EXHIBIT 5-1
CHAPTER 5

CHECK TAMPERING

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

5-1 Define check tampering.
5-2 Understand the five principal categories of check tampering.
5-3 Detail the means by which employees fraudulently obtain company checks.
5-4 Understand how forged signatures are created on blank check stock.
5-5 Be familiar with the methods identified in this chapter for preventing and detecting forged maker schemes.
5-6 Differentiate between forged maker and forged endorsement schemes.
5-7 Detail the methods employees use to intercept outgoing checks before they are delivered to the intended payee.
5-8 Be able to discuss methods that can be used to prevent and detect the theft and/or alteration of outgoing company checks.
5-9 Understand how authorized maker schemes work and why they are especially difficult to prevent.
5-10 Understand how check tampering is hidden in a company’s accounting records.
5-11 Be familiar with proactive audit tests that can be used to detect check tampering.

CASE STUDY: A WOLF IN SHEEP’S CLOTHING

Melissa Robinson was a devoted wife with two adorable children. She was very active at her children’s school and had been known as a charitable person, giving both her time and money to various organizations throughout the community. She spent a good portion of her time working for a worldwide charitable organization chapter in Nashville as the executive secretary. In fact, her fellow employees and club members perceived Robinson’s donation of time and hard work as nothing less than a godsend. “Even if somebody had told [the board of directors] that this lady was stealing,” recalls certified fraud examiner and CPA David Mensel, who is also a member of the organization, “they would have said ‘Impossible, she’d never do it.’”

However, all these accolades could not obscure one cold fact: Melissa Robinson was a thief. Unfortunately, as executive secretary, she was one of two people in the organization allowed to sign checks on its bank accounts. As a result, the club was bilked out of more than $60,000 over five years, until club members put an end to Robinson’s scam.

The Nashville chapter of the organization was very much like other charitable entities—they would engage in fundraising activities, such as selling peanuts or candy bars on street corners around the holiday seasons. Although a percentage came in check form, most of the fundraising revenue was naturally cash.

“There was no oversight in those currency collections,” says Mensel. “If I had gone out on a collecting route, I’d come back with a bag of money and drop it on the secretary’s desk and be gone.”

Several names have been changed to preserve anonymity.
Mensel suspects that Robinson stole far more than the $60,800 that the audit team ultimately established, because the amount of currency that flowed through her office was undocumented. “It is just a supposition, given her behavior with the checking accounts,” Mensel explains. “As well, we saw a basic decline in collections from some activities that the organization had been involved in for many years.”

Robinson’s fraudulent activities were made possible by the relaxed operations of the Nashville chapter’s board of directors. The organization’s charter mandated that an independent audit be performed annually. However, during Robinson’s tenure as executive secretary, not one yearly audit was completed. Mensel describes the board of directors during that tenure as “lackadaisical.”

Robinson arrived at the executive secretary’s desk through hard work. Starting in 1985, she was one of the most dedicated employees the company had, giving as much time as she could to help out. Once she earned the executive secretary position, Robinson apparently began pilfering from the organization’s three bank accounts a little at a time. Although the accounts required two signatures per check, Robinson was able to write checks to herself and others by signing her own name and forging the second signature. Mensel says she would usually write a check to herself or to cash and record the transaction in the organization’s books as a check to a nonexistent name, as the depositor of the check. “But of course, on the back of the check was her own signature.”

The club meetings were regularly held in a hotel in town or at one of the executive meetings clubs,” Mensel recalls, “and those bills would run from two to four thousand dollars a month. The executive secretary would . . . post in the checkbook that she had paid the hotel, but the actual check would be made out to someone else.”

Mensel also remembers that Robinson repeatedly refused to convert her manual checking system into the elaborate computer system the organization wanted her to use. “Now we know why,” says Mensel.

Mensel and another associate were very involved in a fundraising operation when Robinson began her reign as executive secretary. Mensel observed that whenever he asked for any financial information from Robinson, she would stonewall him or make excuses. Mensel became suspicious and took the matter up with the board of directors. But when he told the board that he thought it was very peculiar that he couldn’t get much financial data from Robinson, the board quite definitely sided with the executive secretary.

“The officers of the board essentially jumped down my throat, told me I was wrong and that I was being unreasonable,” Mensel says. “And since I had no substantiation, just a bad feeling . . . I let it pass.”

Mensel felt that the current treasurer was personally offended by his inquiry, as though he were suggesting that the treasurer was not doing his job properly. The treasurer acted defensively and did not check into Robinson’s dealings. As a result, the organization, which Mensel describes as previously “financially very sound,” began to feel some financial strain. There simply wasn’t as much money to run the organization as in the past, and it was at this point Robinson made what was perhaps her most ingenious maneuver. She convinced the board of directors that because the organization was experiencing some economic troubles, they ought to close the office space rented out for the executive secretary. This office was considered the financial center of the organization. Supposedly out of the goodness of her heart, Robinson told the board members that she would be happy to relinquish her precious space and run the financial matters of the club from her home. The board members agreed.

This allowed Robinson to carry out her embezzlement in small doses; Mensel recalls that Robinson wrote several checks for only $200 to $300. All this time, the board did nothing to impede Robinson’s progress, even when she would not divulge financial information on request. When she came to club meetings, board members would sometimes ask her for information about the finances or ask to look at her books. Robinson would apologize and explain that she had forgotten them.

However, during the last year of the embezzlement, a new group of officers was elected, including a new treasurer. The first thing the treasurer did was ask Robinson for the books. Robinson repeatedly denied his requests, until the new chapter president went to Robinson’s house and demanded them. “[The president] stood on her doorstep until she gave the books to him. He said he wouldn’t leave until she gave them to him.” Mensel recalls. “Once [the board] got their hands on the books . . . they could see that something was very definitely wrong.”

In comparing the books with many of the returned checks, the organization could immediately see that not only had some checks been altered or forged, but also many of the checks were simply missing. At that point, the board of directors assigned Mensel and two other club members, one a CPA, to investigate Robinson’s alleged wrongdoings. As Mensel and the other audit committee members looked at the checks, they realized that Robinson hardly attempted to cover up her scams at all.

“She did physically erase some checks and sometimes even used White-Out to rewrite the name of the payee that was in the checkbook after the check had cleared,” Mensel laughs. “But of course, on the back of the check was her name, as the depositor of the check.”

The peculiar thing, in Mensel’s mind, was the varying nature of Robinson’s check writing. Although Mensel says several of the checks were written to casinos such as the Trump Taj Mahal and weekend getaway spots like the Mountain View Chalet, many more of the checks were written to other charities and the school Robinson’s children attended. She apparently didn’t use the embezzled money to substantially improve her lifestyle, which Mensel describes as “a
very standard middle-class life here in Nashville. She and her husband were not wealthy people by any means.”

Robinson was immediately excused from her executive secretary position. She was indicted by a grand jury and was tried and found guilty. She was ordered to pay restitution to the club and its insurance company. At last notice, she was still paying back the money. The court will “wipe her slate clean” when she completes her restitution.

Robinson appeared to be one of the most dedicated volunteers in a charitable organization, giving of her time and efforts. The workers around her praised her generosity and work ethic yet all the while she was stealing from them. If there is a lesson to be learned here, it is that audit functions are in place for a reason and should never be overlooked. Unfortunately for the charitable organization, they were reminded of this lesson the hard way.

OVERVIEW

The story of Melissa Robinson is an example of one of the most common forms of fraudulent disbursement, the check tampering scheme. Check tampering occurs when an employee converts an organization’s funds by either (1) fraudulently preparing a check drawn on the organization’s account for his own benefit, or (2) intercepting a check drawn on the organization’s account that is intended for a third party and converting that check to his own benef- it. Remember, check tampering is a form of fraudulent disbursement and applies only to checks drawn on the victim organization’s bank accounts. If the perpetrator steals an incoming check from a customer that is payable to the victim organization, then this theft will be classified as skimming or cash larceny, depending on whether the check was recorded before it was stolen.

Check Tampering Data from the ACFE 2006 National Fraud Survey

Check tampering, as we have stated, is a form of fraudulent disbursement in which the perpetrator converts an organization’s funds by forging or altering a check drawn on one of the organization’s bank accounts, or steals a check the organization has legitimately issued to another payee. Among fraudulent disbursement cases in the 2006 study, 26 percent involved check tampering. (See Exhibit 5-2.) This ranked check tampering as the

EXHIBIT 5-2  2006 National Fraud Survey: Frequency of Fraudulent Disbursements

*The sum of these percentages exceeds 100 percent because some cases involved multiple fraud schemes that fell into more than one category.
third most common form of fraudulent disbursement in both studies, behind billing and expense reimbursement schemes.

As shown in Exhibit 5-3, the median loss due to check tampering schemes in the 2006 survey was $120,000, making it the second most expensive of the fraudulent disbursement schemes, on average.

CHECK TAMPERING SCHEMES

Check tampering is unique among fraudulent disbursements because it is the one group of schemes in which the perpetrator physically prepares the fraudulent check. In most fraudulent disbursement schemes, the culprit generates a payment to himself by submitting some false document to the victim company such as an invoice or a timecard. The false document represents a claim for payment and causes the victim company to issue a check that the perpetrator then converts. These frauds essentially amount to trickery; the perpetrator fools the company into handing over its money.

Check tampering schemes are fundamentally different. In these frauds the perpetrator takes physical control of a check and makes it payable to himself through one of several methods. Check tampering schemes depend on factors such as access to the company checkbook, access to bank statements, and the ability to forge signatures or alter other information on the face of the check. There are five principal methods used to commit check tampering:

1. Forged maker schemes
2. Forged endorsement schemes
3. Altered payee schemes
4. Concealed check schemes
5. Authorized maker schemes

Forged Maker Schemes

The legal definition of forgery includes not only the signing of another person’s name to a document (such as a check) with a fraudulent intent, but also the fraudulent alteration of a genuine instrument. This definition is so broad that it would encompass all check tampering schemes, so we have narrowed the term to fit our needs. Because we are
interested in distinguishing the various methods used by individuals to tamper with checks, we will constrain the concept of “forgeries” to those cases in which an individual signs another person’s name on a check.

The person who signs a check is known as the “maker” of the check. A forged maker scheme, then, may be defined as a check tampering scheme in which an employee misappropriates a check and fraudulently affixes the signature of an authorized maker thereon (see Exhibit 5-4). Frauds that involve other types of check tampering, such as the alteration of the payee or the changing of the dollar amount, are classified separately.

As one might expect, forged check schemes are usually committed by employees who lack signature authority on company accounts. Melissa Robinson’s case is something of an exception because, although she did have signature authority, her organization’s checks required two signatures. Robinson therefore had to forge another person’s signature.

In order to forge a check, an employee must have access to a blank check, he must be able to produce a convincing forgery of an authorized signature, and he must be able to conceal his crime. If the fraudster cannot hide his crime from his employer, his scheme is sure to be shortlived. Concealment is a universal problem in check tampering schemes; the methods used are basically the same for all categories of check tampering. Therefore, concealment issues will be discussed as a group at the end of the chapter.

Obtaining the Check

Employees with Access to Company Checks One cannot forge a company check unless one first possesses a company check. The first hurdle that a fraudster must overcome in committing a forgery scheme is to figure out how to get his hands on a blank check. Most forgery schemes are committed by accounts payable clerks, office managers, bookkeepers, or other employees whose duties typically include the preparation of company checks. Like Melissa Robinson, these are people who have access to a company’s check stock on a regular basis and are therefore in the best position to steal blank checks. If an employee spends his workday preparing checks on behalf of his company, and if that employee has some personal financial difficulty, it takes only a small leap in logic (and a big leap in ethics) to see that his financial troubles can be solved by writing fraudulent checks for his own benefit. Time and again we see that employees tailor their fraud to the circumstances of their jobs. It stands to reason that those who work around the checkbook would be prone to committing forgery schemes.

Employees Lacking Access to Company Checks If the perpetrator does not have access to the check stock through her work duties, she will have to find other means of misappropriating a check. The way a person steals a check depends largely on how blank checks are handled within a particular company. In some circumstances checks are poorly guarded, left in unattended areas where anyone can get to them. In other companies the checkbook may be kept in a restricted area, but the perpetrator may have obtained a key or combination to this area, or may know where an employee with access to the checks keeps his own copy of the key or combination. An accomplice may provide blank checks for the fraudster in return for a portion of the stolen funds. Perhaps a secretary sees the checkbook left on a manager’s desk or a custodian comes across blank checks in an unlocked desk drawer.

In some companies, checks are computer generated. When this is the case an employee who knows the password that allows checks to be prepared and issued may be able to obtain as many unsigned checks as he desires. There are an unlimited number of
CHAPTER 5 CHECK TAMPERING

EXHIBIT 5-4 Forged Maker Schemes
ways to steal a check, each dependent on the way in which a particular company guards its blank checks.

A fraudster may also be able to obtain a blank check when the company fails to properly dispose of unused checks. In Case 669, for example, a company used voided checks to line up the printer that ran payroll checks. These voided checks were not mutilated. A payroll clerk collected the voided checks after the printer was aligned and used them to issue herself extra disbursements through the payroll account.

**Producing Counterfeit Checks** In more sophisticated forgery schemes, the perpetrator may produce counterfeit check stock with the organization’s bank account number on the counterfeit checks. These counterfeit checks can be practically indistinguishable from the company’s legitimate stock. In Case 1460, for example, the perpetrator had an accomplice who worked for a professional check-printing company and who printed blank checks for the bank account of the perpetrator’s employer. The perpetrator then wrote over $100,000 worth of forgeries on these counterfeit checks.

**Safeguarding the Organization’s Check Stock** Organizations should take steps to safeguard their check stock and proactively seek out stolen and forged checks. These goals can be achieved through a number of relatively simple prevention and detection techniques that may avert a very large fraud scheme.

Obviously, blank checks should be maintained under lock and key and access should be severely limited to those whose duties include check preparation. (If checks are computer generated, access to the code or password that allows issuance of checks should likewise be restricted.) Boxes of blank checks should be sealed with security tape to make it obvious when a new box has been opened, and on a periodic basis, someone independent of the check preparation function should verify the security of unused checks. Organizations should also promptly destroy any voided checks. These checks, if carelessly discarded, may be stolen and forged by employees.

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.

There are certain indicators that organizations can look for to help spot stolen or forged checks. Obviously, as stated above, if checks are noticed missing or if there are signs of tampering with unused check stock, this is a clear indicator of theft. In addition, out-of-sequence checks or duplicate check numbers that show up on an organization’s bank statement may signal theft. When employees steal blank checks, they will often take them from the bottom of the box with the hope that the missing check will not be noticed for some time. When these checks are converted, they should be noted as out-of-sequence on the bank statement. Employees who reconcile the statement should be trained to look for this red flag. Similarly, counterfeit checks often have numbers either that are completely out of sequence or that duplicate numbers of checks that were already issued.

Employees who steal blank checks often do so after hours because there are fewer people around to witness the theft. As a matter of practice, at the start of each business day, organizations should reconcile the first check in the checkbook to the last check written on the previous day. If there is a gap, it should be promptly investigated.
CHAPTER 5 CHECK TAMPERING

To Whom Is the Check Made Payable?

Payable to the Perpetrator Once a blank check has been obtained, the fraudster must decide to whom it should be made payable. He can write the check to anyone, though in most instances forged checks are payable to the perpetrator himself so that they are easier to convert. A check made payable to a third person, or to a fictitious person or business, may be difficult to convert without false identification. The tendency to make forged checks payable to oneself seems to be a result of fraudsters’ laziness rather than a decision based on the successful operation of their schemes. Checks payable to an employee are obviously more likely to be recognized as fraudulent than checks made out to other persons or entities.

If the fraudster owns his own business or has established a shell company, he will usually write fraudulent checks to these entities rather than himself. When the payee on a forged check is a “vendor” rather than an employee of the victim company, the checks are not as obviously fraudulent on their faces. At the same time, these checks are easy to convert because the fraudster owns the entity to which the checks are payable.

Payable to an Accomplice If a fraudster is working with an accomplice, she can make the forged check payable to that person. The accomplice then cashes the check and splits the money with the employee-fraudster. Because the check is payable to the accomplice in her true identity, it is easily converted. An additional benefit to using an accomplice is that a canceled check payable to a third-party accomplice is not as likely to raise suspicion as a canceled check to an employee. The obvious drawback to using an accomplice in a scheme is that the employee-fraudster usually has to share the proceeds of the scheme.

In some circumstances, however, the accomplice may be unaware that she is involved in a fraud. An example of how this can occur was found in Case 729, in which a bookkeeper wrote several fraudulent checks on company accounts, then convinced a friend to allow her to deposit the checks in the friend’s account. The fraudster claimed the money was revenue from a side business she owned and the subterfuge was necessary to prevent creditors from seizing the funds. After the checks were deposited, the friend withdrew the money and gave it to the fraudster.

Payable to “Cash” The fraudster may also write checks payable to “cash” in order to avoid listing himself as the payee. Checks made payable to cash, however, must still be endorsed. The fraudster will have to sign his own name or forge the name of another in order to convert the check. In addition, checks payable to “cash” are usually viewed more skeptically than checks payable to persons or businesses.

Payable to a Vendor The employee who forges company checks may do so not to obtain currency, but to purchase goods or services for his own benefit. When this is the case, forged checks are made payable to third-party vendors who are uninvolved in the fraud. For instance, we saw in the case study at the beginning of this chapter how several of Melissa Robinson’s checks were written to casinos and hotels, apparently for personal vacations.

Forging the Signature After the employee has obtained and prepared a blank check, he must forge an authorized signature in order to convert the check. The most obvious method, and the one that comes to mind when we think of the word forgery, is to simply take pen in hand and sign the name of an authorized maker.
Free-Hand Forgery  The difficulty a fraudster encounters when physically signing the authorized maker’s name is in creating a reasonable approximation of the true signature. If the forgery appears authentic, the perpetrator will probably have no problem cashing the check. In truth, the forged signature may not have to be particularly accurate. Many organizations do not verify the signatures on cancelled checks when they reconcile their bank statements, so even a poorly forged signature may go unnoticed.

Photocopied Forgeries  To guarantee an accurate forgery, some employees make photocopies of legitimate signatures and affix them to company checks. The fraudster is thus assured that the signature appears authentic. This method was used by a bookkeeper in Case 2514 to steal over $100,000 from her employer. Using her boss’s business correspondence and the company Xerox machine, she made transparencies of his signature. These transparencies were then placed in the copy machine so that when she ran checks through the machine the boss’s signature was copied onto the maker line of the check. The bookkeeper now had a signed check in hand. She made the fraudulent checks payable to herself, but falsified the check register so that the checks appeared to have been written to legitimate payees.

Automatic Check-Signing Instruments  Companies that issue a large number of checks sometimes utilize automatic check-signing instruments in lieu of signing each check by hand. Automated signatures are either produced with manual instruments like signature stamps or they are printed by computer. Obviously, a fraudster who gains access to an automatic check-signing instrument will have no trouble forging the signatures of authorized makers. Even the most rudimentary control procedures should severely limit access to these instruments. Nevertheless, several of the forged maker schemes the ACFE reviewed were accomplished through use of a signature stamp. In Case 838, for instance, a fiscal officer maintained a set of manual checks that were unknown to other persons in the company. The company used an automated check signer and the custodian of the signer let the officer have uncontrolled access to it. Using the manual checks and the company’s check signer, the fiscal officer was able to write over $90,000 worth of fraudulent checks to himself over a period of approximately four years.

The same principle applies to computer-generated signatures. Access to the password or program that prints signed checks should be restricted, specifically excluding those who prepare checks and those who reconcile the bank statement. The fraudster in Case 2342, for example, was in charge of preparing checks. The fraudster managed to obtain the issuance password from her boss, then used this password to issue checks to a company she owned on the side. She was able to bilk her employer out of approximately $100,000 using this method.

The beauty of automated check signers, from the fraudster’s perspective, is that they produce perfect forgeries. Nothing about the physical appearance of the check will indicate that it is fraudulent. Of course, forged checks are written for illegitimate purposes, so they may be detectable when the bank statement is reconciled or when accounts are reviewed. The ways in which fraudsters avoid detection through these measures will be discussed later in this chapter.

Preventing and Detecting Forged Maker Schemes  Obviously, a key to preventing forgeries is to maintain a strict set of procedures for the handling of outgoing checks, which includes safeguarding blank check stock, establishing rules for custody of checks that have been prepared but not signed, and separating the duties of check preparation and check signing. Organizations should establish a restrictive list of authorized check
signers and see to it that checks that have been prepared are safeguarded until they are presented to these signatories.

To the extent possible, organizations should rotate authorized check signers and keep track of who is approved to sign checks during a given period. Rotating this duty can help prevent abuse by an authorized signatory, but also if a canceled check shows a signature from the wrong signer for the date of the disbursement, this could indicate fraud. Also, on a periodic basis an organization should have authorized check signers verify their signatures on returned checks or another employee should be required to spot-check signatures against an established signature file.

In organizations that use a signature stamp, access to the stamp should be strictly limited and a custodian should maintain a log of who uses the signature stamp, and at what time. If it is suspected that someone is misusing the signature stamp, temporarily suspend use of the stamp and instruct the bank to honor only checks with original signatures.

Miscoding Fraudulent Checks

Miscoding a check is actually a form of concealment, a means of hiding the fraudulent nature of the check. We will discuss the ways fraudsters code their forged checks in the concealment section at the end of this chapter. It should be noted here, however, that miscoding is typically used as a concealment method only by those employees with access to the checkbook. If a forged maker scheme is undertaken by an employee without access to the checkbook, she usually makes no entry whatsoever in the disbursements journal.

Converting the Check

In order to convert the forged check, the perpetrator must endorse it. The endorsement is typically made in the name of the payee on the check. Since identification is generally required when one seeks to convert a check, the fraudster usually needs fake identification if he forges checks to real or fictitious third persons. As discussed earlier, checks payable to “cash” require the endorsement of the person converting them. Without fake ID, the fraudster will likely have to endorse these checks in his own name. Obviously an employee’s endorsement on a canceled check is a red flag.

Forged Endorsement Schemes

Forged endorsement frauds are those check tampering schemes in which an employee intercepts a company check intended for a third party and converts the check by signing the third party’s name on the endorsement line of the check (see Exhibit 5-5). In some instances the fraudster also signs his own name as a second endorser. The term forged endorsement schemes would seem to imply that these frauds should be categorized along with the forged maker schemes discussed in the previous section. It is true that both kinds of fraud involve the false signing of another person’s name on a check, but there are certain distinctions that cause forged endorsement schemes to be categorized here rather than with the other forgeries.

In classifying fraud types, we look to the heart of the scheme. What is the crucial point in the commission of the crime? In a forged maker scheme, the perpetrator is normally working with a blank check. The trick to this kind of scheme is in gaining access to blank checks and producing a signature that appears authentic.

In a forged endorsement scheme, on the other hand, the perpetrator is tampering with a check that has already been written, so the issues involved in the fraud are different. The key to these schemes is obtaining the checks after they are signed but before they
EXHIBIT 5-5  Forged Endorsement Schemes

are properly delivered. If this is accomplished, the actual forging of the endorsement is somewhat secondary.

A fraudster’s main dilemma in a forged endorsement case is gaining access to a check after it has been written and signed. The fraudster must either steal the check between the point where it is signed and the point where it is delivered, or he must reroute the check, causing it to be mailed to a location where he can retrieve it. The manner used to steal a check depends largely on the way the company handles outgoing disbursements. Anyone who is allowed to handle signed checks may be in a good position to intercept them.
Intercepting Checks before Delivery

Employees Involved in Delivery of Checks  Obviously, the employees in the best position to intercept signed checks are those whose duties include the handling and delivery of signed checks. The most obvious example would be a mailroom employee who opens outgoing mail containing signed checks and steals the checks. Other personnel with access to outgoing checks might include accounts payable employees, payroll clerks, secretaries, and so forth.

Poor Control of Signed Checks  Unfortunately, fraudsters are often able to intercept signed checks because of poor internal controls. For instance, in Case 1000, signed checks were left overnight on the desks of some employees because processing on the checks was not complete. One of the janitors on the overnight cleaning crew found these checks and took them, forged the endorsements of the payees, and cashed them at a liquor store. Another example of poor observance of internal controls appeared in Case 933. In this scheme a high-level manager with authority to disburse employee benefits instructed accounts payable personnel to return signed benefits checks to him instead of immediately delivering them to their intended recipients. These instructions were not questioned despite the fact that they presented a clear violation of the separation-of-duties concept due to the manager’s level of authority within the company. The perpetrator simply took the checks that were returned to him and deposited them into his personal bank account, forging the endorsements of the intended payees.

Case 933 represents what seems to be the most common breakdown of controls in forged endorsement frauds. We have seen repeated occurrences of signed checks being returned to the employee who prepared the check. This typically occurs when a supervisor signs a check and hands it back to the clerk or secretary who presented it to the supervisor; it is done either through negligence or because the employee is highly trusted and thought to be above theft. Adequate internal controls should prevent the person who prepares company disbursements from having access to signed checks. This separation of duties is elemental; its purpose is to break the disbursement chain so that no one person controls the entire payment process.

Theft of Returned Checks  Another way to obtain signed checks is to steal checks that have been mailed, but have been returned to the victim company for some reason such as an incorrect address. Employees with access to incoming mail may be able to intercept these returned checks from the mail and convert them by forging the endorsement of the intended payee. In Case 2288, for example, a manager took and converted approximately $130,000 worth of checks that were returned due to noncurrent addresses. (He also stole outgoing checks, cashed them, and then declared them lost.) The fraudster was well known at his bank and was able to convert the checks by claiming that he was doing it as a favor to the real payees, who were “too busy to come to the bank.” The fraudster was able to continue with his scheme because the nature of his company’s business was such that the recipients of the misdelivered checks were often not aware that the victim company owed them money. Therefore, they did not complain when their checks failed to arrive. In addition, the perpetrator had complete control over the bank reconciliation, so he could issue new checks to those payees who did complain, then “force” the reconciliation, making it appear that the bank balance and book balance matched when in fact they did not. Stealing returned checks is obviously not as common as other methods for intercepting checks, and it is more difficult for a fraudster to plan
and carry out on a long-term basis. However, it is also very difficult to detect and can lead to large-scale fraud, as the previous case illustrates.

Rerouting the Delivery of Checks The other way an employee can go about misappropriating a signed check is to alter the address to which the check is to be mailed. The check either is delivered to a place where the fraudster can retrieve it, or is purposely misaddressed so that he can steal it when it is returned as discussed above. As we have said before, proper separation of duties should preclude anyone who prepares disbursements from being involved in their delivery. Nevertheless, this control is often overlooked, allowing the person who prepares a check to address and mail it as well.

In some instances where proper controls are in place, fraudsters are still able to cause the misdelivery of checks. In Case 1470, for instance, the fraudster was a clerk in the customer service department of a mortgage company where her duties included changing the mailing addresses of property owners. She was assigned a password that gave her access to make address changes. The clerk was transferred to a new department where one of her duties was the issuance of checks to property owners. Unfortunately, her supervisor forgot to cancel her old password. When the clerk realized this oversight, she would request a check for a certain property owner, then sign onto the system with her old password and change the address of that property owner. The check would be sent to her. The next day the employee would use her old password to reenter the system and replace the proper address so that there would be no record of where the check had been sent. This fraudster’s scheme resulted in a loss of over $250,000 to the victim company.

Converting the Stolen Check Once the check has been intercepted, the perpetrator can cash it by forging the payee’s signature, hence the term forged endorsement scheme. Depending on where he tries to cash the check, the perpetrator may or may not need fake identification at this stage. As we alluded to earlier, many fraudsters cash their stolen checks at places where they are not required to show an ID.

If a fraudster is required to show identification in order to cash his stolen check, and if he does not have a fake ID in the payee’s name, he may use a dual endorsement to cash or deposit the check. In other words, the fraudster forges the payee’s signature as though the payee had transferred the check to him, then the fraudster endorses the check in his own name and converts it. When the bank statement is reconciled, double endorsements on checks should always raise suspicions, particularly when the second signer is an employee of the company.

Preventing and Detecting the Theft of Outgoing Company Checks It is very important that the functions of cutting checks, signing checks, and delivering checks be separated. If a check preparer is also allowed to have custody of signed checks, it is easy to commit check tampering. The individual can draft a check for a fraudulent purpose, wait for it to be signed, and simply pocket it. However, if the individual knows he or she will not see the check again after it has been signed, then that person is less likely to attempt this kind of scheme because of the diminished perceived opportunity for success.

In addition to establishing controls designed to prevent the theft of outgoing checks, organizations should train their employees to look for this kind of scheme and should establish routine procedures designed to help detect it if and when it does occur. These proactive detection techniques are generally not very complicated and do not require sophisticated procedures or investigative methods; all that is required is that an organization devote a minimal amount of time to routinely checking for thefts.
If an employee steals a check payable to a vendor and does not issue a replacement, the vendor will almost certainly complain about the nonpayment. This is the point at which most forged endorsement schemes should be detected. Every organization should have a structure in place to handle both vendor and customer complaints. All complaints should be investigated by someone independent of the payables function so that the fraudster will not be able to cover her own tracks. When a complaint regarding nonpayment is received, it should be a relatively simple matter to track the missing check and identify when it was converted, and by whom. As a proactive measure, it may be advisable—particularly in organizations where check theft has been a problem—to have independent personnel randomly contact vendors to confirm receipt of payments.

As was previously discussed, some employees who steal outgoing checks will cause a replacement check to be issued so that the vendor will not complain. In order to detect these schemes, an organization’s accounting system should be set up to detect duplicate payments. Paid vouchers should immediately be stamped “paid” and computerized systems should automatically flag duplicate invoice numbers. In addition, payables reports sorted by payee and amount should be periodically generated in order to detect duplicates when invoice numbers have been altered for the second check.

Instead of stealing checks on the company premises, some employees will cause them to be misdelivered by changing the mailing address of the intended recipient in the organization’s payables system. For this reason, authority to make changes to vendor records should be restricted, and the organization’s accounting system should automatically track who makes changes to vendor records. This will make it easier to identify the perpetrator if an outgoing check is stolen. Periodically, a report listing all changes to vendor addresses, payment amounts, payees, and so on can be generated to determine if there have been an inordinate amount of changes, especially where a vendor’s address is temporarily changed when a check is issued, then restored after the check has been mailed.

To convert an intercepted check, the perpetrator may have to use a dual endorsement. Any canceled checks with more than one endorsement should be investigated, as should any nonpayroll check that an employee has endorsed. The employee or employees who reconcile the bank statement should be required to review the backs of canceled checks for suspicious endorsements as a matter of course.

Another procedure that all organizations should have in place is to chart the date of mailing for every outgoing check. In the event that a signed check is stolen, the date of mailing can be compared to work records of mailroom personnel and other employees who have contact with outgoing checks to determine a list of possible suspects.

Finally, organizations should consider installing surveillance cameras in their mailrooms. Mailroom personnel are in a good position to steal outgoing checks, and also to skim incoming revenues or merchandise shipments. If a theft is discovered, security camera tapes may help identify the wrongdoer. More importantly, the presence of surveillance cameras can help deter employees from stealing.

Altered Payee Schemes

The second type of intercepted check scheme is the altered payee scheme. This is a type of check tampering fraud in which an employee intercepts a company check intended for a third party and alters the payee designation so that the check can be converted by the employee or an accomplice (see Exhibit 5-6). The fraudster inserts his own name, the name of a fictitious entity, or some other name on the payee line of the check. Altering the payee designation eliminates many of the problems associated with converting the check that would be encountered in a forged endorsement fraud. The alteration essentially
CHECK TAMPERING SCHEMES

EXHIBIT 5-6 Altered Payee Schemes
makes the check payable to the fraudster (or an accomplice), so there is no need to forge an endorsement and no need to obtain false identification. The fraudster or his accomplice can endorse the check in his own name and convert it.

Of course, if canceled checks are reviewed during reconciliation of the bank statement, a check made payable to an employee is likely to cause suspicion, especially if the alteration to the payee designation is obvious. This is the main obstacle that must be overcome by fraudsters in altered payee schemes.

**Altering Checks Prepared by Others: Inserting a New Payee** The method used to alter the payee designation on a check depends largely on how that check is prepared and intercepted. (Incidentally, the amount of the check may also be altered at the same time and by the same method as the payee designation.) Checks prepared by others can be intercepted by any of the methods discussed in the forged endorsements section above. When the fraudster intercepts a check that has been prepared by someone else, there are basically two methods that may be employed. The first is to insert the false payee’s name in place of the true payee’s. This is usually done by rather unsophisticated means. The true name might be scratched out with a pen or covered up with correction fluid. Another name is then entered on the payee designation. These kinds of alterations are usually simple to detect.

A more intricate method occurs when the perpetrator of the fraud enters the accounts payable system and changes the names of payees, which occurred in Case 1112. An accounts payable employee in this case was so trusted that her manager allowed her to use his computer password in his absence. The password permitted access to the accounts payable address file. This employee waited until the manager was absent, then selected a legitimate vendor with whom her company did a lot of business. She held up the vendor’s invoices for the day, and after work used the manager’s log-on code to change the vendor name and address to that of a fictitious company. The new name and address were run through the accounts payable cycle with an old invoice number, causing a fraudulent check to be issued. The victim company had an automated duplicate invoice test, but the fraudster circumvented it by substituting “1” for “I” and “0” (zero) for capital “O.” The next day, the employee would replace the true vendor’s name and address, and mutilate the check register so that the check payable to the fictitious vendor was concealed. Approximately $300,000 in false checks were issued using this method.

**Altering Checks Prepared by Others: “Tacking On”** The other method that can be used by fraudsters to alter checks prepared by others is “tacking on” additional letters or words to the end of the real payee designation. This rather unusual approach to check tampering occurred in Case 153, in which an employee took checks payable to “ABC” company and altered them to read “A.B. Collins.” She then deposited these checks in an account that had been established in the name of A.B. Collins. The simple inclusion of a filler line after the payee designation would have prevented the loss of over $60,000 in this case. In addition to altering the payee designation, the amount of the check can be altered by tacking on extra numbers if the person preparing the check is careless and leaves space for extra numbers in the “amount” portion of the check.

**Altering Checks Prepared by the Fraudster: Erasable Ink** When the fraudster prepares the check that is to be altered, the schemes tend to be a bit more sophisticated. The reason for this is obvious: When the perpetrator is able to prepare the check himself, he can prepare it with the thought of how the payee designation will be altered. But if
the perpetrator is preparing the check, why not make the check payable to himself or an accomplice to begin with? In order to get an authorized maker to sign the check, the fraudster must make it appear that the check is made out to a legitimate payee. Only after a legitimate signature is obtained does the fraudster in an altered payee scheme set about tampering with the check.

One of the most common ways to prepare a check for alteration is to write or type the payee’s name (and possibly the amount) in erasable ink. After the check is signed by an authorized maker, the perpetrator retrieves the check, erases the payee’s name, and inserts his own. One example of this type of fraud was found in Case 2212, in which a bookkeeper typed out small checks to a local supplier and had the owner of the company sign them. The bookkeeper then used her erasing typewriter to lift the payee designation and amount from the check. She entered her own name as the payee and raised the amount precipitously. For instance, the owner might sign a $10 check that later became a $10,000 check. These checks were entered in the disbursements journal as payments for aggregate inventory to the company’s largest supplier, who received several large checks each month. The bookkeeper stole over $300,000 from her employer in this scheme. The same type of fraud can be undertaken using an erasable pen. In some cases fraudsters have even obtained signatures on checks written in pencil.

We have already discussed how, with a proper separation of duties, a person who prepares a check should not be permitted to handle the check after it has been signed. Nevertheless, this is exactly what happens in most altered payee schemes. When fraudsters prepare checks with the intent of altering them later, those fraudsters obviously have a plan for reobtaining the checks once they have been signed. Usually, the fraudster knows that there is no effective separation of controls in place. He knows that the maker of the check will return it to him.

**Altering Checks Prepared by the Fraudster: Blank Checks** The most egregious example of poor controls in the handling of signed checks is one in which the perpetrator prepares a check, leaves the payee designation blank, and submits it to an authorized maker who signs the check and returns it to the employee. Obviously, it is quite easy for the fraudster to designate himself or an accomplice as the payee when this line has been left blank. Common sense tells us that one should not give a signed, blank check to another person. Nevertheless, this happened in several cases in our study, usually when the fraudster was a long-time, trusted employee. In Case 1616, for example, an employee gained the confidence of the owner of his company, whom he convinced to sign blank checks for office use while the owner was out of town. The employee would then fill in his own name as the payee on one of the checks, cash it, and alter the check when it was returned along with the bank statement. The owner’s blind trust in his employee cost him nearly $200,000.

**Converting Altered Checks** As with all other types of fraudulent checks, conversion is accomplished by endorsing the checks in the name of the payee. Conversion of fraudulent checks has already been discussed in previous sections and will not be reexamined here.

**Preventing and Detecting the Alteration of Company Checks** Most successful altered payee schemes occur when the person who prepares checks also has access to those checks after they have been signed. As with all forms of check tampering, altered payee schemes can usually be prevented by separating the duties of check preparation, signing, and delivery. It is also critical that the duty of reconciling the bank statement be
separated from other check-preparation functions. Altered payee schemes should be very simple to detect during reconciliation, simply because the name and/or amount on the fraudulent check will not match the entry in the books or the support for the check. In almost all successful altered payee schemes, the perpetrator was able to prepare checks and reconcile the bank statement.

In addition to diligently matching all bank statement items to canceled checks, organizations might consider the use of carbon copy checks. Even if these instruments are altered after they have been cut, the copy will still reflect the intended payee and amount. Another simple method is to require that all checks be drafted in permanent ink to prevent schemes in which the payee and amount are erased and rewritten after a check is signed.

Concealed Check Schemes

Another scheme that requires a significant breakdown in controls and common sense is the concealed check scheme. These are check tampering frauds in which an employee prepares a fraudulent check and submits it along with legitimate checks to an authorized maker who signs it without a proper review (see Exhibit 5-7). Although not nearly as common as the other check tampering methods, it is worth mentioning for its simplicity, its uniqueness, and the ease with which it could be prevented.

The perpetrator of a concealed check scheme is almost always a person responsible for preparing checks. The steps involved in a concealed check scheme are similar to those in a forged maker scheme, except for the way in which the employee gets the fraudulent check signed. These schemes work as follows: The perpetrator prepares a check made out to himself, an accomplice, a fictitious person, and so on. Instead of forging the signature of an authorized maker, the employee takes the check to the authorized maker, usually concealed in a stack of legitimate checks awaiting signatures. The checks are typically delivered to the signer during a busy time of day when he is rushed and will be less likely to pay close attention to them. Generally, the checks are fanned out on the signer’s desk so that the signature lines are exposed but the names of the payees are concealed. If a particular authorized maker is known to be inattentive, the checks are given to him.

The maker signs the checks quickly and without adequate review. Because he is busy or generally inattentive or both, he simply does not look at what he is signing. He does not demand to see supporting documentation for the checks, and does nothing to verify their legitimacy. Once the checks have been signed they are returned to the employee, who removes his check and converts it. This appears to be one of the methods used by Ernie Philips in the case study at the end of this chapter. Philips slipped several checks payable to himself into a stack of company checks, then took them to the operations manager, who was designated to sign checks when the business’s owner was out of town. The operations manager apparently did not check the names of the payees and unknowingly signed several company checks to Philips.

A similar example of the concealed check method took place in Case 2474, where a bookkeeper took advantage of the owner of her company by inserting checks payable to herself into batches of checks given to the owner for signature. The owner simply never looked at whom he was paying when he signed the checks.

The perpetrator of a concealed check scheme banks on the inattentiveness of the check signer. If the signer were to review the checks he was signing, he would certainly discover the fraud. It should be noted that the fraudster in these cases could make the fraudulent check payable to an accomplice, a fictitious person, or a fictitious business
Instead of payable to himself. This is more common and certainly a lot less dangerous for the employee (but not nearly as exciting).

**Authorized Maker Schemes**

The final check tampering scheme, the authorized maker scheme, may be the most difficult to defend against. An authorized maker scheme is a type of check tampering fraud.
Authorized maker prepares and signs company check

Payable to himself | Payable to his own business | Payable to a fictitious person or company | Payable to cash | Payable to an accomplice | Payable to a vendor (personal purchases) | Other

Is the check recorded in the disbursements journal?

NO

Payable to an accomplice | Payable to a vendor

YES

To expense account | To current vendor in accounts payable | To asset account | Record check as "void" | Other

The fraudulent check is endorsed (in the name of the payee) and converted

Employee endorses in his name | Employee endorses in fictitious name | Employee forges endorsement of a third party | Accomplice endorses/splits proceeds with employee | Other

Postconversion concealment

Remove canceled check from bank statement | Alter canceled check–insert legitimate payee | Force the reconciliation | Unconcealed | False expense vouchers | Other

EXHIBIT 5-8 Authorized Maker Schemes

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 (see Exhibit 5-8). 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.

Overriding Controls through Intimidation When a person is authorized to sign company checks, preparing the checks is easy. The employee simply writes and signs the instruments the same way he would with any legitimate check. In most situations, 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 company policy prohibits check signers from handling blank checks, the perpetrator’s influence normally can be used to overcome this impediment. What employee is going to tell the CEO that he can’t have a blank check?
The most basic way an employee accomplishes an authorized maker scheme is to override controls designed to prevent fraud. We have already stated that most authorized signatories have high levels of influence within their companies. This influence may be used by the perpetrator to deflect questions about fraudulent transactions. The most common example is one in which a majority owner or sole shareholder uses his company as a sort of alter ego, paying personal expenses directly out of company accounts. If this arrangement is disclosed and agreed to by other owners, there may be nothing illegal about it. After all, one cannot steal from oneself. On the other hand, in the absence of an agreement between all owners, these disbursements amount to embezzlement. Instead of paying personal expenses, the fraudster might cut checks directly to himself, his friends, or family. Using fear of job security as a weapon, the owner can maintain a work environment in which employees are afraid to question these transactions.

High-level managers or officers may also use their authority to override controls in those companies whose ownership is either absent or inattentive. Intimidation can play a large part in the commission and concealment of any type of occupational fraud where powerful individuals are involved. In Case 878, for example, the manager of a sales office stole approximately $150,000 from his employers over a two-year period. This manager had primary check-signing authority and abused this power by writing company checks to pay his personal expenses. The manager’s fraudulent activities were well known by certain members of his staff, but these employees’ careers were controlled by the perpetrator. Fear of losing their jobs combined with lack of a proper whistleblowing structure prevented the manager’s employees from reporting his fraud.

Poor Controls Although overriding controls is the most blatant way to execute an authorized maker scheme, it is not the most common. Far more of these schemes occur because no one is paying attention to the accounts and few controls are present to prevent fraud. In Case 740, for example, a manager of a small business wrote company checks to purchase assets for his own business. He took approximately $800,000 from his employer, hiding the missing money in accounts receivable because he knew that those accounts were reviewed only once a year. Before audits, the manager would borrow money from the bank to replace the missing funds, then begin the whole process again when the books were closed. This unfortunate scheme ended in tragedy as the manager and his wife committed suicide when the fraud came to light. Setting aside the personal catastrophe that occurred in this case, it is obvious that if the books had been more closely monitored, or if there had been a threat of surprise audits in addition to the regularly scheduled reviews, this fraud might not have gotten so far out of hand.

The failure to closely monitor accounts is supplemented by lack of internal controls, specifically the absence of separation of duties in the cash disbursements process. In Case 2802, for instance, the perpetrator was in charge of signing all company checks, as well as reconciling the bank accounts for a small business. This put the fraudster in perfect position to write fraudulent checks to herself and her husband. Similarly, in Case 196 the bookkeeper of a medium-sized company was charged with paying all bills and preparing the company payroll. She had access to an automatic check signer and total control over company bank accounts. The bookkeeper wrote extra checks to herself, coded the expenditures to payroll, and destroyed the canceled checks when they were returned with the bank statement. Had the duties of preparing checks and reconciling accounts been separated, as they should be, the fraudster would not have been able to complete her scheme.

Preventing and Detecting Check Tampering by Authorized Makers Check tampering committed by authorized signers can be among the most difficult forms of
CHAPTER 5 CHECK TAMPERING

Occupational fraud to prevent, simply because the check signer is relied on by an organization to serve as a control against fraud by reviewing prepared checks and affixing her signature only to legitimate disbursements. When the check signer is herself a part of the fraud, this control evaporates.

As with all forms of check tampering, the most important preventative measure is to establish a firm separation of duties in the check-writing function, specifically to separate the duties of preparing and signing checks, and to ensure that check signers do not have access to blank checks. If an authorized maker has access only to checks that have already been prepared by someone else, then she cannot create a fraudulent check on her own.

Another control that can help limit losses caused by authorized maker schemes is to require dual signatures for disbursements over a threshold amount. This will not prevent fraudulent checks below the threshold, but it will limit the damage a single fraudster can do by abusing his or her check-signing authority.

Organizations should also maintain up-to-date vendor lists and confirm all disbursements to the list, giving scrutiny to checks written to unknown vendors. Payments to known vendors in unusual amounts or at unusual times should also be investigated. In addition, canceled checks should be spot-checked for proper support and to verify the business purpose of the disbursements. Obviously, all of these tests should be performed by persons who are independent of the disbursements function.

CONCEALING CHECK TAMPERING

Since most check tampering schemes do not consist of a single occurrence but instead continue over a period of time, concealing the fraud is arguably the most important aspect of the scheme. If a fraudster intended to steal a large sum of money and skip to South America, hiding the fraud might not be so important. But the vast majority of occupational fraudsters remain employees of their companies as they continue to steal from them. Therefore, hiding the fraud is extremely important. Concealment of the fraud means not only hiding the identity of the criminal, but in most cases hiding the fact of the fraud. The most successful frauds are those in which the victim company is unaware that it is being robbed. Obviously, once a business learns that it is being victimized it will take steps to staunch its bleeding and the end of the fraudster’s scheme will be at hand.

Check tampering schemes can present especially tricky concealment problems for fraudsters. In other types of fraudulent disbursements such as invoice or payroll schemes, the fraudulent payment is entered in the books as a legitimate transaction by someone other than the fraudster. Remember that the payments in those schemes are generated by the production of false documents that cause accounts payable personnel to think that money is owed to a particular person or vendor. When accounts payable issues a disbursement for a bogus invoice, it does so because it believes the invoice to be genuine. The payment is then entered in the books as a legitimate payment. In other words, the perpetrator generally does not have to worry about concealing the payment in the books, because someone else unwittingly does it for him.

Check tampering schemes do not always afford this luxury to the fraudster. In forgery and authorized maker schemes the perpetrator is the one writing the check, and he is usually the one coding the check in the disbursements journal. He must “explain” the check on the books. Forged endorsement schemes and altered payee schemes are
different because they involve the alteration of checks that were already prepared and coded by someone else. Nevertheless, they create a problem for the fraudster because the intercepted check was intended for a legitimate recipient. In short, someone is out there waiting for the check that the fraudster has taken. The culprit in these schemes must worry not only about hiding the fraud from his employer, but also about appeasing the intended payee. If the intended recipient of the check does not receive his payment, he will complain to the fraudster’s employer about the nonpayment. This could trigger an investigation into the whereabouts of the missing check, something the fraudster definitely wants to avoid.

The Fraudster Reconciling the Bank Statement

Many of those who perpetrate check tampering frauds are involved in reconciling the company’s bank statement. The bank statement that a company receives normally includes the canceled checks that have been cashed in the preceding period. A person who reconciles the accounts is therefore in a position to hide the existence of any fraudulent checks that he has written to himself. He can remove the fraudulent checks or doctor the bank statement or both.

We said earlier that in forged maker and authorized maker schemes, the perpetrator usually has to code the check in the disbursements journal. The most fundamental way to hide the check is to code it as “void” or to include no listing at all in the journal. Then, when the bank statement arrives, the perpetrator removes the fraudulent check from the stack of returned checks and destroys it. Now there is no record of the payment in the journal and no physical evidence of the check on hand. Of course, the bank will have a copy of the check, but unless someone questions the missing check there will be little chance that the company will routinely discover the problem. And since the perpetrator is the one who reconciles the account, it is unlikely that anyone will even notice that the check is missing.

The problem with simply omitting the fraudulent check from the disbursements journal is that the bank balance will not reconcile to the book balance. For instance, if the fraudster wrote a $25,000 check to himself and did not record it, then the book balance will be $25,000 higher than the bank balance ($25,000 was taken out of the bank account by the fraudster, but was not credited out of the company’s cash account). Fraudsters usually omit their illicit checks from the disbursements journal only in situations where they personally reconcile the bank statement and no one reviews their work. This allows the fraudster to force the reconciliation. In other words, the fraudster reports that the bank balance and book balance match, when in fact they do not. These are circumstances in which the employer basically takes the perpetrator’s word that the book balance and bank balance reconcile.

Some of the victim companies in our study simply did not reconcile their accounts regularly. Because no one was reconciling the book balance and the bank balance, the fraudster was able to write checks without recording them. In a system where controls are so lax, almost any concealment method will be effective to disguise fraud. In fact, no effort to conceal the crime may even be necessary in these circumstances.

Fraudsters might physically alter the bank statement to cause it to match the company’s book balance. For instance, a person engaging in a forged maker scheme may decide to steal blank checks from the back of the checkbook. These checks are out of sequence and therefore will be listed last on the bank statement. The employee then
deletes this clump of checks and alters the final total to match the victim company’s books. We will see this method of concealment used in the following case study.

In some cases, an employee’s duties do not include reconciling the bank accounts, but he is nevertheless able to intercept bank statements and alter them to hide his crimes. In the following case study, Ernie Philips was able to persuade his company’s bank to send the bank statements directly to him instead of his boss. Philips then altered the bank statements to conceal his fraudulent activities. This case describes how CFE James Sell put an end to Philips’s scheme.

CASE STUDY: WHAT ARE FRIENDS FOR?

Ernie Philips had fallen on hard times. Several back operations left him barely able to move around. He became addicted to the pills that made the pain bearable. His CPA practice was going under. He and his wife had six adopted children to support. Not surprisingly, he suffered from depression and chronic anxiety. But Ernie’s luck changed when he ran into his old friend, James Sell. The two men had worked together at a federal agency and known each other over 20 years. Ernie talked about the trouble he was having and James said he could help. At the time, Ernie was in a rehabilitation program for his substance abuse, so James told him, “Let me know when you’re finished with that, and I’ll have some work for you.”

James rented Ernie an office and started sending a few small projects his way. “I wanted to try him out, see how he would do,” Sell remarks. “He seemed like he was trying to get himself together.” Ernie completed the work on time, and performed well, so when James got a big account with the Arizona and Nevada governments, he brought his friend into the main office. They agreed on a salary just over $38,000 a year, which James upped to $42,000 after six months.

Sell was appointed receiver for CSC Financial Services in Arizona and Nevada. CSC owners had been caught diverting $5.5 million of customer escrow funds from its operations in Arizona and Nevada. The computer equipment used in the operation dated from the 1960s, and a lack of supervision and proper controls had obviously allowed the embezzlement to take place. The company didn’t use a double-entry system, so management could alter ending totals with a wide latitude. Even after a regulatory audit discovered that things were in disarray at CSC, the Arizona administrators had allowed the offending owners to continue operating for a year and a half. So when Sell finally took over, he found a rather large mess. That’s part of the game, he says. “When you get a company as receiver, you try to survive with what you inherit.” The receivership involved more than 15,000 active accounts, with about $285 million in-house payments each year, and over 30,000 transactions a month. Sorting out the trouble wouldn’t be easy. Sell knew Ernie had experience, and so tapped him for the job. “One of the reasons I brought him in,” Sell says, “was to establish controls where there were none before.”

But Ernie had little respect for controls. When James asked the mailroom clerk about the bank statements for a particular month, he told him that Ernie had them. “Why is that?” James asked. “He knows those are supposed to come to me unopened. He shouldn’t have them.” The clerk said Ernie needed the statements for a reconciliation. James didn’t want to overreact, but he was nervous. “There’s limited control over any position and even less over a key financial position,” he says, “and any time you lose a control point, you’re in jeopardy. So you have to take a strong position in order to restore the process.” He discussed the matter with Ernie and thought they had an understanding.

Ernie was having problems with other people in the company too. He and the operations manager had a heated exchange when the manager retrieved some account papers from Ernie’s desk. Ernie had been out and the papers were needed right away. When Ernie aired his grievance, James sided with the operations manager. There shouldn’t be any problem, James said. It wasn’t like anyone was rifling Ernie’s desk. Besides that, Sell traveled frequently, and spent a lot of time in the Nevada office, so having open access in the Arizona office allowed for informal oversight. Sell muses, “One of the best controls in the world is to create an atmosphere of uncertainty. Usually embezzlement doesn’t occur unless the person thinks he can hide what he’s doing. So I figured this would be a way to keep things on the up and up.”

The uncertainty didn’t prevent the fraud, but it did help detect what was going on. The operations manager discovered Ernie’s sting during a search for accounting records. He brought Sell a company check from Ernie’s desk, made out in the name of Ernie Philips for $2,315. It wasn’t Ernie’s payroll check, so what was it? The check hadn’t been cashed, but Sell’s signature had been forged. Not sure yet about the situation, Sell arranged to meet Ernie away from the main office.

Sell had been out of town and needed some updates on the escrow operations, so he dropped by Ernie’s private office one afternoon. After they finished their discussion, James said, “There’s one more thing I wanted to ask you about.” He pulled a copy of the check from his briefcase and told Ernie, “I was hoping you could explain this.”
There was a long silence. Ernie stared at the check, pursing his lips and scratching his hands across the desktop. The pause stretched into what seemed like minutes. Finally he confessed, “I’ve been taking money.”

“I could tell from the look on his face this was trouble.” Sell reports. The worst was confirmed. He had been hoping there was an explanation, an innocuous one, despite all the signs. Still, he had come prepared. “I wanted to confront him there was an explanation, an innocuous one, despite all the Sell reports. The worst was confirmed, “I’ve been taking money.”

“A pause stretched into what seemed like minutes. Finally he pursed his lips and scratching his hands across the desktop. The pause stretched into what seemed like minutes. Finally he confessed, “I’ve been taking money.”

Sell barred Ernie from both his offices, and began tracing his friend’s activities over the past seven months. In some cases, Sell’s name was forged onto the checks in handwriting that wasn’t his and which bore a resemblance to Ernie’s. Others were marked with the signature stamp that was supposed to remain locked in a clerk’s office except when she was using it for a very limited set of transactions. Somehow, Ernie had been able to slip the stamp away and mark his checks.

He covered his tracks by taking checks out of sequence so they would show up at the end of the bank statement. Then he’d intercept the statement, and alter the report at the end, returning a copy of the statement to the clerk for filing. After the clerk told Sell about Ernie having the statement, Ernie arranged with the bank for the statements to come addressed to his attention. Without getting authorization, the bank agreed; Ernie could then doctor the statement, copy it, and send it down the line. If someone did ask about an unidentified disbursement, Ernie told them the money went to a supplier vendor and, since he was the controller, he was taken at his word. He even managed on a couple of occasions to slip checks made out to himself into a regular batch, which the operations manager—who was authorized to sign checks in Sell’s absence—signed.

Sell was, to put it mildly, chagrined. He had believed that his office was set up to avoid the kind of flagrant defalcation he was facing now. But, he admits, “No matter how good a system you design, one knowledgeable person can circumvent it... The trick is to make sure the procedures you set up are followed. I don’t know if there’s a system in the world that’s immune. The key is to limit and control the extent of any one person’s action, so you can at least detect when things go awry.”

Sell figured his losses at about $109,000. He got a complete run of the bank statements from Ernie’s tenure, identified checks out of sequence, or gaps in issued checks, and then verified to whom they were payable and the stated purpose. The scheme had required some footwork, but wasn’t terribly sophisticated. The checks were written in odd-number amounts, $4,994.16 for example, but Ernie had made the payments in his own name. He had left behind some of his personal bank statements, which showed deposits correlated with the money he’d taken from Sell. (The amounts didn’t always match, because Ernie would take cash back from the deposit, but they were close enough to link the transactions.)

Ernie’s brief era of good feelings had ended. He had used the proceeds from his finagling for a lavish family vacation, a new car, a new computer, and improvements on the house where he lived with his wife and their adopted family, but in the fallout of his dismissal Ernie’s house went into foreclosure. He was charged around the same time with Driving Under the Influence. The CPA board revoked his license and fined him for ethics violations. He made no defense at his civil trial, where a judgment was rendered against him for the $109,000 he took plus treble damages. While he was out on bail for the criminal charges against him, Ernie took his family and fled. Sell was able to locate him through an Internet search service. Ernie died in May 1996. “He threw everything away,” Sell laments. “For $109,000 he fouled up his life, and his family.”

Sell takes the matter philosophically. There are plenty of cases that echo Ernie’s. For example, Sell just investigated a paralegal who not only wrote company checks to herself, but also sent one to the County Attorney’s office—to pay the fine she owed for writing bad checks. “Typically, these people don’t take the time to set up a new identity or a dummy company,” James says. “They just want the money fast and grab it the easiest way they can.”

“And often enough,” he adds, “they want to get caught. . . Ernie knew he was out of control; we had been friends for so long. He knew he was doing more than just breaking the law. During one of our conversations after this he told me, ‘You know, the first check was real hard to write. But I had clients I had borrowed from, I owed money all over the place, I had a family. As it went on, writing the checks just got easier.’”

**Re-Altering Checks**

In altered payee schemes, remember that it is common for the perpetrator to take a check intended for a legitimate recipient, then doctor the instrument so that he is designated as
the payee. A company check payable to an employee will obviously raise suspicions of fraud when the canceled check is reconciled with the bank statement. To prevent this, some employees re-alter their fraudulent checks when the bank statement arrives. We have already discussed how some fraudsters alter checks by writing the payee’s name in erasable ink or type when the check is prepared. These employees obtain a signature for the check, then erase the true payee’s name and insert their own. When these checks return with the statement, the employee erases his own name and reenters the name of the proper payee. Thus there will be no appearance of mischief. The fraudster in Case 1616 used the re-alteration method to hide over $185,000 in fraudulent checks.

The re-alteration method is not limited to altered payee schemes. The concealment will be equally effective in forged maker schemes, authorized maker schemes, and concealed check schemes. Re-altered checks will match the names of legitimate payees listed in the disbursements journal.

Falsifying the Disbursements Journal

Rather than omit a fraudulent check from the disbursements journal or list it as void, the perpetrator might write a check payable to himself but list a different person as the payee on the books. Usually, the fake payee is a regular vendor—a person or business that receives numerous checks from the victim company. Employees tend to pick known vendors for these schemes because one extra disbursement to a regular payee is less likely to stand out.

The false entry is usually made at the time the fraudulent check is written, but in some cases the fraudster makes alterations to existing information on the book. In the opening case study in this chapter, for instance, Melissa Robinson used correction fluid and an eraser to change the payee names in her company’s checkbook. Obviously, alterations found in a company’s books should be carefully scrutinized to make sure they are legitimate.

The fraudster can also conceal a fraudulent check by falsely entering the amounts of legitimate checks in the disbursements journal. He overstates the amounts of legitimate disbursements in order to absorb the cost of a fraudulent check. For instance, assume that a company owes $10,000 to a particular vendor. The fraudster would write a check to the vendor for $10,000, but enter the check in the disbursements journal as a $15,000 payment. The company’s disbursements are now overstated by $5,000. The fraudster can write a $5,000 check to himself and list that check as void in the disbursements journal. The bank balance and the book balance will still match, because the cost of the fraudulent check was absorbed by overstating the amount of the legitimate check. Of course, the fact that the canceled checks do not match the entries in the journal should indicate potential fraud. This type of concealment is really effective only when the bank accounts are not closely monitored or where the employee is in charge of reconciling the accounts.

If possible, fraudsters will try to code their fraudulent checks to existing accounts that are rarely reviewed or to accounts that are very active. In Case 804, for instance, the perpetrator charged his checks to an intercompany payables account because it was reviewed only at the end of the year, and not in great detail. The perpetrator in this case might also have coded his checks to an account with extensive activity in the hopes that his fraudulent check would be lost in the crowd of transactions on the account. In the cases the ACFE researchers reviewed, most checks were coded to expense accounts or liability accounts.
This particular method can be very effective in concealing fraudulent checks, particularly when the victim company is not diligent in reconciling its bank accounts. For instance, in Case 1761, the victim company reconciled its accounts by verifying the amount of the checks with the check numbers, but did not verify that the payee on the actual check matched the payee listed in the disbursements journal. As a result, the company was unable to detect that the checks had been miscoded in the disbursements journal. As we discussed in the previous section, the fraudster might also intercept the bank statement before it is reconciled and alter the payee name on the fraudulent check to match the entry he made in the disbursements journal.

**Reissuing Intercepted Checks**

We mentioned before that in intercepted check schemes, the employee faces detection not only through his employer’s normal control procedures, but also from the intended recipients of the checks he steals. After all, when these people do not receive their payments from the victim company they are likely to complain. These complaints, in turn, could trigger a fraud investigation.

Some employees head this problem off by issuing new checks to the people whose initial checks they stole. In Case 579, for instance, an employee would steal checks intended for vendors and deposit them into her own checking account. She would then take the invoices from these vendors and reenter them in the company’s accounts payable system, adding a number or letter to avoid the computerized system’s duplicate check controls. This assured that the vendors received their due payment, and therefore would not blow the whistle on her scheme, which netted approximately $200,000.

Another example of reissuance was provided by an accounts payable troubleshooter in Case 1328. The employee in this case was in charge of auditing payments to all suppliers, reviewing supporting documents, and mailing checks. Every once in a while, she would purposely fail to mail a check to a vendor. The vendor, of course, would call accounts payable about the late payment and would be told that his invoice had been paid on a certain date. Since accounts payable did not have a copy of the canceled check (because the fraudster was still holding it), they would call the troubleshooter to research the problem. Unfortunately for the company, the troubleshooter was the one who had stolen the check. She would tell accounts payable to issue another check to the vendor while she stopped payment on the first check. Thus the vendor received his payment. Meanwhile, instead of stopping payment on the first check, the troubleshooter deposited it into her own account.

The difference between these two schemes is that in the latter, two checks were issued for a single invoice. The troubleshooter in Case 1328 did not have to worry about this problem because she performed the bank reconciliations for her company and was able to force the totals. Once again we see how access to the bank statement is a key to concealing a check tampering scheme.

**Bogus Supporting Documents**

While some fraudsters attempt to wipe out all traces of their fraudulent disbursements by destroying the checks, forcing the bank reconciliation, and so on, others opt to justify their checks by manufacturing fake support for them. These fraudsters prepare false payment vouchers, including false invoices, purchase orders, and/or receiving reports, to create an appearance of authenticity. This concealment strategy is practical only when the employee writes checks payable to someone other than himself (e.g., an accomplice or a
shell company). A check made payable to an employee may raise suspicions regardless of any supporting documents he manufactures.

Conceptually, the idea of producing false payment vouchers may seem confusing in a chapter on check tampering. If the fraudster is using fake vouchers, shouldn’t the crime be classified as a billing scheme? Not necessarily. In a check tampering scheme, the fraudster generates the disbursement by writing the check himself. He may create fake support to justify the check, but the support—the voucher—had nothing to do with the disbursement being made. Had the fraudster not created a fake invoice, he would still have had a fraudulent check.

In a billing scheme, on the other hand, the fraudster uses the false voucher to cause a payment to be generated. Without a fake voucher in these schemes, there would be no fraudulent disbursement at all, because the employee depends on someone else to actually cut the check. In other words, the false voucher is a means of creating the unwarranted payment in these schemes, rather than an attempt to hide it.

### PROACTIVE COMPUTER AUDIT TESTS FOR DETECTING CHECK TAMPERING SCHEMES

<table>
<thead>
<tr>
<th>Title</th>
<th>Category</th>
<th>Description</th>
<th>Data file(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract all voided checks and summarize by issuer for reasonableness.</td>
<td>All</td>
<td>Checks may be voided in the system and then cashed (which requires another entry in the bank reconciliation to conceal the fraud).</td>
<td>• Check Register</td>
</tr>
<tr>
<td>Extract all reconciling items per the bank reconciliation and summarize for reasonableness.</td>
<td>All</td>
<td>Most of the concealment of check tampering is done between the bank balance and the general ledger. Therefore, these adjusting entries should be closely scrutinized.</td>
<td>• General Ledger Detail</td>
</tr>
<tr>
<td>Summarize debit memos by vendor, issuer, and type.</td>
<td>All</td>
<td>Debit memo trends that appear unusual should be investigated as attempts to cover unauthorized payments.</td>
<td>• Invoice Payment</td>
</tr>
<tr>
<td>Identify duplicate payments based on various means.</td>
<td>All</td>
<td>Duplicate payments are made to properly pay down open vendor balances when another check, intended for the vendor, is stolen. Duplicate payment tests can be enacted on the vendor, invoice number, amount. More complicated tests can look where the same invoice and amount are paid yet the payment is made to two different vendors. Another advanced test would be to search for same vendor and invoice when a different amount is paid.</td>
<td>• Invoice Payment</td>
</tr>
<tr>
<td>Summarize accounts payable activity by general ledger account, sort from high to low, and review for reasonableness.</td>
<td>All</td>
<td>Expense account trends that appear unusual should be investigated as attempts to cover unauthorized payments.</td>
<td>• Invoice Payment G/L Distribution</td>
</tr>
</tbody>
</table>
## PROACTIVE COMPUTER AUDIT TESTS FOR DETECTING CHECK TAMPERING SCHEMES

<table>
<thead>
<tr>
<th>Test Description</th>
<th>Access Levels</th>
<th>Description</th>
<th>Files Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compare balance per accounts payable subledger to vendor account balances per their accounts receivable system.</td>
<td>All</td>
<td>Vendors that are not paid will show their customer account from the defrauded company as an old receivable. In order to obtain an electronic file of all customer account statements, it may be necessary to request statements and enter them into a spreadsheet. Please note that even vendors with no balance should be requested to provide customer statements.</td>
<td>• Accounts Payable Subledger&lt;br&gt;• Customer Account Statements (from all vendors)</td>
</tr>
<tr>
<td>Extract users who can write checks and also post entries to the general ledger.</td>
<td>All</td>
<td>Users who can write checks and also subsequently conceal the misappropriation through adjustments to the general ledger cash accounts would be taking advantage of a nonsegregation of duties to conceal their fraud. User access should be reviewed from the perspective of adjustments within the application and adjustments to the data itself.</td>
<td>• Check Register User Access Master File&lt;br&gt;• General Ledger User Access Master File&lt;br&gt;• Check Register User Access Log File&lt;br&gt;• General Ledger User Access Log File</td>
</tr>
<tr>
<td>Extract all employee payments equal to zero in any given pay period.</td>
<td>All</td>
<td>Reports unusual check amounts to employees for review. Check amounts may be written in after printing.</td>
<td>• Check Register*</td>
</tr>
<tr>
<td>Extract all checks payable to &quot;cash&quot; and summarize by issuer for reasonableness.</td>
<td>Forged maker</td>
<td>Checks issued to “cash” have a higher incidence of fraud.</td>
<td>• Check Register*</td>
</tr>
<tr>
<td>Extract manual checks and summarize by vendor and issuer.</td>
<td>Forged maker</td>
<td>Manual checks are more prone to abuse and therefore should be scrutinized, especially if a particular issuer is drafting the majority of manual checks.</td>
<td>• Check Register*</td>
</tr>
<tr>
<td>Extract all purchases with no purchase orders and summarize by vendor and issuer.</td>
<td>Forged maker</td>
<td>Purchases with no purchase orders are more prone to abuse and therefore should be scrutinized, especially if a particular issuer is drafting the majority of payments without purchase orders.</td>
<td>• Invoice Payment</td>
</tr>
<tr>
<td>Sequence gaps in checks.</td>
<td>Forged maker</td>
<td>Check that are stolen will normally not appear in the check register and therefore will be seen as a gap in the check sequence.</td>
<td>• Check Register*</td>
</tr>
<tr>
<td>Extract checks that are out of the normal sequence.</td>
<td>Forged maker, concealed check, and authorized maker</td>
<td>Checks that are fabricated or stolen will many times not be in the same general sequence as the company’s normal check sequence.</td>
<td>• Check Register*</td>
</tr>
<tr>
<td>Sample vendor open invoices for confirmation with vendor.</td>
<td>Forged maker, concealed check, and authorized maker</td>
<td>Similar to the above comparison test, vendor invoices may appear paid on the subledger when the vendor believes such invoices have not been paid.</td>
<td>• Invoice Payment</td>
</tr>
</tbody>
</table>

*Please note that the file “Check Register” may designate the vendor check register but could also refer to the payroll check register.
SUMMARY

Check tampering is a form of occupational fraud in which an employee converts an organization’s funds by fraudulently preparing a company check for his own purpose, or by intercepting and converting an organization’s check that is intended for a third party. Most check tampering frauds fall into one of five categories: (1) forged maker schemes, (2) forged endorsement schemes, (3) altered payee schemes, (4) concealed check schemes, and (5) authorized maker schemes.

In a forged maker scheme, the perpetrator obtains or counterfeits an organization’s blank check and makes it payable to himself, an accomplice, or a third party. The perpetrator forges the signature of an authorized check signer (or “maker”) in order to convert the fraudulent instrument.

A forged endorsement scheme occurs when an employee intercepts an outgoing check intended for a third party and converts the check by forging the intended payee’s name on the endorsement line of the check. A third form of check tampering—the altered payee scheme—also involves the theft of outgoing checks. In this type of fraud, the perpetrator alters the name of the payee on the stolen check so that he will be able to convert it. It should be remembered that these schemes will be classified as check tampering only if they involve the theft of outgoing checks drawn on the organization’s bank accounts. This is because check tampering is a form of fraudulent disbursement; hence there must be a disbursement of the organization’s funds. If an employee intercepts an incoming check that is payable to the organization, then that scheme will be classified as either skimming or cash larceny (see Chapters 2 and 3).

A fourth category of check tampering is the authorized maker scheme, in which an employee with check-signing authority abuses the trust of his employer by writing fraudulent checks on organization accounts. Finally, an employee lacking signature authority can obtain signatures on fraudulent checks by concealing them within a large group of legitimate checks awaiting signature, where they are likely to be overlooked.

Check tampering frauds occur primarily because of the lack of adequate internal controls. The most effective control is to segregate duties among those employees with access to the organization’s checks, including the preparation, posting, signing, delivery, and reconciliation functions. Additional controls include a routine review of supporting documentation, canceled checks, out-of-sequence check numbers, and changes to vendor addresses. Finally, check stock should be adequately safeguarded to preclude theft.

ESSENTIAL TERMS

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

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

**Maker** The person who signs a check.

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

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

**Forced reconciliation** A method of concealing a check tampering scheme by manipulating the bank reconciliation so that the bank balance and the book balance match.

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

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

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

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?

5-2 (Learning objective 5-2) There are five principal categories of check tampering frauds. What are they?

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?

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?

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?

5-6 (Learning objective 5-6) What are the differences between a forged maker and a forged endorsement scheme?

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

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?

5-9 (Learning objective 5-7) How can a perpetrator conceal check tampering activity from 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.

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?

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?

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?

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?

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 a check signing instrument. What are some controls an organization could institute to minimize the chance a forgery will occur?

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.

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 fraud?

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?

ENDNOTES


2. Lanza, pp. 58–60.