victim company.

4-6 (Learning objective 4-9) Karen Martinis was responsible for opening mail, processing vendor claims, and authorizing payments. She was involved in a scheme in which she either double-paid vendor invoices, paid the wrong vendors, or overpaid the right vendors. What type of billing scheme is being described in this case?
Answer: This is a pay-and-return billing scheme involving non-accomplices. In a pay-and-return billing scheme the perpetrator does not prepare fake invoices and submit them to the victim company. Instead, she intentionally mishandles vendor payments that are owed to a legitimate vendor. The perpetrator then requests that the vendor send a check for the amount owed back to the victim company.

4-7 (Learning objective 4-9) What type of internal controls can be used to help prevent pay-and-return billing schemes?
Answer: As with most billing frauds, pay-and-return schemes can be mostly prevented if the duties of the purchasing, authorizing, and payment functions are separated and if invoices are matched to purchase orders before payments are made. Also, incoming mail should never be delivered directly to an employee, but rather opened at a centralized point with all incoming checks being properly recorded. Organizations should also instruct their banks not to cash checks made payable to the company. In some cases, employees attempt to conceal the theft of returned checks by running targeted invoices through the payables system a second time so that the intended recipient of a stolen check still gets paid. An effective duplicate checking system can help prevent this type of scheme and make it easier to detect a pay-and-return fraud.

4-8 (Learning objective 4-12) In terms of classifying frauds under the Fraud Tree system, how does a scheme in which an employee fraudulently orders merchandise for his personal use differ from a scheme in which an employee steals merchandise from his company's warehouse?
Answer: Even though both schemes involve an employee taking merchandise, the first scheme is classified as a billing scheme, whereas the second is classified as a theft of inventory (as will be discussed in Chapter 9). This is because when a person steals inventory from a warehouse, he is stealing an asset that the victim organization needs, that it has on hand for a particular reason. The harm to the victim company is not only

the cost of the stolen asset, which will have to be replaced, but also the loss of the asset itself.

In contrast, when an employee fraudulently buys merchandise with company funds, the asset he acquires is superfluous. The perpetrator causes the victim company to order and pay for an item which it does not really need, so the only damage to the victim organization is the money lost in purchasing the particular item. The victim organization suffers no harm in the loss of the asset that was purchased, because the victim had never designated a need for that asset in the first place.

Chapter 5

Review Questions

5-1 (Learning objective 5-1) Assume there are two thefts of checks at ABC Company. In the first case, an employee steals an outgoing check that is drawn on ABC's account, and is payable to "D. Jones." The perpetrator forges the endorsement of "D. Jones" and cashes the check. In the second case, an employee steals an incoming check from "D. Jones" that is payable to ABC Company. The employee fraudulently endorses the check and cashes it. Which of these schemes would be classified as check tampering? Why?
Answer: Only the first scheme would be classified as check tampering, because check tampering is a form of fraudulent disbursement, and the first scheme involved a disbursement of the victim organization's funds, whereas the second scheme did not. Check tampering applies only to checks drawn on the victim organization's accounts. If an employee steals an incoming check that is payable to the victim organization, then this theft will be classified as either skimming or cash larceny, depending on whether the check was recorded by ABC Company before it was stolen or afterward.

5-2 (Learning objective 5-2) There are five principal categories of check tampering frauds. What are they?
Answer: The five principal categories of check tampering are: (1) forged maker schemes, (2) forged endorsement schemes, (3) altered payee schemes, (4) concealed check schemes, and (5) authorized maker schemes.

5-3 (Learning objective 5-3) What are the methods discussed in this chapter by which fraudsters gain access to blank company checks as part of a forged maker scheme?
Answer: Most forged maker schemes are committed by employees whose duties include the preparation of company checks, so in most cases the fraudster has legitimate access to blank check stock. When an employee does not have access to blank checks through his

job duties, he may be able to steal checks that are not properly safeguarded. For example, a company's checkbook or blank check stock might be stored in an open, unlocked area that is not always supervised. The perpetrator might also obtain a key or combination to a restricted area where checks are stored. When check stock is properly safeguarded and the fraudster does not have access, he might be able to obtain blank checks from another employee who does have legitimate access, typically in return for a portion of the stolen funds. If unused checks are not properly disposed of after they have been voided, an employee may be able to use them in a forged maker scheme. Finally, a fraudster might produce counterfeit check stock and use this to draw funds from the organization's accounts.

5-4 (Learning objective 5-4) Perpetrators of check tampering schemes must obtain a signature on the check. What are methods used to affix a signature to the check?
Answer: The perpetrator can simply write an authorized person's name on the check. A more elaborate method is to create a legitimate signature on a transparency and use it to place a signature on blank checks. Some companies use signature stamps or computerized signatures that a perpetrator can gain access to. The perpetrator may be an authorized signer and will simply sign a check himself. Finally, he may hide a tampered check in a group of legitimate checks and present them for signing by an authorized signer.

5-5 (Learning objective 5-5) How can the type of paper on which an organization's checks are printed be a factor in preventing and detecting forged maker schemes?
Answer: The type of paper a check is printed on can sometimes help distinguish a legitimate check from a counterfeit. Organizations should print their checks on watermark paper supplied by a company independent of its check printer. (This will prevent a dishonest employee of the printer from using the company's watermarked paper). Security threads or other markers can also be incorporated to help verify that company checks are legitimate. If an organization uses high-quality, distinctly marked paper for its checks, counterfeits will be easier to detect. In addition, it is a good idea to periodically rotate check printers and/or check stock to help make counterfeits stand out.

5-6 (Learning objective 5-6) What are the differences between a forged maker and a forged endorsement scheme?
Answer: A forged maker scheme is one in which an employee misappropriates a check and fraudulently affixes the signature of a legitimate check signer to authorize

disbursement of funds. In a forged endorsement scheme, the employee intercepts a signed company check intended for a third party and fraudulently endorses the check in order to obtain the funds that were intended for someone else.

An important distinction is that the two schemes attack an organization's control structure at different points. A forged maker scheme typically involves the falsification of a blank check. The key to this kind of scheme, from the fraudster's perspective, is in obtaining a blank check, producing a signature that appears to be authentic, and in some cases, recording the check in such a way that the fraud will not be detected. In a forged endorsement scheme, by contrast, the perpetrator is working with a check that has already been prepared, so the issues are different. Instead of gaining access to blank check stock, the perpetrator must find a way to gain access to a check after it has been signed but before it has been delivered. Typically, this means the fraudster must steal the check before it is sent out in the mail, although in some cases the fraudster might alter the mailing address of a legitimate payee.

From a concealment standpoint, forged endorsement schemes present different challenges than forged maker schemes. In a forged endorsement scheme, the stolen check was intended for a real payee, so the perpetrator must be concerned with the probability that the intended payee will complain about not receiving the check that has been stolen. In a forged maker scheme this is not generally a concern because the check is originally written for a fraudulent purpose; there is no legitimate payee.

5-7 (Learning objective 5-7) What are some methods of intercepting a check intended for a third party?

Answer: A perpetrator may be an employee authorized to mail or deliver a check but who diverts it for his own benefit. Checks that are signed but are left unattended instead of being immediately mailed can be stolen by a fraudster. Checks that are returned because they could not be delivered to the addressee could be intercepted or a perpetrator could change the address of a legitimate payee to his own address prior to mailing. After a check has been intercepted, the payee name can be altered by adding a second payee to the payee line, or the perpetrator can use erasable ink to prepare the check, then change the payee (and amount) on the check after it has been signed.

5-8 (Learning objective 5-9) What is an authorized maker scheme, and why are these frauds especially difficult to prevent through normal internal controls?

Answer: An authorized maker scheme is a type of check tampering fraud in which an employee with signature authority on a company account writes fraudulent checks for his

own benefit and signs his own name as the maker. The perpetrator in these schemes can write and sign fraudulent checks without assistance. He does not have to alter a pre-prepared instrument or forge the maker's signature.

This may be the most difficult form of check tampering to defend against because in most cases check signers are owners, officers, or otherwise high-ranking employees, and thus have or can obtain access to all the blank checks they need. Even if a company's control structure ostensibly prohibits check signers from handling blank checks, the perpetrator typically has enough influence and authority to override this control.

5-9 (Learning objective 5-7) How can a perpetrator conceal check tampering activity from others in the organization?

Answer: If the perpetrator is responsible for bank reconciliations he can remove fraudulent canceled checks, mark fraudulent checks as void on the reconciliation, force balance the reconciliation, or physically alter the bank statement to conceal the fraudulent checks. If a fraudster has committed an altered payee scheme, he might re-alter the canceled checks during the reconciliation (by inserting the name of the intended payee and the proper amount) so that they correspond to the disbursements journal. The fraudster can also falsify disbursement journals, hide the tampered disbursements in an account where they are unlikely to draw attention, or falsify supporting documents to make the bogus checks appear legitimate. In forged endorsement or altered payee schemes, which involve the theft of outgoing checks intended for a third party, the fraudster may reissue the intercepted checks to avoid having the intended payee complain to others in the organization.

5-10 (Learning objectives 5-5, 5-8, and 5-10) There are several duties that should be segregated among employees to minimize the opportunity for check tampering. List these duties.

Answer: Duties that should be segregated among employees include: (1) check cutting and posting, (2) check signing, (3) check delivery, and (4) bank statement reconciliations.

5-11 (Learning objective 5-11) What measures can companies can take to prevent and detect fraudulent electronic payments?

Answer: Companies can best defend against fraudulent electronic payments through a combination of solid internal controls and bank security services. Separation of duties (e.g., segregating duties for creating, approving, and releasing wires) is one of the most important internal controls for preventing and detecting electronic payments fraud.

Other essential internal controls include segregation of bank accounts (e.g., using separate accounts for paper and electronic transactions), daily account monitoring and reconciliation, and management and protection of user access and account information. Bank security services that can help business account holders mitigate electronic payment fraud include ACH blocks and filters, positive pay for ACH, multi-factor authentication tools, dual authorization, transaction limits, and software access restrictions.

Discussion Issues

5-1 (Learning objectives 5-5 and 5-10) In the case study of Melissa Robinson, she was able to steal over $60,000 from her employer. Why was she able to commit her fraud without detection?

Answer: Melissa Robinson was given check signing authority and sole control of the bookkeeping function. She was given large amounts of cash that were not verified by a second person. External audits that may have uncovered the fraud were never completed. In addition, she was not challenged when she failed to allow others access to the books and records and failed to provide financial information.

5-2 (Learning objectives 5-5, 5-8, and 5-10) Assume you are a new hire in the accounting department of an organization. One of your responsibilities is the reconciliation of the operating account. After the end of the month you are given a copy of the bank statement and the canceled checks and instructed to perform your reconciliation. You notice there are some faint markings on a portion of the bank statement that could be alterations. What steps would you take in performing the reconciliation?

Answer: The first oddity that should be noticed is that you were given a copy of the bank statement, not the original. This is an indication that the bank statement may have been manipulated. This is further evidenced by the faint markings noted on the copy. These could be from tape, correction fluid, or some other method used to hide the true data on the original bank statement. You should add the individual items on the statement and reconcile the totals to the amounts reported on the bank statement (e.g., add deposits and compare the total to the "total deposit" amount on the bank statement). Each canceled check should be compared to the bank statement to ensure all canceled checks reported on the statement are included with the statement. A request should also be made to review the original bank statement and determine why you were given only a copy. A review of the age of reconciling items should be made and any old or unusual items investigated. A comparison should be made between each canceled check and the

corresponding listing in the check register and the account to which it was posted. Finally, a review of endorsements may be prudent.

5-3 (Learning objective 5-3) If a fraudster does not have legitimate access to check stock, he must obtain access to the check stock in order to commit a forged maker scheme. What are some ways blank checks can be fraudulently obtained and what measures could an organization take to prevent this from occurring?
Answer: Blank check stock may be poorly protected by those who have legitimate access. Organizations should make sure that the blank checks are always under lock and key and that the key is closely guarded. Computer-generated check stock should also be safeguarded. Employers should allow access to computerized check-writing applications by password only and change the password on a frequent basis. Finally, these internal controls should be tested on a periodic basis to ensure they are properly working.

5-4 (Learning objectives 5-3 and 5-5) Access to an organization's funds can be gained through counterfeiting the organization's check stock. What types of controls would help detect a counterfeit check?
Answer: The use of watermark paper or paper with security threads would help identify counterfeit checks. Use of multiple types of check stock and check printers that are periodically rotated would also help identify counterfeits as would a search for out-of-sequence or duplicate check numbers on bank reconciliations.

5-5 (Learning objectives 5-4 and 5-5) Checks can be forged by several methods: free-hand forgeries, photocopies of legitimate signatures, and by obtaining access to an automatic check-signing mechanism. What are some controls an organization could institute to minimize the chance a forgery will occur?
Answer: A list of authorized check signers should be prepared and a rotation schedule for signers set up. Canceled checks should then be reviewed each period to ensure the correct signer's name appears on each check. A periodic comparison of the authorized signer's signature should be made with canceled checks to spot obvious forgeries. Finally, access to any automatic check-signing mechanisms should be severely restricted and the related internal controls tested on a surprise basis to ensure the internal controls are being followed by employees.

5-6 (Learning objectives 5-6, 5-7, and 5-8) Forged endorsement schemes and altered payee schemes both involve the theft of outgoing checks that are intended for third parties

for some legitimate purpose (e.g., a check payable to a vendor for services rendered). In this respect, these schemes differ from other forms of check tampering, in which the check is usually drafted by the perpetrator for a fraudulent purpose. Discuss how this distinction affects the way in which forged endorsement and altered payee schemes must be concealed.

Answer: When an employee steals an outgoing check that was intended for a third party, this creates a concealment problem because the third party presumably expects the check and will in all likelihood complain if it is not received. Therefore, a fraudster who engages in a forged endorsement or altered payee scheme must often find a way to issue a check to the intended recipient to cover for the stolen payment. This is not a necessary step in other types of check tampering, such as a forged maker scheme, because in these cases the stolen check was originally written for a fraudulent purpose; it has no intended payee other than the fraudster.

In addition, when a fraudster attempts to convert a stolen check that was payable to a third party, this may leave clues that will later have to be concealed. For example, in an altered payee scheme, the fraudster inserts his name (or that of an accomplice) onto the payee line of the check. This information will not match the check register and should be a red flag. Therefore, the perpetrator may have to re-alter the canceled check (by replacing the original information) when it is returned with the bank statement.

If a fraudster uses a dual endorsement to convert a check as part of a forged endorsement scheme, the second endorsement (in the name of an employee) would be a clear red flag of fraud. The perpetrator may have to destroy the canceled check to prevent detection.

5-7 (Learning objective 5-8) In altered payee schemes, the perpetrator changes the name of the intended third party and negotiates the check himself. This can be done by adding a second payee or changing the original payee's name. What is the best method for detecting this type of fraud?

Answer: The best way to detect an altered payee scheme is to include as part of the bank reconciliation process a comparison of canceled checks to the check register to ensure both payees are identical. Implied in this statement is the understanding that the person who performs the reconciliation must be independent of the check-cutting process. Most altered payee schemes are successful only when the perpetrator is in charge of reconciling the bank statement.

5-8 (Learning objectives 5-5 and 5-10) In the Ernie Philips case, $109,000 was stolen through check tampering. How was this scheme accomplished and what could management have done differently to prevent the scheme from occurring?
Answer: Ernie wrote unauthorized checks, forged the authorized signers' names, and then manipulated the bank statements to hide the disbursements. He also obtained access to the signature stamp and included unauthorized checks with legitimate checks when submitting them for signing. Finally, he used his position of authority to deflect questioning about unidentified disbursements. Mr. Sell had implemented some good internal controls but Ernie did not respect them. For example, Ernie fraudulently obtained bank statements after being warned by Mr. Sell that he was not to receive or review them. This procedure should not have been tolerated in-house, and the bank should not have been permitted to send bank statements directly to Ernie in the first place (this kind of change should have required Sell's authorization). A stronger control over comparing checks presented for signing to supporting documentation and a stronger control over the signature stamp could have been implemented. If the organization had required Sell to spot-check his signature on canceled checks, it is possible some of Ernie's forgeries could have been detected.

Chapter 6

Review Questions

6-1 (Learning objective 6-1) According to this chapter, what are the three main categories of payroll fraud?
Answer: A payroll scheme is an occupational fraud in which a person who works for an organization causes that organization to issue a payment by a making false claim for compensation. There are three main categories of payroll fraud: ghost employee schemes, falsified hours and salary schemes, and commission schemes.

6-2 (Learning objective 6-2) In terms of median losses, which is larger: billing schemes or payroll schemes? Can you offer a possible explanation?
Answer: According to the statistics from the 2009 Global Fraud Survey, *billing schemes have larger median losses than payroll schemes. One possible explanation is that - disbursements to vendors are typically larger than those to employees; therefore, it would be easier to conceal a large fraudulent disbursement by concealing it as a payment to a vendor.*

6-3 (Learning objective 6-3) What is a "ghost employee"?

Answer: The term ghost employee refers to someone on the payroll who does not actually work for the victim company. The ghost employee may be a fictitious person or a real individual who simply does not work for the victim employer. When the ghost is a real person, he or she is often a friend or relative of the perpetrator. In some cases the ghost employee is an accomplice of the fraudster who cashes the fraudulent paychecks and splits the money with the perpetrator.

6-4 (Learning objective 6-3) There are four steps that must be completed in order for a ghost employee scheme to be successful. What are they?
Answer: The four steps to making a ghost employee scheme work are: (1) adding the ghost to the victim company's payroll records, (2) collecting and maintaining timekeeping and wage information, (3) issuing a company payroll check to the ghost, and (4) delivering the ghost's check to the perpetrator or his or her accomplice.

6-5 (Learning objective 6-3) Within a given organization, who is the individual most likely to add ghost employees to the payroll system?
Answer: Regardless of how the hiring of new employees is handled within a business, it is the person or persons with the authority to add new employees to the company's records who are in the best position to put ghosts on the payroll.

6-6 (Learning objective 6-6) The key to a falsified hours scheme in a manual system is for the perpetrator to obtain authorization for the falsified timecard. There were four methods identified in this chapter by which employees achieved this. What were they?
Answer: The four ways an employee can obtain authorization for a falsified timecard are: (1) forging a supervisor's signature on a fraudulent timecard, (2) colluding with a supervisor, (3) relying on a "rubber stamp" supervisor to approve the timecard without review, and (4) altering a timecard after it has been approved by a supervisor.

6-7 (Learning objectives 6-7 and 6-8) What is meant by the term "rubber stamp" supervisor and how are these individuals utilized in a payroll fraud scheme?
Answer: The term rubber stamp supervisor refers to a manager who approves timecards without reviewing their accuracy. This is a very serious breach in controls, because the role of the manager in verifying hours worked and authorizing timecards is critical to preventing and detecting payroll fraud. Obviously, rubber stamp supervisors play a part in payroll fraud in the sense that they fail to detect crimes that are otherwise detectable. In addition, the fact that a manager is known to approve timecards without reviewing

them may provide the perceived opportunity that convinces an employee to attempt a payroll fraud scheme.

6-8 (Learning objective 6-8) List at least three tests that could be performed to detect falsified hours and salary schemes.
Answer: Several tests were discussed in this chapter, including the following:

- *Comparisons of overtime expenses by employee and by department*
- *Comparisons of payroll expenses to budget projections or prior year totals on a company-wide and departmental basis*
- *Exception reports showing any employee whose compensation has increased from the prior period by a disproportionately large percentage*
- *Verification of payroll taxes to federal tax forms*
- *Comparison of net payroll to payroll checks issued*

In addition to the preceding, several proactive audit tests were recommended at the end of the chapter.

6-9 (Learning objective 6-9) There are two ways that an employee working on commission can fraudulently increase his pay. What are they?
Answer: A commissioned employee's wages are based on two factors, the amount of sales he generates and the percentage of those sales he is paid. In other words, there are two ways an employee on commission can fraudulently increase his pay: (1) falsify the amount of sales made (either by creating fictitious sales or by overstating the amount of legitimate sales), or (2) increase his rate of commission.

Discussion Issues

6-1 (Learning objective 6-1) List and explain at least three computer-aided audit tests that can be used to detect a ghost employee scheme.
Answer: There are several suggested tests listed at the end of this chapter. For example, a comparison of payroll data files to human resource data files could be performed to look for differences. Employees that show up on the payroll register but not in the employee master file should be verified. Another possible test is to extract all employee payments with no deductions or taxes withheld from the payroll register. These types of payments are more prone to fraud and are often associated with ghost employee schemes. The payroll register can also be matched against the employee master file to extract employees with no name, no employee number, no social security number, or whose

payment dates occur after their termination dates. All of these conditions would be consistent with a ghost employee scheme.

6-2 (Learning objectives 6-4 and 6-5) The ability to add ghost employees to a company's payroll system is often the result of a breakdown in internal controls. What internal - controls prevent an individual from adding fictitious employees to payroll records?
Answer: The most effective method of preventing an individual from adding fictitious employees to a company's payroll records is to segregate duties for payroll preparation, disbursement, distribution, and payroll account reconciliation. As long as these duties are separated, it is very difficult for a single individual to add ghosts to the payroll system.

6-3 (Learning objective 6-7) In the case study of Jerry Harkanell ("Say Cheese!"), what internal controls could have prevented the falsification of his timesheet?
Answer: Harkanell should not have been allowed to deliver the signed timesheets to the payroll department. Additionally, procedures should have required him to complete his timesheet using permanent ink, rather than pencil (which can be erased).

6-4 (Learning objective 6-7) In terms of preventing payroll fraud, why is it important for hiring and wage rate changes to be administered through a centralized and independent human resources department?
Answer: There are several ways in which a centralized human resources department can help to prevent payroll fraud. By having all hiring be conducted through its human resources department, an organization can limit its exposure to ghost employee schemes. This control would prevent a rogue manager from adding ghosts to her staff and pocketing their paychecks. Absent collusion, a human resources employee would also not be able to add a ghost, because there would be no line manager to approve the ghost's timecards, and therefore payroll would not issue a check to the ghost. The human resources department and the line manager would act as independent checks on one another.

In addition, if all wage rate changes must be independently administered through human resources, this would tend to prevent an employee from falsely obtaining an increase in his wage rate or salary, and it would prevent a payroll employee from overpaying himself. Absent collusion with a human resources employee, these individuals would be unable to authorize the increase.

6-5 (Learning objective 6-10) If you suspect a salesperson is inflating his commissions, what would you do to determine if this were occurring?
Answer: If a salesperson is suspected of inflating his commissions, an examiner should compare the salesperson's commissions to those of other salespeople and to his sales figures to determine whether there is an appropriate correlation. Rates at which the salesperson is paid should be determined and verified with personnel or other company records. Proper segregation of duties should also be confirmed.

6-6 (Learning objective 6-10) Beta is one of 10 salespeople working for ABC Company. Over a given period, 15 percent of Beta's sales are uncollectable, as opposed to an average of 3 percent for the rest of the department. Explain how this fact could be related to a commission scheme by Beta.
Answer: Commissions are a form of compensation calculated as a percentage of the amount of sales a salesperson generates; therefore, one of the ways a salesperson could create fraudulent commission payments for himself is by overstating the amount of sales he generates. As was explained in this chapter, one way employees falsify the amount of sales they make is by creating fictitious sales to nonexistent customers. The employee collects the commission on the sales but no payment is ever made by the "customer." The receivables associated with these fake sales age and eventually are written off as uncollectible.

Chapter 7

Review Questions

7-1 (Learning objective 7-1) Explain what constitutes expense reimbursement fraud and list the four categories of expense reimbursement schemes.
Answer: Expense reimbursement schemes, as the name implies, occur when employees make false claims for reimbursement of fictitious or inflated business expenses. This is a very common form of occupational fraud and one that, by its nature, can be extremely difficult to detect. Employees who engage in this type of fraud generally seek to have the company pay for their personal expenses, or they pad the amount of business expenses they have incurred in order to generate excess reimbursements. The four categories of expense reimbursement fraud are: (1) mischaracterized expense reimbursements; (2) overstated expense reimbursements; (3) fictitious expense reimbursements; and (4) multiple reimbursements.

7-2 (Learning objective 7-3) Alpha is a salesperson for ABC Company. In July, Alpha flies to Miami for two weeks of vacation. Instead of buying a coach class ticket, he flies business class, which is more expensive. A few weeks later, Alpha prepares an expense report and includes the Miami flight on it. He lists the reason for the flight as "customer development." What category of expense reimbursement fraud has Alpha committed?
Answer: Alpha has committed a mischaracterized expense reimbursement scheme, which occurs when an employee seeks to be reimbursed for personal—rather than business-related—expenses.

7-3 (Learning objective 7-5) Why is it important to require original receipts as support for expenses listed on a travel and entertainment expense report?
Answer: One of the ways in which employees commit expense reimbursement fraud is by overstating business expenses. This is often accomplished when an employee alters supporting documentation to reflect a higher cost than what he actually paid. These alterations are less noticeable on a photocopy than on the original document. Therefore, by requiring original support an organization will be more likely to detect this kind of fraud, and employees will be less likely to attempt it.

7-4 (Learning objective 7-5) What is meant by the term "overpurchasing"?
Answer: Overpurchasing is a method of overstating business expenses in which a fraudster buys two or more business expense items at different prices (such as airline tickets). The perpetrator returns the more expensive item for a refund yet still claims reimbursement for this item. As a result, he is reimbursed for more than his actual expenses.

7-5 (Learning objective 7-7) Provide two examples of how an employee can commit a fictitious expense reimbursement scheme.
Answer: An employee can document wholly fictitious items for reimbursement by producing her own fictitious receipts and/or bogus support documentation, which are used to support nonexistent items on an expense report. Additionally, an employee may steal or otherwise obtain blank receipts from common vendors, such as hotels or restaurants, and fill these in to justify fictitious expenses. Another method is for an - employee to claim expenses that were paid by someone else, such as a case in which a client pays for a business lunch but the employee submits an expense report for the lunch.

7-6 (Learning objective 7-9) How is a multiple reimbursement scheme committed?

Answer: This type of fraud involves the submission of a single expense several times to receive multiple reimbursements. The most frequent example of a duplicate reimbursement scheme is the submission of several different types of support for the same expense, such as submitting an airline ticket stub and the travel agency invoice on separate expense reports. Alternatively, the same expense report may be submitted more than once. Typically, the perpetrator will have the duplicate reports approved by separate supervisors and will also allow a time lag between the two reports to help avoid detection.

7-7 (Learning objective 7-5) Beta is an auditor for ABC Company. He runs a report that extracts payments to employees for business expenses incurred on dates that do not coincide with scheduled business trips or that were incurred while the employee was on leave time. What category or categories of expense reimbursement scheme would this report most likely identify?

Answer: Beta's report would most likely detect a mischaracterized expense scheme. Since the report targets expenses that were incurred on leave time or apart from scheduled business trips, it most likely would highlight personal expenses that are being claimed as business expenses. Beta's report could also catch a fictitious expense scheme because a fraudster who creates hypothetical expenses might inadvertently use dates that do not correspond to actual business trips.

Beta's test would be unlikely to detect overstated expenses or multiple reimbursements, because these two schemes both seek to create extra reimbursement for actual business expenses. These expenses would typically be incurred on scheduled business trips or meetings, not on personal or leave time. Thus, they would not be highlighted by Beta's report.

Discussion Issues

7-1 (Learning objective 7-4) What internal controls can be put into place to prevent an employee from committing a mischaracterized expense scheme?

Answer: If a company wishes to prevent employees from charging their personal expenses to the company, there are several things it can do. The company should require detailed expense reports for all reimbursable expenses. Expense reports should include the following information: original support documents, dates and times of business expenses, methods of payment, and descriptions of the business purpose for expenses. All travel and entertainment expenses should be independently reviewed by a direct

supervisor who is familiar with the employee's schedule and duties. High-level managers should not be exempt from this monitoring.

Organizations should also develop a policy on expenses that clearly explains what types of expenses are reimbursable and sets reasonable limits for expense reimbursements. This policy should be disseminated to all employees, who should be required to sign a statement acknowledging that they have received and understood its provisions.

Additionally, vacation and business schedules should be compared to the dates for which reimbursement is requested. This can help to prevent someone from claiming his or her vacation expenses as business related.

7-2 (Learning objectives 7-4, 7-6, and 7-8) In the case study "Frequent Flier's Fraud Crashes," what internal controls could have detected the fraud earlier?
Answer: Clarification and better enforcement of the policy that travel for the entire company must be booked through the company travel agent using a designated company credit card could have helped to detect Marcus Lane's fraud sooner, and likely would have prevented it altogether.

7-3 (Learning objectives 7-4, 7-6, 7-8, and 7-10) Discuss how establishing travel and entertainment budgets can help an organization detect expense reimbursement fraud.
Answer: Expense reimbursement fraud is very common and can be very difficult to detect. One detection method that is often employed is to compare expense reimbursement levels to budgeted amounts and prior years' expenses. This enables an organization to see if reimbursed expenses have significantly increased over expected and/or historical amounts, which may be a sign of fraud. In addition, establishing budgets is a good way to control costs, regardless of fraud. Finally, if employees know this kind of comparison is made, they may be less likely to attempt expense reimbursement schemes, at least on a large scale.

7-4 (Learning objectives 7-5 and 7-6) ABC Company has three in-house salespeople (Red, White, and Blue) who all make frequent trips to Santa Fe, New Mexico, where one of the company's largest customers is based. A manager at ABC has noticed that the average airfare expense claimed by Red for these trips is $755 round trip. The average airfare expense claimed by White is $778. The average airfare expense claimed by Blue is $1,159. What type of expense reimbursement fraud might this indicate, and what controls would you recommend to the company to prevent this kind of scheme?

Answer: These facts point to an overstated expense scheme. While all three salespeople have legitimate, business-related purposes for their trips, it appears that Blue might be inflating the costs of his airfare on his expense reports, given the fact that his flight costs are significantly higher than those claimed by the other two employees, even though they all have the same destination. (Note that additional investigation would be required to make sure there was not a legitimate reason for the discrepancy. For example, maybe Blue's flights coincided with busy travel dates or had to be booked at the last minute, which might have caused the extra expense).

Assuming this is an overstated expense scheme, the company should make sure to establish proper controls for the review of expenses, including detailed expense reports and independent review by direct supervisors. Furthermore, the company should specify that it will accept only original support for expenses, and should specify the type of support that is allowable (e.g., airline ticket receipts, not travel agency itineraries). It would be advisable for the company to have all travel booked through a centralized in-house department, or through a specified travel agency using a company credit card. This would help ensure consistency in travel costs and should prevent an employee from exaggerating his expenses.

7-5 (Learning objectives 7-7 and 7-8) Baker is an auditor for ABC Company. He is reviewing the expense reports that Green, a salesperson, has submitted over the last 12 months. Baker notices that Green's expenses for "customer development dinners" consistently range between $160 and $170, and the amounts are almost always a round number. ABC Company has a policy that limits reimbursement for business dinners to $175 unless otherwise authorized. In addition, most of the expense reports show that Green paid for the meals in cash, even though he has been issued a company credit card that he usually uses for other travel and entertainment expenses. What kind of expense reimbursement scheme is most likely, based on these circumstances?

Answer: These facts are all consistent with a fictitious expense scheme, particularly because the expenses are just below the reimbursement limit and were ostensibly paid in cash, which is not how Green normally pays for business expenses. Fraudsters who commit fictitious expense schemes often claim to have paid in cash because this explains the lack of an audit trail for the expense. It is also possible that this is a mischaracterized expense scheme (involving personal expenses) or an overstated expense scheme in which Green is inflating the costs of real business dinners.

7-6 (Learning objective 7-10) What internal controls would help to prevent an employee from claiming an expense more than once?
Answer: Employees should be allowed to submit only original receipts for expenses. They should be required to submit all documentation of expenses, including receipts showing charge totals, and that includes details of what exactly was purchased. Photocopies of receipts should not be allowed. Additionally, expense reports should identify the budget from which the reimbursement should be paid, to help prevent multiple reimbursements being made from two different budgets. All expense reports should be closely reviewed by both the supervisor and accounting personnel for potential fraud.

Chapter 8

Review Questions

8-1 (Learning objective 8-1) What is a register disbursement scheme?
Answer: A register disbursement scheme is a type of occupational fraud in which an employee processes a fraudulent reversing transaction on a cash register to justify the removal of cash from that cash register.

8-2 (Learning objective 8-2) How do register disbursement schemes differ from skimming and cash larceny, both of which frequently involve thefts of cash from cash registers?
Answer: Register disbursements schemes differ from other types of cash register frauds in that in these schemes the removal of money is recorded on the cash register as though it were a legitimate disbursement of funds. This is why these schemes are referred to as register disbursements. In skimming and cash larceny, by contrast, there is no record of the disbursement.

8-3 (Learning objective 8-3) What are the two main categories of register disbursement schemes?
Answer: The two basic fraudulent disbursement schemes that take place at the cash register are false refunds and false voids.

8-4 (Learning objective 8-4) What is the difference between a fictitious refund scheme and an overstated refund scheme?

Answer: In a fictitious refund scheme the fraudster processes a refund as if a customer were returning merchandise, even though there is no actual return. The perpetrator then steals cash from the register in the amount of the false return. The disbursement appears legitimate because the register tape shows that a merchandise return has been made. Because the money that was taken from the register was supposed to have been removed and given to a customer as a refund, the register tape balances with the amount of money in the register. This scheme differs from an overstated refund scheme in which the fraudster overstates the amount of a legitimate refund and skims off the excess money.

8-5 (Learning objective 8-5) How are fraudulent void schemes used to generate a disbursement from a cash register?
Answer: Normally, when a sale is voided, an honest employee attaches a copy of the customer's sales slip to a completed void slip and asks a manager to initial the transaction for approval. To process a falsified void slip, a fraudster must first get access to a customer's sales slip and then get the approval of the transaction from a manager. A customer's sales slip can be obtained by simply "forgetting" to give it to a customer. The fraudulent transaction is completed when the dishonest employee takes the cash from the register. The copy of the customer's receipt is used to verify the authenticity of the transaction.

8-6 (Learning objective 8-6) How do register disbursement schemes cause shrinkage?
Answer: When a false refund or void is recorded on a cash register, two things happen. The first is that the employee committing the fraud removes cash from the register, and the second is that the item allegedly being returned is debited back into inventory. The result is shrinkage: The amount of inventory that is actually on hand will be less than the amount that should be on hand.

8-7 (Learning objective 8-7) How can the processing of low-dollar refunds help a fraudster conceal a register disbursement scheme?
Answer: Companies often set limits below which management review of a refund is not required. When this is the case, fraudsters are sometimes able to avoid detection by processing numerous refunds that fall below the review limit, as opposed to processing a smaller number of high-dollar transactions.

8-8 (Learning objective 8-8) Why is it important for all cashiers to maintain distinct login codes for work at the cash register?

Answer: If all cashiers are required to log into a cash register before using it, this enables an organization to trace fraudulent reversing transactions back to the employee who processed them. It also enables organizations to run tests for various red flags such as employees who process an inordinate number of reversing transactions, process transactions for unusually large amounts, process recurring transactions for the same amount, and so on.

Discussion Issues

8-1 (Learning objective 8-4) In the case study involving Bob Walker at the beginning of this chapter, what type of register disbursement schemes did he commit? Discuss the role his recent demotion played in the scheme.

Answer: Bob Walker committed fictitious refund and overstated refund schemes. In both cases, he took money from the cash register and wrote fake cash refunds by recording either fictitious or real names and telephone numbers in the refund log. With the use of real names, he simply altered legitimate refunds that he had issued earlier in the day.

Shortly before the scheme began, Walker was demoted and received a pay cut. This likely provided the rationalization Walker needed to commit the scheme. Recall that under the Fraud Triangle model, there are three factors that are typically present when an employee commits fraud. A non-shareable financial need, a perceived opportunity, and a rationalization. Wanting to get even with one's company for perceived unfair treatment is a common rationalization that is used to justify fraud. Indeed, when confronted about his crime, Walker referred to his managers who had "unjustly" demoted him.

The pay cut may also have created a non-shareable financial need for Walker. In his interview with the investigators he stated that he had financial problems that were exacerbated by the pay cut, and that proceeds from the fraud initially went to his mortgage payments.

8-2 (Learning objective 8-2) In the *2009 Global Fraud Survey*, register disbursements were reported far less frequently than any other fraudulent disbursement scheme. Discuss some reasons why this result might not reflect the true frequency of register disbursements.

Answer: Although register disbursement schemes accounted for a small percentage of the reported fraudulent disbursement schemes, it must be remembered that the respondents to the survey were only asked to report one case they had investigated; the study was not designed to measure the overall frequency of various types of schemes within a particular organization. So the low response rate for register disbursements does not necessarily reflect how often these schemes occur. Furthermore, the type of fraud that occurs within an organization is to some extent determined by the nature of business the organization conducts. For example, register disbursement schemes would tend to be much more common in a large retail store that employs several cash register clerks than in a law firm where a cash register would not even be present.

8-3 (Learning objectives 8-8 and 8-9) What are some tests that can help detect fictitious refund schemes that involve the overstatement of inventories?

Answer: When a customer returns merchandise, a journal entry is normally made to increase the merchandise inventory account and decrease the cost of goods sold account for the cost of the returned merchandise. In a fictitious refund scheme, no merchandise is actually returned. Nevertheless, the same journal entry is made as if a real refund were taking place. Because no merchandise was returned, the merchandise inventory account is overstated and will not agree with the actual inventory on hand. This scheme may be detected by periodically taking a count of the physical inventory and comparing it to the perpetual inventory records, which measure the amount of inventory that "should be on hand." An unusual discrepancy may indicate that a fictitious refund scheme is occurring. However, in many register disbursement cases the level of shrinkage is not large enough to raise a red flag. Other tests that could be used to detect fictitious refund schemes include running audit tests for the following conditions:

- *Locations with unusually high levels of refunds or voids*
- *Employees who process unusually high levels of refunds or voids*
- *Unsupported adjustments to inventory, particularly those entered by employees who also record refunds or voids*

8-4 (Learning objective 8-4) In the "silent crime" case study mentioned in the chapter, how did Joe Anderson involve other individuals in his credit card refund scheme?

Answer: Joe eventually used over 200 credit cards belonging to 110 individuals to steal from his employer. Each week he would credit over $2,000 in fake returns to the credit cards of his friends, neighbors, and relatives. In return, he was paid up to 50 percent of the amount charged to the credit card.

8-5 (Learning objectives 8-8 and 8-9) Explain how each of the following three conditions could be a red flag for a register disbursement scheme.

1. Able, a cash register teller, is authorized to approve sales refunds and she is also authorized to make inventory adjustments.
2. Baker is a cashier who, in the last week, processed 15 refunds. No other cashier processed more than 5 over that same period. Each of the transactions was for between $13.50 and $14.99.
3. Over 70 percent of the refunds processed by Chase, a cash register clerk, were run on the same date as the original sale.

Answer: The conditions under which Able works are ripe for fraud. Able is a cash register teller, which means she is in a position to enter refunds, but she also has the authority to approve refunds, meaning there is an inadequate separation of duties. In addition, Able is authorized to make inventory adjustments, which could enable her to conceal any shrinkage that would result from a register disbursement scheme. Even though this scenario does not contain any evidence that Able is actually committing fraud, the conditions are such that if she did commit fraud, she would most likely be successful.

The fact that Baker processed three times more refunds than any other cashier over the relevant period does not prove that he is involved in a register disbursement scheme, but it is consistent with that type of scheme and there is sufficient reason to conduct further inquiry. The fact that all of the refunds were for amounts in a very narrow range just under $15.00 is also suspicious. It would be worth checking to see whether Baker's company has a review limit for refunds at or near $15, since the pattern of his transactions suggests he may be structuring false refunds to avoid review.

The scenario involving Chase contains less hard evidence than the other two, but the fact that most of the refunds Chase processes occur on the same date as the underlying sales could point to fraud. It would make sense for an employee to run fraudulent refunds close to the time of the original sale, since he would be more likely to remember the details from the sales transaction, such as the amount, the customer's name, the item purchased, etc. There is no information here that would tell us whether it is typical for a customer to return merchandise on the same date he or she purchased it, but that is something that should be tested, given the information here.

Chapter 9

Review Questions

9-1 (Learning objective 9-1) What are the five categories of schemes used to misappropriate non-cash tangible assets identified in this chapter?

Answer: The five categories identified in this chapter are misuse, unconcealed larceny, asset requisitions and transfers, purchasing and receiving schemes, and fraudulent shipments.

9-2 (Learning objective 9-2) According to the *2009 Global Fraud Survey*, how do non-cash misappropriations compare with cash misappropriations in terms of frequency and cost? What two types of non-cash assets were most commonly misappropriated?

Answer: According to the 2009 Global Fraud Survey, *cash schemes were much more common than non-cash schemes. Eighty-six percent of asset misappropriations involved the theft of cash, whereas only 20% involved the theft or misuse of non-cash assets. In terms of median loss, cash schemes were also slightly costlier: cash schemes had a median loss of $120,000, while non-cash schemes had a median loss of $90,000. Physical assets, such as equipment and inventory, were the most frequently targeted type of non-cash asset in the study, with seventy-five percent of non-cash cases involving the misappropriation of a physical asset.*

9-3 (Learning objective 9-3) What are some examples of asset misuse? Give at least three.

Answer: There are many ways in which non-cash assets are misused by employees without being stolen. Company vehicles can be used for personal trips. Computers, supplies, and office equipment can be used by employees for personal work on company time. Employees might also take home tools or equipment for a personal project, then return them.

9-4 (Learning objective 9-4) What is an "unconcealed larceny" scheme?

Answer: An unconcealed larceny scheme is one in which an employee takes property from the organization without attempting to conceal the theft on the organization's books and records.

9-5 (Learning objective 9-6) Able is a job-site supervisor for ABC Construction. Able is responsible for overseeing the construction of a number of residential homes, and for making sure each of his crews has sufficient materials to complete its work. All of ABC's lumber and other building materials are stored in a central warehouse and are released upon signed authorization from job-site supervisors as needed. Able requests twice the amount of lumber that is actually needed for a particular job. He uses the excess materials to build a new deck on his home. How would Able's scheme be categorized?
Answer: Able has committed an asset requisition and transfer scheme. He falsified internal materials requisitions in order to gain access to lumber that he then stole. This is not a case of unconcealed larceny because Able falsified documentation (the materials requisition) to conceal the theft (by justifying the removal of the lumber from the warehouse).

9-6 (Learning objective 9-9) What is "shrinkage"?
Answer: Shrinkage is the unaccounted-for reduction in an organization's inventory that results from theft. When inventory is stolen, shrinkage is generally the key concealment issue for the fraudster.

9-7 (Learning objectives 9-8 and 9-10) Baker works in the sales department of ABC Company, which manufactures computer chips. Baker creates false documentation indicating that XYZ, Inc. (a nonexistent company) has agreed to purchase a large quantity of computer chips. The computer chips are shipped to XYZ, Inc. "headquarters," which is really Baker's house. How would Baker's scheme be categorized and what are some red flags that might occur as a result of the scheme?
Answer: Baker's scheme would be classified as a fraudulent shipment. The fake sale he generated resulted in the unauthorized shipment of inventory to a nonexistent customer. Several red flags could show up in this scheme:

- *The "customer" has the same address as Baker, an employee.*
- *The "sale" was fabricated, meaning any support documents and/or authorization for the sale were bogus.*
- *Since the customer does not exist, no credit check could have been done on XYZ prior to the issuance of this sale on credit. (The sale had to have been on credit since XYZ, a nonexistent company, could not have paid for the chips.)*
- *Presumably, XYZ's account will age and eventually need to be written off as uncollectible.*

9-8 (Learning objective 9-7) How do employees use falsified receiving reports as part of schemes to steal inventory?
Answer: Falsified receiving reports are sometimes used as part of a purchasing and receiving scheme. The perpetrator—typically a warehouse employee—falsifies records of incoming shipments by marking them "short" (meaning that items were missing) or by listing certain items as being damaged or substandard. The perpetrator then steals the unaccounted-for items. For instance, if 1,000 units of an item are received, the fraudster indicates that only 900 are received, then steals the 100 "missing" units.

9-9 (Learning objective 9-10) What is meant by the term "physical padding"?
Answer: Physical padding is a method for concealing inventory theft in which fraudsters attempt to create the physical appearance of extra inventory in a warehouse or stockroom to compensate for the inventory they have stolen. For example, empty boxes may be stacked on top of existing inventory or merchandise may be moved from one storage location to another so that it is counted twice.

9-10 (Learning objective 9-10) What are the four methods identified in this chapter by which employees conceal inventory shrinkage?
Answer: The four methods are: (1) altering inventory records (or forced reconciliation); (2) creating fictitious sales and debiting fictitious or existing accounts receivable (and in some cases writing off the fictitious accounts); (3) writing off non-cash assets as scrap, lost, damaged, obsolete, and so on; and (4) physically padding the warehouse or storeroom.

9-11 (Learning objective 9-11) Provide an example of a misappropriation of intangibles scheme.
Answer: An example of an intangibles scheme is an employee who, out of a sense of entitlement, steals a building plan he helped design from his former employer to attempt to get ahead in his new job with a competitor. Another example is a disgruntled employee who retaliates against his employer, for perceived unfair treatment, by selling a trade secret of his employer to a competitor.

Discussion Issues
9-1 (Learning objective 9-3) Jones is the manager of ABC Auto Repair. Unbeknownst to his employer, Jones also does freelance auto repair work to earn extra cash. He

sometimes uses ABC's facilities and tools for these jobs. Discuss the costs and potential costs that ABC might suffer as a result of Jones's actions.

Answer: Jones is engaged in a misuse scheme that could cause losses to ABC in a number of ways. First, Jones is making unauthorized use of tools that could damage them or shorten their lifespan. Second, ABC may suffer from a loss of productivity since Jones is performing freelance repairs at ABC's facilities. He is occupying space, equipment, and labor that could be used for legitimate business. The company may even have to buy new equipment or hire additional labor to make up for the shortfall. Third, ABC may be losing customers as a result of Jones's scheme. Presumably, at least some of the customers who have hired Jones to fix their cars would have come to ABC if he were not freelancing. Jones also has an unfair competitive advantage in this respect. His expenses are significantly lower than ABC's, since he is getting free use of facilities and equipment that most likely required a significant investment by ABC. Therefore, he is probably undercutting ABC's prices in order to attract customers, which is common in this type of scheme.

9-2 (Learning objectives 9-4 and 9-5) Discuss how establishing a strong system of communication between employees and management can help deter and detect inventory larceny.

Answer: As was discussed in this chapter, employees often know that others in the organization are stealing assets, yet they refrain from reporting the crimes. This can occur for a number of reasons, such as a sense of duty to friends, a "management versus labor" mentality, intimidation, poor channels of communication, or simply not knowing how to report a crime. When management makes an effort to foster open communication with employees, this removes many obstacles that may otherwise keep thefts from being reported. Employees should be educated on how fraud hurts everyone in the organization, and they should be made aware that crimes can be reported anonymously and without fear of retribution. In addition, a clear means of reporting crimes (such as a hotline) should be specified so that employees know how and to whom they can make their reports. Remember that according to the 2009 Global Fraud Survey, *employee tips are one of the most common methods for detecting occupational fraud. Organizations that do not make use of employees as a fraud detection tool are shortchanging themselves.*

9-3 (Learning objectives 9-5 and 9-6) In the case study "Chipping Away at High-Tech Theft," do you believe the procedures and controls maintained by the manufacturer contributed to the theft? Why or why not?

Answer: While the company's controls and procedures (or lack thereof) did not cause the theft, they certainly contributed to its success. There were a number of deficiencies that aided Larry Gunter in his scheme. First, the company had no internal transfer documentation, which meant that product could be moved from one building to another without being accounted for. Employees were simply moving the inventory across an open, unmonitored parking lot without boxes being checked or documented. To compound the problem, the company's security cameras were set up improperly so that they did not deter theft, and security tapes were not saved long enough, which made the security cameras useless in trying to determine who had committed the thefts. In addition, security guards were inattentive and did not do a good job of checking the product that left the building. Finally, the fact that the company verified its product inventory only once a month meant that it took longer for the company to detect the missing inventory.

9-4 (Learning objective 9-5) Discuss the controls that an organization should have in place to effectively prevent and detect larceny of inventory.

Answer: As with most forms of asset misappropriation, the first key to preventing and detecting non-cash larceny is to make sure the organization has adequately separated duties. To prevent inventory larceny, it is crucial that the duties of requisitioning, purchasing, and receiving inventory should be separated. In addition, physical controls should be in place. All merchandise should be physically guarded and locked, with access restricted to authorized personnel only. Access logs should be used to track those who enter restricted areas, including their entry times. Any removal or transfer of inventory to another location should be properly documented. Security cameras also can be effective at deterring theft of inventory. To maximize the deterrent effect of security cameras, employees should be made aware of the presence of the cameras. Physical inventory counts should be conducted on a periodic basis by someone independent of the purchasing and warehousing functions. Shipping and receiving activities should be suspended during physical counts to ensure a proper cut-off, and the physical counts should be subject to recounts or spot-checks by independent personnel. It is also important for organizations to have in place a mechanism for receiving customer complaints, to help detect cases in which employees steal merchandise from outgoing shipments. An employee who is independent of the purchasing and warehousing functions should be assigned to follow up on complaints.

9-5 (Learning objective 9-7) Baker was in charge of computer systems for ABC Company. As part of a general upgrade, the company authorized the purchase of 20 new computers for the employees in its marketing department. Baker secretly changed the order so that 21 computers were purchased. When they were delivered, he stole the extra computer. Later, 10 more new computers were purchased for the 10 employees in the company's research and development department. Baker also stole one of these computers. How should these two schemes be classified under the fraud tree?
Answer: The first scheme should be classified as a billing scheme (personal purchases), and the second scheme should be classified as a non-cash misappropriation (purchasing and receiving). The difference in the two frauds is that in the first, Baker caused the company to buy a computer it did not need. The harm to the company was that it overpaid for what it received. The fact that Baker took the computer is inconsequential because the company did not need and did not order the computer; Baker could have purchased anything with the excess funds and the harm to the company would have been the same.

In the second scheme, Baker stole an asset that was intentionally purchased by the company. All 10 computers were needed for the 10 employees in the research and development department. Now, the company has not only lost the money it paid for the computer, but it has lost the computer itself and will presumably have to replace it. This scheme is classified as a non-cash misappropriation because the harm to the company is that it has been deprived of a non-cash asset.

9-6 (Learning objectives 9-8 and 9-12) Baker is an auditor for ABC Company. As part of a proactive fraud audit, Baker runs the following tests: (1) a review of the Sales Register for dormant customer accounts that posted a sale within the last two months; and (2) a comparison of the Sales Register and the Shipment Register for shipping documents that have no associated sales order. Taken together, what type of non-cash scheme is Baker most likely to find with these tests? Explain how each one might identify fraud.
Answer: The tests Baker is performing were both identified in this chapter as proactive audit tests for false shipments. The first test may identify cases in which employees have posted fraudulent sales to justify the false shipment of inventory. Frequently, these fraudulent sales are charged to dormant accounts and then allowed to age or are subsequently written off. The second test would tend to identify cases in which inventory was fraudulently shipped offsite without a corresponding sale, a clear indicator of fraud.

9-7 (Learning objective 9-8) Explain why the following circumstances might indicate that one or more employees are stealing merchandise: (1) an increase in uncollectible sales from previous periods and (2) an increase in damaged or obsolete inventory from previous periods.

Answer: The conditions listed above are consistent with two techniques that are sometimes used to conceal the theft of merchandise. As was explained in this chapter, employees sometimes create fictitious sales to justify the shipment of merchandise, then later write off those sales as uncollectible. Similarly, employees sometimes designate merchandise as damaged or obsolete, either to justify the fact that it is missing, or to make it easier to steal (because some organizations do not maintain strict controls over scrap items). Keep in mind that neither of these conditions provides concrete proof that fraud has occurred; there may be legitimate reasons to explain them. But they may be sufficient to warrant further investigation, particularly if combined with other indicators of fraud, such as missing inventory.

Chapter 10

Review Questions

10-1 (Learning objective 10-2) What are the four categories of corruption?

Answer: The four categories of corruption schemes are bribery, illegal gratuities, economic extortion, and conflict of interest.

10-2 (Learning objective 10-4) How are bribery, extortion, and illegal gratuities different?

Answer: While bribery seeks to influence a decision, an illegal gratuity rewards such decision, after the fact. Extortion schemes use coercion by demanding payment from another to prevent harm or loss of business.

10-3 (Learning objective 10-5) What are the two classifications of bribery schemes?

Answer: Bribery schemes fall into two broad categories: kickbacks and bid-rigging schemes.

10-4 (Learning objective 10-6) What are some of the different types of kickback schemes?

Answer: Kickback schemes may take the form of diverting extra business to a certain vendor, approving inflated or fictitious invoices for payment, or allowing the acceptance of substandard product.

10-5 (Learning objective 10-7) What is a bid-rigging scheme?
Answer: Bid-rigging occurs when an employee of a purchasing company illegally assists a certain vendor to win a contract by compromising the competitive bidding process.

10-6 (Learning objective 10-7) How are bid-rigging schemes categorized?
Answer: Generally, bid-rigging schemes are categorized according to the stage of bidding at which the fraud occurs. This may be at the pre-solicitation phase, the solicitation phase, or the submission phase in the competitive bidding process.

10-7 (Learning objective 10-8) How might competition be eliminated in the solicitation phase of a bid-rigging scheme?
Answer: A corrupt contractor may pay an employee of the purchasing company to ensure that one or more of the contractor's competitors are not allowed to bid on the contract. This might occur by requiring bidders to be represented by certain sales or manufacturing representatives. Other ways of limiting or eliminating competition may include bid pooling or soliciting bids from fictitious suppliers.

10-8 (Learning objective 10-8) What types of abuses may be found in the submission phase of a bid-rigging scheme?
Answer: Some types of abuses found in the submission phase include compromising the confidentiality of the sealed-bid process, giving information to certain vendors on how to prepare their bid, or falsifying the bid log.

10-9 (Learning objective 10-11) What is a conflict of interest?
Answer: A conflict of interest occurs when an employee, manager, or executive has an undisclosed economic or personal interest in a transaction that adversely affects the company. The key word in this definition is undisclosed. The crux of a conflict case is that the fraudster takes advantage of his employer; the victim organization is unaware that its employee has divided loyalties.

10-10 (Learning objective 10-12) What is meant by the term "turnaround sale"?
Answer: In this type of purchasing scheme, an employee is aware that his company plans to purchase a specific asset, such as land, so the employee then takes advantage of his knowledge by purchasing the asset himself. The asset is then sold to the company by the employee at an increased rate.

10-11 (Learning objective 10-12) How are underbillings usually accomplished?
Answer: In this type of sales scheme, an employee undercharges a vendor in which he has a hidden interest. The victim company then ends up selling its goods or services at less than fair market value, resulting in a diminished profit margin or even a loss on the sale.

10-12 (Learning objective 10-12) What is the difference between business diversions and resource diversions?
Answer: While both are considered conflicts of interest in which "favors" may be performed, business diversions tend to involve cases in which the employee undercuts his own employer through activities such as steering potential clients toward the employee's business and away from the company's business, resulting in unfair competition and a loss to the victim company. Comparatively, resource diversions consist of the actual manipulation of a company's funds or monetary resources to the benefit of the employee.

Discussion Issues
10-1 (Learning objective 10-3) Offering a payment can constitute a bribe, even if the illegal payment is never actually made. Why?
Answer: Because the purpose of a bribe is "to influence," the mere offering of a bribe may serve that end.

10-2 (Learning objective 10-1) What is the common ingredient shared by the four classifications of corruption?
Answer: Bribery, illegal gratuities, economic extortion, and conflicts of interest each involve the exertion of an official's or employee's influence to the detriment of his constituency or company.

10-3 (Learning objective 10-3) What is the difference between official bribery and commercial bribery?
Answer: While official bribery seeks to influence an official act, that is, the decisions of government agents or employees, commercial bribery attempts to influence a business decision.

10-4 (Learning objectives 10-6 and 10-9) If you suspected someone of being involved in a kickback scheme, what would you look for?

Answer: Kickback schemes often involve diverting business to a certain vendor, overbilling for goods or services, or paying for fictitious goods or services. Therefore, some of the indications of a kickback scheme may include goods being ordered repeatedly from the same vendor, established bidding policies not being followed, and higher costs of materials than normal.

10-5 (Learning objective 10-6) An employee can implement a kickback scheme regardless of whether she has approval authority over the purchasing function. How might this be accomplished?

Answer: An employee might be able to circumvent accounts payable controls by filing a false purchase requisition. If the person with the authority to approve this requisition relies on the corrupt employee and does not exercise proper judgment and responsibility, this type of scheme may be accomplished without the fraudster having purchasing approval authority.

10-6 (Learning objectives 10-7, 10-8, and 10-9) What are some clues that might alert you to possible fraudulent activity at the different stages of a bid-rigging scheme?

Answer: Suspicions of a bid-rigging scheme might arise when seemingly unnecessary restrictions that artificially limit competition are placed in the solicitation documents. At the pre-solicitation phase, this includes:

- *Tailoring specifications of a contract to fit the capabilities of a single contractor*
- *Providing confidential information about the contract on a preferential basis*
- *Splitting the contract into several smaller parts in order to circumvent mandatory bidding thresholds*

At the solicitation phase, this includes:

- *Allowing only companies that are represented by a certain sales representative to submit bids*
- *Bid pooling, whereby several bidders conspire to split the contract up and ensure that each gets a certain piece*
- *Soliciting bids from fictitious suppliers*

At the submission phase, this includes:

- *Abuse of the sealed-bid process*
- *Providing information to certain vendors on how to prepare their bid*
- *Falsifying the bid log*
- *Extending the bid opening date*

10-7 (Learning objective 10-11) How do conflicts of interest differ from bribery?
Answer: Conflicts of interest and bribery are both distinct forms of corruption. A typical bribery case involves a fraudster who approves an invoice and receives a kickback in return, whereas a conflict case generally involves a fraudster who approves an invoice because of his own hidden interest in the vendor. Although the two schemes are very similar, the fraudsters have different motives. In the bribery case, the fraudster approves the invoice because he receives some form of payment from a third party. In the conflict case, the fraudster approves the invoice because of his secret interest in the vendor; in a sense, the fraudster is the third party.

10-8 (Learning objective 10-12) Compare the characteristics of purchasing schemes to sales schemes.
Answer: Purchasing schemes are the most common type of conflict of interest. In purchasing schemes, the victim company unwittingly buys something at a high price from another company in which one of its employees has a hidden interest. Comparatively, sales schemes take place when a victim company sells something at a low price to a company in which one of its employees has a secret hidden interest.

10-9 (Learning objectives 10-10 and 10-12) Assume an employee is responsible for purchasing an apartment complex on behalf of his company. The employee owns stock in the management company that operates the apartment complex. The employee does not let his company know about his stock ownership, and proceeds to make the purchase. Why does this example represent a conflict of interest?
Answer: This case is an example of a purchasing scheme. Because the employee owns stock in the management company that operates the apartment complex and will profit from the sale of the complex, the employee may not negotiate to get the best price for his employer. This is a conflict of interest because it violates the employee's duty of good faith to his company.

10-10 (Learning objectives 10-9 and 10-13) What are some of the ways organizations can determine whether a particular vendor is being favored?
Answer: Companies can review tips and complaints from competing vendors. Companies can also compare the addresses of their vendors to the addresses of their employees to determine whether a match exists, indicating a possible conflict of interest. Vendor ownership information should also be kept on file and updated whenever an ownership

change takes place. Purchasing personnel can also be interviewed and asked whether any vendors are receiving favorable treatment.

Chapter 11

Review Questions

11-1 (Learning objective 11-1) Why are the fraudulent statement methods under discussion referred to as "financial statement fraud"?
Answer: They are referred to as financial statement fraud because the fraudster participates in falsification of a company's financial statements, typically either by overstatement of revenue/assets or understatement of expenses/liabilities.

11-2 (Learning objective 11-2) There are three main groups of people who commit financial statement fraud. Who are they?
Answer: The three main groups of people who commit financial statement fraud are organized criminals, mid- and lower-level employees, and senior management.

11-3 (Learning objective 11-3) What are the three primary reasons people commit financial statement fraud?
Answer: The three main reasons people commit financial fraud are to conceal true business performance, to preserve personal status/control, and to maintain personal income/wealth.

11-4 (Learning objective 11-4) What are the three general methods commonly used to commit financial statement fraud?
Answer: The three general methods commonly used to commit financial statement fraud are playing the accounting system, beating the accounting system, and going outside the accounting system.

11-5 (Learning objective 11-5) What is meant by the term "overstatement"?
Answer: "Overstatement" refers to a financial statement fraud in which the perpetrator purposely inflates a company's financial information (assets or revenues) to provide a false picture of the company's performance.

11-6 (Learning objective 11-6) What is meant by the term "understatement"?
Answer: "Understatement" refers to a financial statement fraud in which the perpetrator provides a lowered value of a company's financial information (liabilities or expenses).

11-7 (Learning objective 11-7) What are the components of the conceptual framework for financial reporting?
Answer: The components of the conceptual framework for financial reporting include recognition and measurement concepts—the economic entity, going concern, monetary unit, and periodicity assumptions; the historical cost, revenue recognition, matching, and full disclosure principles; and the cost-benefit, materiality, industry practice, and conservatism constraints—as well as the qualitative characteristics of relevance, reliability, comparability, and consistency.

11-8 (Learning objective 11-8) Define the term "financial statement" and provide examples of types of financial statements used in companies.
Answer: The term financial statement refers to almost any financial data presentation that is prepared in accordance with generally accepted accounting principles. Some common types of financial statements include balance sheets, statements of cash flows, summaries of operations, proxy statements, and registration statement disclosures.

Discussion Issues
11-1 (Learning objective 11-1) Why is financial statement fraud commonly referred to as "cooking the books"?
Answer: Financial statement fraud is commonly referred to as "cooking the books" because it involves the false presentation of a company's financial data. Records (or books) are manipulated by the fraudster to overstate or understate a company's financial information.

11-2 (Learning objectives 11-2 and 11-3) Compare the three main groups of people who may commit financial statement fraud, and describe their potential reasons for the fraud.
Answer: Financial statement fraud may be committed by organized criminals, who may engage in the fraud as part of a scheme to obtain fraudulent loans from a financial institution. A second group that may commit financial statement fraud is mid- and lower-level employees, who may falsify financial statements for their own area of responsibility for purposes of concealing their true business performance. The third group that may commit financial statement fraud is senior management. This group may have varied motives, but some common reasons include to maintain their own personal wealth or salary, or to preserve their status and control.

11-3 (Learning objective 11-4) Although three general methods of producing fraudulent statements have been identified, one of these methods is typically used first. Which method is this, and why is it more likely to be selected first as opposed to the other two?
Answer: In producing fraudulent statements, the method referred to as "playing the accounting system" is usually committed first. In this method, the fraudster uses the company's accounting system to produce desired results (e.g., to increase or decrease earnings to a desired dollar amount), taking advantage of regular practices such as reporting of genuine sales. The other two methods (beating the accounting system and going outside the accounting system) require more direct manipulation to achieve desired results.

11-4 (Learning objective 11-7) What is the generally accepted accounting principle known as matching? Describe how a company may be involved in fraud that violates this principle.
Answer: The concept of matching refers to the standard that books and records from a given time period must coincide with the revenue and expenses in the same time period. Fraud can take place when a company purposely counts revenue from the subsequent year in the current year, or when it records the current year's expenses in the following year.

11-5 (Learning objective 11-7) Management of a cellular phone company learns that a new technological advance will occur within the next year that will make the company's current phones and related products obsolete. As a result, there is a strong chance that the company will close. When financial statements appear for auditors, management does not reveal its knowledge of the new technology. In this case, what accounting concepts are involved?
Answer: In this example, management has reason to question the "going concern" assumption with regard to this business. This concept assumes that a business can continue indefinitely; however, when evidence reveals otherwise, management has a duty to report negative information that will affect a company's future ability to earn revenue. Therefore, the principle of "full disclosure" has been violated.

11-6 (Learning objective 11-8) In an organization, who is generally responsible for the financial statements, and how can those responsible help to deter financial statement fraud?

Answer: Financial statements are the responsibility of a company's management, which means that financial statement fraud is rarely committed without the knowledge of members of management. In the instances in which management is not responsible for investigating suspected frauds, it is critical that a code of conduct is in place. This will provide an ethical standard for all employees to follow, which in turn will decrease the likelihood of financial statement fraud.

Chapter 12

Review Questions

12-1 (Learning objective 12-1) What is financial statement fraud?

Answer: Financial statement fraud is the deliberate misstatement or omission of amounts or disclosures in the financial statements to deceive financial statement users.

12-2 (Learning objective 12-2) List five different ways in which financial statement fraud can be committed.

Answer: Five ways in which financial statement fraud can be committed are (1) fictitious revenues, (2) timing differences, (3) concealed liabilities and expenses, (4) improper disclosures, and (5) improper asset valuation.

12-3 (Learning objective 12-3) What are the two methods of engaging in fictitious revenues?

Answer: Fictitious revenues schemes can involve making fictitious sales, which involves the use of fake or phantom customers and/or legitimate customers. The second method of recording fictitious revenues is to utilize legitimate customers and artificially inflate or alter invoices reflecting higher amounts or quantities than actually sold.

12-4 (Learning objective 12-3) What are the two most common pressures and motivations to commit financial statement fraud?

Answer: Owners may feel pressured by bankers, stockholders, and even family and community to exceed financial analysts' earnings forecasts. Additionally, departmental budget requirements may place pressures on managers to meet income and profit goals.

12-5 (Learning objective 12-4) List three methods of engaging in timing differences.

Answer: Schemes involving timing differences usually take the form of one of three methods: (1) failing to match revenues with expenses, (2) early revenue recognition, or (3) recording expenses in the wrong period.

12-6 (Learning objective 12-4) What is the motivation for violating the generally accepted accounting principle of matching revenues with expenses? What is the result of committing this fraud?
Answer: Typically, the motivation for this type of timing difference scheme is to boost net income for the current year. The result is the overstatement of net income of the company in the period in which the sales were recorded. However, it also has the effect of understating net income in the subsequent year when the corresponding expenses finally are reported.

12-7 (Learning objective 12-4) What is the motivation of early revenue recognition? What is the result of engaging in this type of fraud?
Answer: The motivation for early revenue recognition is to show additional profit. This fraud leads to earnings misrepresentation and frequently serves as a catalyst to further fraud.

12-8 (Learning objective 12-5) List the three common methods for concealing liabilities and expenses.
Answer: The three common methods for concealing liabilities and expenses are (1) omitting liabilities/expenses, (2) capitalizing expenses, and (3) failing to disclose warranty costs and liabilities.

12-9 (Learning objective 12-5) What is the motivation for concealing liabilities and expenses?
Answer: The motivation for concealing liabilities and expenses is to report inflated financial results. Concealing liabilities improves the company's balance sheet, and concealing expenses results in a higher reported net income.

12-10 (Learning objective 12-6) List five common categories of improper disclosures.
Answer: Five common categories of improper disclosures are liability omissions, significant events, management fraud, related-party transactions, and accounting changes.

12-11 (Learning objective 12-7) What are the four common forms of improper asset valuation?
Answer: Improper asset valuations usually take of one of the following forms: inventory valuation, business combinations, accounts receivable, and fixed assets.

12-12 (Learning objective 12-7) What is the likely result of committing an improper asset valuation?
Answer: This type of fraud tends to inflate the current assets at the expense of long-term assets, and thus falsely improves financial ratios, such as the current ratio and quick ratio.

12-13 (Learning objective 12-8) What is the difference between fraudulent financial reporting and misappropriation of assets?
Answer: Fraudulent financial reporting frequently involves a pressure or incentive to commit fraud and a perceived opportunity to do so. In general, fraudulent reporting occurs through intentional fraudulent omissions or inclusions in the financial statements. Asset misappropriation involves the theft or misuse of company assets.

12-14 (Learning objective 12-9) Describe three analytical techniques for financial statement analysis.
Answer: Horizontal analysis is a technique for analyzing the percentage change in individual financial statement items from one year to the next. Vertical analysis is the expression of the relationship or percentage of financial statement components to a - specific base item. Ratio analysis is a means of measuring the relationship between two different financial statement amounts.

Discussion Issues
12-1 (Learning objective 12-3) What is the most effective way to prevent fictitious revenue from being fraudulently reported in the financial statements?
Answer: FASB Concepts Statement No. 6 defines revenue as "inflows or other enhancements of assets of an entity or settlements of its liabilities (or a combination of both) from delivering or producing goods, rendering services, or other activities that constitute the entity's ongoing major or central operations." Implementing controls to ensure that the criteria inherent in this definition are met prior to recording revenue will assist in mitigating the problem of fictitious revenue.

12-2 (Learning objective 12-3) How can fictitious revenue be created through the use of false sales to shell companies? Discuss the method and result of committing this fraud.
Answer: A company's management can utilize several shell companies as customers in a number of favorable sales transactions. The sales transactions are fictitious, as are the

supposed customers. An example entry from this type of case is detailed below. A fictional entry is made to record a purchase of fixed assets:

Date	*Description*	*Debit*	*Credit*
12-01-X1	*Fixed Assets*	*300,000*	
	Cash		*300,000*

A fictitious sales entry is then made for the same amount as the false purchase:

Date	*Description*	*Debit*	*Credit*
12-01-X1	*Accounts Receivable*	*300,000*	
	Sales		*300,000*
12-01-X1	*Cash*	*300,000*	
	Accounts Receivable		*300,000*

From the above journal entry, we can see that the cash outflow that supposedly covered the purchase of assets is returned as payment on the receivable account to cover the fictitious sale. The result of the completely fabricated sequence of events is an increase in both company assets and yearly revenue.

12-3 (Learning objective 12-4) How might a company utilize timing differences to boost revenues for the current year? Discuss and analyze the method and result of committing the fraud.

Answer: Suppose at the end of the year, the following journal entry was made:

Date	*Description*	*Debit*	*Credit*
12-01-X1	*Accounts Receivable*	*20,000*	
	Sales—Project A		*20,000*

In January of next year, the project is started and completed. The entries below show accurate recording of the 15,000 of costs associated with the sale:

Date	*Description*	*Debit*	*Credit*
1-31-X2	*Cost of Sales—Project A*	*12,000*	
	Inventory		*12,000*
1-31-X2	*Labor Costs—Project A*	*3,000*	
	Cash		*3,000*

From the above journal entries we can see that a company may accurately record sales that occurred in the month of December, but fail to fully record expenses associated with those sales. This error overstates the net income of the company in the period in which the sales were recorded, and also understates net income when the expenses are reported.

12-4 (Learning objective 12-4) In the case study, "The Importance of Timing," what kind of fraud did the accountant commit? How could this fraud have been discovered?
Answer: He committed a fraud involving a timing difference. In this fraud, he made payment for materials and supplies in one year, even though they were not received until the next year. He also recognized the repair in the year that the actual repair occurred.

Division management asked Isbell to conduct an examination. He found $150,000 in repair invoices without proper documentation. The records for materials and supplies, which were paid for in one year and received in the next year, totaled $250,000. A check of later records and an inspection showed that everything paid for had, in fact, been received, just some days later than promised.

12-5 (Learning objective 12-5) Liability/expense omission is the preferred and easiest method of concealing liabilities/expenses. Why? Discuss how to detect this type of fraud.
Answer: Failing to record liabilities/expenses is very easy to conceal and very difficult to detect. The perpetrators of liability and expense omissions believe they can conceal their fraud in future periods. They often plan to compensate for their omitted liabilities with visions of other income sources such as profits from future price hikes. For example, the perpetrators may have planned to conceal the fraud by increasing the sales price in future periods when the expense would actually be recorded. These frauds can be discovered through a thorough review of all post-financial-statement-date transactions, such as accounts payable increases and decreases.

12-6 (Learning objective 12-7) What internal control activities and related test procedures can detect or deter overstated inventory?
Answer: When an overstated inventory scheme is suspected, the use of analytical procedures can help uncover suspicious activity. Red flags of overstated inventory include unusual growth in the number of days' purchases in inventory and an allowance for excess and obsolete inventory that is shrinking in percentage terms or that is otherwise out of line with industry peers.

Additionally, a review of the accounts receivable (A/R) aging report and bills of lading can help detect this fraud. For example, in one case described in this chapter, an A/R aging report indicated sales of approximately $1.2 million to a particular customer in prior months. The aging showed that cash receipts had been applied against those receivables. An analysis of ending inventory failed to reveal any improprieties because the relief of inventory had been properly recorded with cost of sales. Copies of all sales documents to this particular customer were then requested. The product was repeatedly sold FOB shipping point, and title had passed. But bills of lading indicated that only $200,000 of inventory had been shipped to the original purchaser. There should have been $1 million of finished product on hand for the food processor. However, there was nothing behind the facade of finished products. An additional comparison of bin numbers on the bill of lading with the sales documents revealed that the same product had been sold twice.

12-7 (Learning objective 12-9) What financial reporting analysis techniques can help to detect fraudulent financial statement schemes?

Answer: Three primary financial statement analysis techniques are available to the fraud examiner. The first is vertical analysis, which is a technique for analyzing the relationships between the items on an income statement, balance sheet, or statement of cash flows by expressing components as percentages. This method is often referred to as "common sizing" financial statements. In the vertical analysis of an income statement, net sales are assigned 100 percent; for a balance sheet, total assets are assigned 100 percent, and so are total liabilities plus owner's equity. All other items in each of the statements are expressed as a percentage of these numbers. It is the expression of the relationship or percentage of component items to a specific base item. Vertical analysis emphasizes the relationship of statement items within each accounting period. These relationships can be used with historical averages to determine statement anomalies.

The second financial statement analysis technique is horizontal analysis, also known as trend analysis. This technique is used to determine changes (i.e., increases or decreases) in a series of financial data over a period of time. The first period in the analysis is considered the base, and the changes in the subsequent period are computed as a percentage of the base period. If more than two periods are presented, each period's changes are computed as a percentage of the preceding period.

The third financial reporting analysis technique is ratio analysis. It is a means of measuring the relationship between two different financial statement amounts. The relationship and comparison are the keys to the analysis. Traditionally, financial

statement ratios are used in comparisons to an entity's industry average. They can be very useful in detecting red flags for a fraud examination.

12-8 (Learning objectives 12-3, 12-5, and 12-7) In the case study, "That Way Lies Madness," what kind of fraud did Eddie Antar commit? How was the fraud committed? How could the fraud be discovered?

Answer: Eddie Antar committed fictitious revenues, concealed liabilities and expenses, and improper asset valuation frauds. The schemes used by Crazy Eddie include the following:

- *Listing smuggled money from foreign banks as sales. Through these fictitious sales, he generated fictitious revenues. This fraud resulted in the increase of assets and yearly revenue.*
- *Making false entries to accounts payable.*
- *Overstating Crazy Eddie, Inc.'s inventory by breaking into and altering audit records.*
- *Taking credit for merchandise as "returned," while also counting it as inventory.*
- *"Sharing inventory" from one store to boost other stores' audit counts.*
- *Arranging for vendors to ship merchandise and defer the billing, besides claiming discounts and advertising credits.*
- *Selling large lots of merchandise to wholesalers, then spreading the money to individual stores as retail receipts.*

There were many clues: Stores were alarmingly understocked, shareholders were suing, and suppliers were shutting down credit lines because they were paid either late or not at all. An initial review showed that the company's inventory had been overstated by $65 million—a number later increased to over $80 million.

12-9 (Learning objective 12-10) During the audit of financial statements, an auditor discovers that the financial statements might be materially misstated due to the existence of fraud. Describe (1) the auditor's responsibility according to SAS No. 99 (AU 316) for discovering financial statement fraud; (2) what the auditor should do if he or she is precluded from applying necessary audit procedures to discover the suspected fraud; and (3) what the auditor should do if he or she finds that the fraud materially affects the integrity of the financial statements.

Answer: According to SAS No. 99 (AU 316),

1. *The auditor should (a) exercise professional skepticism in conducting the audit by discussing among the audit team members the risks of material misstatement due to*

fraud; (b) consider the implications for other aspects of the audit and discuss the matter with an appropriate level of management; and (c) obtain sufficient and competent evidential matter to determine whether material fraud exists and what its impact is on the fair presentation of financial statements.

2. *If the auditor is precluded from applying necessary audit procedures to find out about the existence of fraud, the auditor should (a) discuss the matter with the legal counsel; (b) disclaim or qualify an opinion on the financial statements; and (c) communicate audit findings to the audit committee or the board of directors.*
3. *If the auditor concludes that financial statements are materially affected by discovered frauds, the auditor should (a) require that financial statements be revised to correct the fraud; (b) issue a qualified or an adverse opinion if management refuses to revise the fraudulent financial statements; (c) consider withdrawing from the audit engagement and inform the audit committee, the board of directors, or the authorities about the fraud.*

Chapter 13

Review Questions

13-1 (Learning objective 13-1) What are four factors that influence the level of fraud risk faced by an organization?

Answer: Four factors that influence the level of fraud risk faced by an organization are (1) the nature of the business, (2) its operating environment, (3) the effectiveness of its internal controls, and (4) the ethics and values of the company and the people within it.

13-2 (Learning objective 13-2) What is the difference between preventive controls and detective controls?

Answer: Preventive controls are designed to stop an undesirable event from occurring, whereas detective controls are designed to identify an undesirable event that has already occurred.

13-3 (Learning objective 13-3) What is the objective of a fraud risk assessment?

Answer: The objective of a fraud risk assessment is to help management recognize the factors that make the organization most vulnerable to fraud so that management can address those factors to reduce the exposure.

13-4 (Learning objective 13-4) What can an effective fraud risk assessment help management to accomplish?

Answer: An effective fraud risk assessment can help management to accomplish the following: (1) improve communication and awareness throughout the organization about fraud; (2) identify what activities are the most vulnerable to fraud; (3) know who puts the organization at the greatest risk for fraud; (4) develop plans to mitigate fraud; (5) develop techniques to determine whether fraud has occurred in high-risk areas; (6) assess internal controls; and (6) comply with regulations and professional standards.

13-5 (Learning objective 13-5) What characteristics constitute a good fraud risk assessment?
Answer: The following are characteristics of a good fraud risk assessment: (1) it involves a collaborative effort of management and auditors; (2) it is sponsored by a competent and respected individual; (3) those leading and conducting the work are independent, objective, and open-minded; have a good working knowledge of the business; and engender the trust of management and employees; (4) it includes the perceptions of people at all levels of the organization; (5) it is kept alive and relevant.

13-6 (Learning objective 13-6) What are three considerations for developing an effective fraud risk assessment?
Answer: One consideration for developing an effective fraud risk assessment is presenting it in a manner to which people can relate. Another consideration is tailoring the approach and execution to the individual organization. Finally, the fraud risk assessment should be kept simple to ensure ease of execution.

13-7 (Learning objective 13-7) What can management do to prepare a company for a fraud risk assessment?
Answer: In order to prepare a company for a fraud risk assessment, management can build a fraud risk assessment team, consisting of individuals with diverse knowledge, skills, and perspectives, to lead and conduct the assessment. Also, management can determine the best techniques to use in performing the assessment and obtain the sponsor's agreement on the work to be performed. Finally, management can openly promote the fraud risk assessment process to encourage employee participation.

13-8 (Learning objective 13-8) What steps are involved in conducting a fraud risk assessment using the sample framework discussed in the chapter?
Answer: The steps involved in conducting a fraud risk assessment using the sample framework discussed in the chapter are as follows:
1. *Identify potential inherent fraud risks.*

2. *Assess the likelihood of occurrence of the identified fraud risks.*
3. *Assess the significance to the organization of the fraud risks.*
4. *Evaluate which people and departments are most likely to commit fraud and identify the methods they are likely to use.*
5. *Identify and map existing preventive and detective controls to the relevant fraud risks.*
6. *Evaluate whether the identified controls are operating effectively and efficiently.*
7. *Identify and evaluate residual fraud risks resulting from ineffective or nonexistent controls.*

13-9 (Learning objective 13-9) Describe four approaches for responding to an organization's residual fraud risks.

Answer: In responding to an organization's residual fraud risks, management can choose to avoid, transfer, mitigate, or assume each risk. Management may decide to avoid a risk by eliminating an asset or exiting an activity if the control measures required to protect the organization against an identified threat are too expensive. To transfer some or all of a risk, management may purchase fidelity insurance or a fidelity bond. Management can mitigate a risk by implementing appropriate countermeasures such as prevention and detection controls. If management determines that the probability of occurrence and impact of loss are low, management may choose to accept a risk. Finally, for certain risks, management may elect a combination of these approaches.

13-10 (Learning objective 13-10) What are four important considerations to keep in mind when reporting the fraud risk assessment results?

Answer: In reporting the fraud risk assessment results, the fraud risk assessment team should stick to the facts, focus on the most important points, identify actions that are clear and measurable, and present information in an easy-to-understand manner.

13-11 (Learning objective 13-11) What actions can management take to make the most impact with the fraud risk assessment?

Answer: In order to make the most impact with the fraud risk assessment, management can use the results in its ongoing anti-fraud efforts. By using the results to begin a dialog across the company that promotes awareness, education, and action planning, management can reduce fraud risk. Also, by using the results to identify high-risk areas, management can better focus its anti-fraud efforts. Management must ensure that the fraud risk assessment stays current and relevant, and that someone in the organization is assigned ownership of the process.

13-12 (Learning objective 13-12) How can a fraud risk assessment inform and influence the audit process?
Answer: The results of a fraud risk assessment can help auditors design programs and procedures in a way that enables the auditors to look for fraud in known areas of high risk.

Discussion Issues

13-1 (Learning objective 13-1) How is fraud risk influenced by a company's internal controls? How is fraud risk influenced by a company's ethics, values, and expectations?
Answer: A good system of internal controls, with the right balance of preventive and detective controls, can greatly reduce an organization's vulnerability to fraud by reducing the fraudster's opportunity to commit fraud and by increasing the likelihood of detection of a fraud that is committed. Any gap in alignment between a company's ethics, values, and expectations and those of the individuals that make up the organization can significantly increase an organization's fraud risk.

13-2 (Learning objective 13-6) Why is it important that management and auditors collaborate on a fraud risk assessment?
Answer: By collaborating on a fraud risk assessment, management and auditors can increase the effectiveness of the assessment. Each party brings a unique perspective to the assessment. Management has intricate familiarity with the day-to-day business operations, responsibility for assessing business risks and implementing organizational controls, authority to adjust operations, influence over the organization's culture and ethical atmosphere, and control over the organization's resources. Auditors are trained in risk identification and assessment, and have expertise in evaluating internal controls, which is critical to the fraud risk assessment process.

13-3 (Learning objective 13-6) What qualities and characteristics should be considered when choosing a sponsor for a fraud risk assessment?
Answer: A sponsor for a fraud risk assessment should be senior enough in the organization to command the respect of the employees and to elicit full cooperation in the process. The sponsor must be someone who is committed to learning the truth about where the company's fraud vulnerabilities are. In addition, he must be independent and open in his evaluation of the situation and response to the identified risks.

13-4 (Learning objective 13-6) Green is an internal auditor and the lead on the company's fraud risk assessment. In the past, he and Blue, an accounts receivable clerk, have had several heated disagreements over accounting procedures. What risk would Green be taking by having Blue perform the fraud risk assessment work related to the accounts receivable department's activities? How might this risk be best addressed?
Answer: Because Green and Blue have had some bad past experiences, by having Blue perform the work related to the accounts receivable department's activities, Green risks allowing those bad experiences to affect his evaluation of the fraud risks related to that area of the business. To preclude this possibility, someone else should perform the fraud risk assessment work related to the activities of the accounts receivable department.

13-5 (Learning objective 13-7) Who should be included on a fraud risk assessment team?
Answer: The fraud risk assessment team should consist of individuals with diverse knowledge, skills, and perspectives. The team members can include accounting and finance personnel who are familiar with the financial reporting process and internal controls; nonfinancial business unit and operations personnel who have knowledge of day-to-day operations, customer and vendor interactions, and industry issues; risk management personnel who can ensure that the fraud risk assessment process integrates with the organization's enterprise risk management program; the general counsel or other members of the legal department; members of any ethics and compliance functions within the organization; internal auditors; external consultants with fraud and risk experience; and any business leader with direct accountability for the effectiveness of the organization's fraud risk management efforts.

13-6 (Learning objective 13-8) What topics should be discussed in identifying fraud risks that could apply to the organization?
Answer: The following topics should be discussed in identifying fraud risks that could apply to the organization: incentives, pressures, and opportunities to commit fraud; and risk of management's override of controls. In addition, information should be gathered about the business itself, including its business processes, industry, and operating environment.

13-7 (Learning objective 13-8) What risks related to each of the three primary categories of fraud should the fraud risk assessment team consider?
Answer: Fraud risks can be classified according to the three major categories of fraud: fraudulent financial reporting, asset misappropriation, and corruption. The fraud risk assessment team should consider the following fraudulent financial reporting risks:

inappropriately reported revenues, expenses, or both; inappropriately reflected balance sheet amounts, including reserves; inappropriately improved or masked disclosures; concealed misappropriation of assets; concealed unauthorized receipts, expenditures, or both; and concealed unauthorized acquisition, use, or disposition of assets. The team should also consider asset misappropriation risks, including the risks of misappropriation of tangible and intangible assets, and proprietary business opportunities. Potential corruption risks that the team should consider include payment of bribes or gratuities to companies, private individuals, or public officials; receipt of bribes, kickbacks, or gratuities; and aiding and abetting of fraud by outside parties such as customers or vendors.

13-8 (Learning objective 13-8) What risks should the fraud risk assessment team consider in addition to the specific risks related to each of the three primary categories of fraud?

Answer: In addition to the specific risks related to each of the three primary categories of fraud, the fraud risk assessment team should consider risks related to regulatory and legal misconduct, reputation risk, and risk to information technology.

13-9 (Learning objective 13-9) When might an organization choose to avoid a risk rather than assume, transfer, or mitigate it?

Answer: Rather than assume, transfer, or mitigate a risk, management might choose to avoid it—by eliminating an asset or exiting an activity—if the control measures required to protect the organization against an identified threat are too expensive.

Chapter 14

Review Questions

14-1. (Learning objective 14-1) What are some of the reasons a fraud examination should be commenced?

Answer: A fraud examination may be undertaken to determine the source of and losses from an alleged fraud, and to gather evidence for a criminal prosecution or civil trial. Examinations may also be conducted to comply with federal statutes, to fulfill the professional duties of loyalty and reasonable care, to protect against allegations of wrongful termination, and to mitigate the company's liability related to employee misconduct.

14-2. (Learning objective 14-2) Who are some of the professionals that should be included on a typical fraud examination team?
Answer: Professionals from a variety of fields can provide valuable assistance to the examination. A typical investigation team might include Certified Fraud Examiners, legal counsel, internal auditors, security personnel, IT and computer forensics experts, human resources personnel, a management representative, and outside consultants.

14-3. (Learning objective 14-2) Under what circumstances might the fraud examination team include outside consultants?
Answer: In some cases, particularly when the suspect employee is especially powerful or popular, it might be useful to employ outside specialists who are relatively immune to company politics or threats of reprisal. Such experts might also have greater experience and investigative contacts than insiders. In addition, some investigatory procedures, such as forensic document analysis, require a high level of proficiency and expertise and should therefore only be undertaken by professionals specifically trained in that field.

14-4. (Learning objective 14-3) What is evidence? What types of things can be considered evidence?
Answer: Evidence is anything perceivable by the five senses, and includes any proof, such as testimony of witnesses, records, documents, facts, data, or tangible objects, that is legally presented at trial to prove a contention and induce a belief in the minds of a jury.

14-5. (Learning objective 14-4) What are some of examples of evidence gathering techniques that might be utilized in a fraud examination?
Answer: Fraud examinations frequently employ a wide variety of investigative techniques to gather evidence. Some of these include interviewing witnesses, examining public sources of information, conducting covert and surveillance operations, using informants, "dumpster diving," acquiring subpoenas and search warrants, and obtaining voluntary consent.

14-6. (Learning objective 14-5) When handling documentary evidence, what types of precautions should a fraud examiner take?
Answer: Original documents should be obtained where feasible. However, the originals should not be touched more than necessary, as they may later need to undergo forensic analysis. Therefore, the investigator should make working copies for review, and keep the

originals segregated. Additionally, a good filing system for the documents is essential. Losing a key document may irreparably damage the case.

So that it can be identified later, all documentary evidence received should be uniquely marked, either by initialing and dating the items or by making small tick marks or other nondescript identifiers on them. Other than these identifiers, the examiner should never write or make markings on the original documents. The investigator should also never add new folds to, staple, place paper clips on, crumple, or do anything else to documents that would affect or change them from their original condition. Finally, if fingerprint examinations are anticipated, gloves should be used to handle the documents.

14-7. (Learning objective 14- 7) What types of information can be obtained by examining internal documentation?

Answer: An investigator can learn a great deal about an individual by examining routine in-house information on file at his or her place of employment. Internal sources can provide the framework necessary for continued investigation from other sources. For example, personnel files can provide full names, addresses, social security numbers, dates of employment, previous employers, and salary information. Phone, voicemail, and email records can provide information about communication between parties. Access codes and user identification codes can identify when employees entered buildings and logged onto and off of computer systems. Security videos provide evidence of employee location and activity.

14-8. (Learning objective 14-8) What are three characteristics/objectives of a good investigation report?

Answer: The way in which the information is presented at the end of an investigation can often make or break the case. Therefore, a good investigation report should 1) convey all evidence necessary for thorough and proper evaluation of the case, 2) add credibility to the investigation and corroborate earlier facts, and 3) accomplish the objectives of case.

14-9. (Learning objective 14-8) What are five sections that should be included in a standard investigation report? What information is found in each of these sections?

Answer: A standard report should include the following sections:

- *Summary. This section sets out the main points of the report in a few sentences and should include the subject, basis, findings, and outcome of the investigation.*
- *Introduction/purpose. This section provides more detail on what the report is about and prepares the reader for what is to come, as well as explaining the*

purpose of the report along with any background information that may be required.

- *Body. This section identifies the employee(s) and other individuals implicated or involved in the matter and provides any background information that may have been obtained about the employee(s) or other parties. This section also details the methods used to investigate the matter.*
- *Results. This section will range from a sentence or two to a narrative supplemented by spreadsheets or graphics, depending on the nature of the investigation and the information collected.*
- *Follow-up/recommendations. This section identifies any investigation procedures that remain outstanding and outlines any recommendations related to procedures and controls.*

Discussion Issues

14-1. (Learning objective 14-2) Who should be responsible for directing an internal fraud investigation? Why?

Answer: Typically, the company's legal counsel should be involved in and, in most cases, charged with "directing" an internal investigation, at least as far as the legal aspects are concerned. Investigations can raise countless legal questions, and if certain legal precautions are not taken, the case can be severely damaged. The investigation team must have legal counsel on hand to sort out these issues; otherwise, the company risks exposing itself to greater danger than the threat it is investigating. In addition, by having an attorney directing the investigation, the company may be able to protect the confidentiality of its investigation under the attorney-client privilege.

14-2. Learning objectives (14-2, 14-6, and 14-7) How can computers and technology help in investigating a fraud? What kinds of challenges can the involvement of technology present to a case?

Answer: Just as computers are being used increasingly in the committal of fraud, investigators are making extensive use of technology in preventing, detecting, and investigating fraud. Because most frauds now involve the use of a computer in some capacity, IT professionals may need to be part of an investigation to safeguard data until it can be analyzed. Additionally, computer forensics professionals should be used to capture and analyze digital data. Electronic data can be easily altered; therefore, only trained professionals should be used to secure such data so that it can be analyzed more thoroughly without disturbing the original files.

The Internet has been an enormous tool in the fraud examiner's repertoire, as investigators now have a wealth of public records information at their fingertips. A number of resources and online search services are available to help investigators locate individuals, research financial information, identify business relationships and transactions, and uncover litigation history. Additionally, several software programs exist specifically to help investigators in organizing and managing evidence, and in reporting the results of their investigations.

14-3. (Learning objective 14-4) Jim Block, CFE, is investigating Randy Smith for his role in a potential kickback scheme. Gathering evidence about Randy's financial activity has been difficult. While on a stakeout at Randy's home, Jim sees Randy's wife take out the garbage and place it on the curb. Jim steals the trash bag, sorts through its contents, and discovers multiple bank statements that provide detail of some of Randy's illicit financial transactions. Is Jim's acquirement of the bank statements legal even though there was no search warrant?

Answer: Yes. Jim's use of "dumpster diving" to obtain evidence about Randy's financial dealings is legal. The courts have upheld that investigators may sift through trash without a search warrant, provided that the trash has left the suspect's possession. At that point, there is no longer the reasonable expectation of privacy, and thus it is fair game.

14-4. (Learning objective 14-6) What are some considerations a fraud examiner should keep in mind when organizing documentary evidence? Which method of evidence organization is preferred?

Answer: Keeping track of the amount of paper generated is one of the biggest problems in fraud investigations. Therefore, documents should be continuously reorganized and reevaluated as to importance and relevance to the case. Investigators should make a "key document" file for easy access to the most relevant documents and periodically review the key document file, moving the less important documents to back-up files and keeping only the most relevant paper in the main file.

A database of documents should be established early on in the case, and should include, at a minimum, the date of the document, the individual from whom the document was obtained, the date it was obtained, the subject to which the document pertains, and a brief description. Documents should be segregated and organized by either witness or transaction. Chronological organization is generally the least preferred method.

14-5. (Learning objective 14-7) An investigator is looking for information about some vacant land that may be owned by a suspect in a fraud case. What source(s) of public records would be a good place to find this information?
Answer: The investigator would find the information he is seeking in the public records of the county in which the land is located. The county should have on record a deed verifying the transfer of the property. Additionally, information about the land will be reflected in the county real property indexes. A search of the county real property records will reveal the residency and addresses of buyer and seller of the land, the purchase price of the property, and the title companies involved in the transaction. If the property was financed, the records will also list the mortgage company and amount originally financed.

The investigator should also search the county property tax records, which contain information about the estimated value of the property listed for tax purposes, the identity of the owner of the vacant piece of land, and the name of the last person to pay taxes on the property.

14-6. (Learning objective 14-8) When reporting the results of an investigation, why is it important that fraud examiners do not express opinions in their professional report?
Answer: The fraud examiner's job is to present the evidence in his report. Opinions regarding technical matters are permitted if the fraud examiner is qualified as an expert in the matter being considered. No opinions of any other kind should be included in the written report. In particular, opinions should not be voiced regarding the guilt or innocence of any person or party, as forming this type of opinion is the job of the judge and jury.

Chapter 15

Review Questions

15-1 (Learning objective 15-1) What are the five types of interview questions?
Answer: The five types of interview questions are introductory, informational, closing, assessment, and admission seeking.

15-2 (Learning objective 15-2) What four steps are involved in introductory questions?
Answer: The steps involved in the introduction are provide the introduction, establish rapport, establish the interview theme, and observe reactions.

15-3 (Learning objective 15-3) What topics should be covered during informational questioning?
Answer: Once the introductory questions are out of the way, the informational phase is used to gather the appropriate facts in a nonaccusatory way. Generally, the interviewer should begin with background questions, and then proceed logically to the facts that are - already known.

15-4 (Learning objective 15-4) When should open questions be used?
Answer: Open questions should be used during the informational phase of the interview.

15-5 (Learning objective 15-4) When should closed questions be used?
Answer: Closed questions should be used principally during the closing of the interview in order to sum up facts learned during the informational phase.

15-6 (Learning objective 15-4) When should leading questions be used?
Answer: Leading questions should generally be used during the admission-seeking phase of the interview.

15-7 (Learning objective 15-5) What are the purposes of closing questions?
Answer: Closing questions have three purposes: to reconfirm the facts gathered, to obtain additional information, and to conclude the interview.

15-8 (Learning objective 15-6) What is the purpose of assessment questions, and when are they asked?
Answer: The purpose of assessment questions is to establish the credibility of the respondent. They are asked only when the interviewer has a reason to doubt the truthfulness of the interviewee.

15-9 (Learning objective 15-7) What are some nonverbal clues to deception?
Answer: Nonverbal clues to deception include the following: full-body motions, changes in anatomical physical responses, changes in the rate of illustrators, placing the hands over the mouth, increased use of manipulators, fleeing positions, crossing the arms, inconsistent reactions to evidence, and fake smiles.

15-10 (Learning objective 15-8) What are some of the verbal clues to deception?

Answer: Verbal clues include to deception include the following: changes in speech patterns, repetition of the question, comments regarding the interview environment, displaying a selective memory, making excuses, increased use of oaths, excessive character testimony, answering with a question, overuse of respect, increasingly weaker denials, failure to deny wrongdoing, avoidance of emotive words, refusal to implicate other suspects, tolerant attitudes toward wrongdoing, reluctance to terminate the interview, and feigned unconcern about the issue at hand.

15-11 (Learning objective 15-9) What are the steps used in admission-seeking questions?
Answer: The following steps are used in admission-seeking questions: Make a direct accusation of wrongdoing, observe the subject's reaction, repeat the accusation, interrupt denials, establish a rationalization for the wrongful conduct, diffuse alibis, present an alternative question, obtain a benchmark admission, obtain a verbal confession, and reduce the confession to a written statement.

15-12 (Learning objective 15-10) What are the key elements of a signed statement?
Answer: The key elements of a signed statement are state that the accused knew the conduct was wrong; include facts known only to the accused; estimate the number of instances involved; establish a motive for the offense; state when the misconduct began and concluded; detail others involved; describe any physical evidence; explain how the proceeds were used, along with the location of any assets accumulated; and give specifics for each offense.

Discussion Issues

15-1 (Learning objective 15-1) Why are all five types of interview questions not used in all interviews?
Answer: Introductory, informational, and closing questions are used in all interviews. Most interviews are conducted with ordinary witnesses for the purpose of information gathering. Assessment and admission-seeking questions are used only in cases involving possible deception and for the purpose of confronting the suspect of a fraud.

15-2 (Learning objective 15-2) Why are introductory questions so important to an interview's success?
Answer: The introduction establishes the tone of the interview. If the witness feels comfortable, he or she is likely to provide information. If the witness feels threatened, this

will inhibit fact-finding. Additionally, only when the person is relaxed can you observe nonthreatening behavior and calibrate the witness.

15-3 (Learning objective 15-3) If during the informational phase of an interview, the witness becomes difficult, how should this be handled?
Answer: There are three specific techniques that can be used. The first is not to react to hostility. The second technique is to attempt to disarm the witness by surprise. The third is to change tactics.

15-4 (Learning objective 15-4) Why does the interviewer not use closed or leading questions during the information-gathering phase of the interview?
Answer: Closed or leading questions inhibit the flow of information from the witness. An open question does not restrict the subject's response. The interviewer's job is to allow the witness to convey as much information as necessary about the topic at hand.

15-5 (Learning objective 15-5) Why is establishing goodwill with the witness important during the closing phase of the interview?
Answer: In the case of most witnesses, you may have additional questions at some future point. By establishing and maintaining goodwill, the witness will be more likely to cooperate in any subsequent inquiry.

15-6 (Learning objective 15-6) What is the theory behind how assessment questions work?
Answer: The whole notion is that honest people will answer questions one way and dishonest people will answer them differently.

15-7 (Learning objectives 15-7 and 15-8) What is the connection between calibrating a witness and the verbal and nonverbal clues to deception?
Answer: In order to assess the verbal and nonverbal clues to deception, the interviewer must first observe the witness when the questioning is not threatening.

15-8 (Learning objective 15-9) Why are admission-seeking questions asked in a specific order?
Answer: The questions are designed to clear the innocent person and encourage those culpable to confess. People confess when they perceive that the benefits of confessing outweigh the disadvantages.

15-9 (Learning objective 15-10) Why is the excuse clause used in preparing a signed statement?
Answer: The confessor is usually more willing to sign a statement of responsibility if it includes information portraying him or her in a more favorable moral light.

Chapter 16

Review Questions

16-1 (Learning objective 16-1) What is "abusive conduct"?
Answer: Behaviors by employees of organizations that are counter to the entity's goals. Examples include "gold-bricking," excessive absenteeism, tardiness, theft, pilferage, and fraud.

16-2 (Learning objective 16-2) Why is attempting to achieve perfection in the workplace not desirable?
Answer: Standards regarding employee conduct should be reasonable. If they are not, employees may be forced to fail or lie in order to achieve unreasonable goals.

16-3 (Learning objective 16-3) Why is it difficult or impossible to measure the actual level of occupational fraud and abuse within organizations?
Answer: Not all occupational fraud is uncovered. For those frauds that are discovered, not all are reported. Furthermore, there is no organization or government agency that tracks comprehensive data for occupational fraud.

16-4 (Learning objective 16-4) Why is greed an inadequate explanation as the motive for occupational fraud?
Answer: Greed is a natural human trait. Many "greedy" people do not lie, cheat, and steal to achieve their goals.

16-5 (Learning objective 16-5) What is meant by "wages in kind"?
Answer: If employees feel underpaid or mistreated, they may be tempted to right their perceived wrongs through fraud and abuse.

16-6 (Learning objective 16-6) What is the difference between fraud prevention and fraud deterrence?

Answer: Fraud prevention implies removing the root causes of fraudulent behavior. Fraud deterrence is the modification of behavior through the threat of negative sanctions.

16-7 (Learning objective 16-7) What is the significance of the "perception of detection"?
Answer: Employees who believe that their fraudulent conduct will be detected are less likely to commit it.

16-8 (Learning objective 16-8) What are some of the factors that may help increase the perception of detection?
Answer: Factors that may help increase the perception of detection include: employee education, proactive fraud policies, a higher stance for management and auditors, increased use of analytical review, surprise audits, and adequate reporting programs.

16-9 (Learning objective 16-9) Why are adequate reporting programs so important to fraud deterrence?
Answer: Many employees who are aware of possible illegal conduct are fearful of being "dragged into" the investigation. An adequate reporting program provides anonymity to those who report fraudulent activity. This serves to encourage reporting and, therefore, increases the perception of detection.

16-10 (Learning objective 16-10) What are the key elements of the Corporate Sentencing Guidelines?
Answer: Corporations convicted of criminal offenses will be held liable for the illegal acts of their employees even if those in management had no knowledge of, or participation in, the acts. The liability can be limited if the company voluntarily discloses the illegal conduct and has taken specific steps to mitigate it.

16-11 (Learning objective 16-11) What is ethics?
Answer: Ethics is the branch of philosophy that focuses on the systematic study of reflective choice, of the standards of right and wrong by which a person is to be guided, and of the goods toward which it may ultimately be directed.

Discussion Issues

16-1 (Learning objective 16-1) Why do employees engage in abusive conduct against organizations?

Answer: The principal reason that employees engage in abusive conduct is to express dissatisfaction with their employer or terms of employment. This dissatisfaction leads to abusive conduct as a retaliatory measure.

16-2 (Learning objective 16-2) How are employees likely to react to unreasonably restrictive rules in the workplace?
Answer: The more rules that an organization sets, the greater the likelihood that employees will run afoul of them, especially if the rules make little or no sense to them. In that case, employees will usually ignore the rules or make their own.

16-3 (Learning objective 16-3) What are some of the ways an organization might improve measurement of the level of occupational fraud and abuse?
Answer: In order to measure the level of occupational fraud and abuse, the first step would entail detecting it. Methods for improving detection include instituting and enforcing internal control procedures and mechanisms for individuals to report, anonymously, instances related to fraud and abuse.

In addition, an organization should keep good records of the company history as it pertains to fraud-related matters. This may provide some insight into the company's risk of fraud as well as its areas of vulnerability.

16-4 (Learning objective 16-4) Since everyone is greedy to some extent, why do only some individuals engage in fraudulent activity?
Answer: Greed is only one factor in occupational fraud and abuse. Fraudulent activity, like any crime, depends on motive and opportunity. Although some individuals may have the motive, certain controls may be in place to diminish the opportunity. Alternately, if the opportunity is present, the motive may not exist.

16-5 (Learning objective 16-5) What actions might an organization take to prevent "wages in kind"?
Answer: Since wages in kind depends on the employees' perception that they are justified in committing fraud, the employer must confront this judgment from a moral and legal perspective. Additionally, educating employees as to the repercussions involved may reduce the likelihood of such occurrences.

Good personnel policies are also important in preventing this type of fraud. These policies should include (1) adequate personnel screening procedures, (2) antifraud training, and (3) equitable employee compensation.

16-6 (Learning objective 16-6) Why should fraud examiners seek to deter fraud rather than prevent it?

Answer: Since we are unable to control the societal factors that motivate the fraudster, we can attempt only to modify the behavior of these individuals. This may be accomplished by imposing the threat of detection and the negative repercussions associated therewith.

16-7 (Learning objectives 16-7 and 16-8) How do internal controls impact the "perception of detection"?

Answer: Internal controls, such as the segregation of duties, serve as a deterrent to fraud, because they increase the perception in the employee's mind that her fraudulent activity will be discovered. Controls that are not in place, but are perceived to be, can have the same deterrent effect.

However, internal controls alone are not sufficient to effectively fight fraud. Employee education, proactive fraud policies, increased use of analytical review, surprise audits, and adequate reporting programs should all be utilized to enhance the perception of detection.

16-8 (Learning objective 16-9) What is the most essential element of an adequate reporting program? Why?

Answer: According to most professionals, hotlines provide the best source of information for fraud detection. In fact, many of the schemes reported through hotlines probably would not have been discovered by any other method. In addition to providing anonymity for the employee reporting the fraud, hotlines assist organizations in complying with the federal Corporate Sentencing Guidelines and the Sarbanes–Oxley Act.

16-9 (Learning objective 16-10) What basic procedures should an organization follow in order to fulfill its due diligence responsibility as it relates to the Corporate Sentencing Guidelines?

Answer: Proactively, a corporation should establish and communicate policies, standards, and procedures regarding any criminal conduct by its employees in the course and scope of their employment. Furthermore, monitoring compliance and enforcement of those policies, standards, and procedures is also a necessary component. Criminal and civil sanctions against the organization may be reduced as a result of appropriate preventative measures taken.

16-10 (Learning objective 16-11) What is meant by "tone at the top"?

Answer: According to the Treadway Commission, tone at the top is a determining factor for the ethical environment of an organization. It indicates that employees take their cues from the leadership of an enterprise. Tone at the top reflects more than just a formal ethics policy; it involves leading by example.