FRAUD SCHEMES

**Fraud** – An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, **involving the use of deception** to obtain an **unjust or illegal advantage**.

**Financial statement fraud schemes** are one of a large category of frauds that fall under the heading of *Occupational Fraud and Abuse*, which is defined as “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.” Simply stated, occupational frauds are those in which an employee, manager, officer, or owner of an organization commits fraud to the detriment of that organization. The three major types of occupational fraud are: **Corruption, Asset Misappropriation, and Fraudulent Statements**

**Bribery and Corruption**

Generally, bribery and corruption are off-book frauds that occur in the form of kickbacks, gifts, or gratuities to government employees from contractors or to private business employees from vendors.

At its heart, a bribe is a business transaction, albeit an illegal or unethical one. A person “buys” something with the bribes he pays. What he buys is the influence of the recipient.

Bribery schemes can be difficult and expensive. Though they are not nearly as common as other forms of occupational fraud such as asset misappropriations, bribery schemes tend to be much more costly.

There are two basic reasons why a bribe occurs:

- Because the transaction is not in the interests of the organization for whom the person being bribed acts. Therefore, if the other party wants the transaction to be effected, it is necessary to bribe that person.
- Although the person receiving the bribe may be acting in the best interests of his organization by agreeing/approving the transaction, he may refuse to act until he has received the bribe. This may be the convention of the industry/country in which he is operating and accepted by the person offering the bribe not as immoral but as a necessary expense and in the interests of his own organization.

Bribery is often defined as the offering, giving, receiving, or soliciting anything of value to influence an official act. The term *official act* means that bribery only encompasses payments made to influence the decisions of government agents or employees.

Many occupational fraud schemes, however, involve **commercial bribery**, which is similar to the traditional definition of bribery except that something of value is offered to influence a business decision rather than an official act of government.

**Conflict of Interest**:

Conflict of interest schemes generally constitute violations of the principal that a fiduciary, agent, or employee must act in good faith, with full disclosure, and in the best interest of the principal or employer. A conflict of interest occurs when an employee, manager, or executive has an undisclosed economic or personal interest in a transaction that adversely affects that person’s employer. As with other corruption frauds, conflict schemes involve the exertion of an
employee’s influence to the detriment of his company. In bribery schemes, fraudsters are paid to exercise their influence on behalf of a third party.

If an employee engages in a transaction that involves a conflict of interest, then the employee might also have breached his fiduciary duty to his employer. An agent (employee) owes a fiduciary duty (duty of loyalty) to the principal (employer). The agent must act solely in the best interest of the principal and cannot seek to advance personal interest to the detriment of the principal.

Breach of fiduciary duty is a civil action that can be used to redress a wide variety of conduct that might also constitute fraud, commercial bribery, and conflicts of interest. The elements of proof of breach of fiduciary duty are considerably simpler than fraud, and may not require proof of wrongful intent. As in conflicts of interest, the wrongdoer must reimburse the principal for any losses and pay over profits earned, even if the principal suffered no loss.

The vast majority of conflict of interest cases occur because the fraudster has an undisclosed economic interest in a transaction. But the fraudster’s hidden interest is not necessarily economic. In some scenarios an employee acts in a manner detrimental to his company in order to provide a benefit to a friend or relative, even though the fraudster receives no financial benefit from the transaction himself.

In order to be classified as a conflict of interest scheme, the employee’s interest in the transaction must be undisclosed. The crux of a conflict case is that the fraudster takes advantage of his employer; the victim organization is unaware that its employee has divided loyalties. If an employer knows of the employee’s interest in a business deal or negotiation, there can be no conflict of interest, no matter how favorable the arrangement is for the employee.

**Bribery**

Bribery schemes generally fall into two broad categories:

- a. kickbacks
- b. bid-rigging schemes

**Kickback Schemes:**

Kickbacks are undisclosed payments made by vendors to employees of purchasing companies. The purpose of a kickback is usually to enlist the corrupt employee in an overbilling scheme. Sometimes vendors pay kickbacks simply to get extra business from the purchasing company.

Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and vendors. In a common type of kickback scheme, a vendor submits a fraudulent or inflated invoice to the victim organization and an employee of that organization helps make sure that a payment is made on the false invoice. For his assistance, the employee-fraudster receives a payment from the vendor. This payment is the kickback.

Kickback schemes almost always attack the purchasing function of the victim company, so it stands to reason that these frauds are often undertaken by employees with purchasing responsibilities.

**Diverting Business to Vendors**

In some instances, an employee-fraudster receives a kickback simply for directing excess business to a vendor. There might be no overbilling involved in these cases; the vendor simply pays the kickbacks to ensure a steady stream of business from the purchasing company.
Employees with Approval Authority
In most instances, kickback schemes begin as overbilling schemes in which a vendor submits inflated invoices to the victim organization. The false invoices either overstate the cost of actual goods and services, or reflect fictitious sales. The vendor in a kickback scheme generally seeks to enlist the help of an employee with the authority to approve payment of the fraudulent invoices. This authority assures payment of the false billings without undue hassles.

Fraudsters Lacking Approval Authority
While the majority of kickback schemes involve persons with authority to approve purchases, this authority is not an absolute necessity. When an employee cannot approve fraudulent purchases himself; he can still orchestrate a kickback scheme if he can circumvent accounts payable controls. In some cases, all that is required is the filing of a false purchase requisition. If a trusted employee tells his superior that the company needs certain materials or services, this is sometimes sufficient to get a false invoice approved for payment. Such schemes are generally successful when the person with approval authority is inattentive or when he is forced to rely on his subordinate’s guidance in purchasing matters.

Other Kickback Schemes
Bribes are not always paid to employees to process phony invoices. Some outsiders seek other fraudulent assistance from employees of the victim organization. For instance, inspectors are sometimes paid off to accept substandard materials, or to accept short shipments of goods.

Kickback Payments
It should also be noted that every bribe is a two-sided transaction. In every case where a vendor bribes a purchaser; there is someone on the vendor’s side of the transaction who is making an illicit payment. It is therefore just as likely that your employees are paying bribes as accepting them. In order to obtain the funds to make these payments, employees usually divert company money into a slush fund, a non-company account from which bribes can be made.

Assuming that bribes are not authorized by the briber’s company, he must find a way to generate the funds necessary to illegally influence someone in another organization. Therefore, the key to the crime from the briber’s perspective is the diversion of money into the slush fund. This is a fraudulent disbursement of company funds, which is usually accomplished by the writing of company checks to a fictitious entity or the submitting of false invoices in the name of a false entity. Payments to a slush fund are typically coded as “fees” for consulting or other services.

Bid-rigging Schemes
Bid-rigging schemes occur when an employee fraudulently assists a vendor in winning a contract through the competitive bidding process. The competitive bidding process, in which several suppliers or contractors are vying for contracts in what can be a very cutthroat environment, is tailor made for bribery. Any advantage one vendor can gain over his competitors in this arena is extremely valuable. The benefit of “inside influence” can ensure that a vendor will win a sought-after contract. Many vendors are willing to pay for this influence.

The Pre-solicitation Phase
In the pre-solicitation phase of the competitive bidding process—before bids are officially sought for a project—bribery schemes can be broken down into two distinct types. The first is the need recognition scheme, where an employee of a purchasing company is paid to convince his company that a particular project is necessary. The second reason to bribe someone in the pre-solicitation phase is to have the specifications of the contract tailored to the strengths of a particular supplier.
Need Recognition Schemes
The typical fraud in the need recognition phase of the contract negotiation is a conspiracy between the buyer and contractor where an employee of the buyer receives something of value and in return recognizes a “need” for a particular product or service. The result of such a scheme is that the victim organization purchases unnecessary goods or services from a supplier at the direction of the corrupt employee.

Specifications Schemes
The other type of pre-solicitation fraud is a specifications scheme. The specifications of a contract are a list of the elements, materials, dimensions, and other relevant requirements for completion of the project. Specifications are prepared to assist vendors in the bidding process, telling them what they are required to do and providing a firm basis for making and accepting bids.

The Solicitation Phase
In the solicitation phase of the competitive bidding process, fraudsters attempt to influence the selection of a contractor by restricting the pool of competitors from whom bids are sought. In other words, a corrupt vendor pays an employee of the purchasing company to assure that one or more of the vendor’s competitors do not get to bid on the contract. In this manner, the corrupt vendor is able to improve his chances of winning the job.

Bid Pooling
Bid pooling is a process by which several bidders conspire to split contracts up and assure that each gets a certain amount of work. Instead of submitting confidential bids, the vendors discuss what their bids will be so they can guarantee that each vendor will win a share of the purchasing company’s business.

Fictitious Suppliers / Vendors
Another way to eliminate competition in the solicitation phase of the selection process is to solicit bids from fictitious suppliers. This gives the appearance of a competitive bidding situation, when in fact only one real supplier bids on the job. Furthermore, the real contractor can hike up his prices, since the other bids are fraudulent and sure to be higher than his own. In effect, the bids from fictitious suppliers serve to validate the exaggerated quote from the real contractor.

Other Methods
In some cases, competition for a contract can be limited by severely restricting the time for submitting bids. Certain suppliers are given advanced notice of contracts before bids are solicited. These suppliers are therefore able to begin preparing their bids ahead of time. With the short time frame for developing bid proposals, the supplier with advance knowledge of the contract will have a decided advantage over his competition.

The Submission Phase
In the actual submission phase of the process, where bids are proffered to the buyer, several schemes may be used to win a contract for a particular supplier. The principal often tends to be abuse of the sealed bid process. Competitive bids are confidential; they are, of course, supposed to remain sealed until a specified date at which all bids are opened and reviewed by the purchasing company. The person or persons who have access to sealed bids are often the targets of unethical vendors seeking an advantage in the process.

Economic Extortion
Economic extortion cases are the “Pay up or else …” corruption schemes; basically the flip side of bribery schemes. Instead of a vendor offering a payment to influence a decision, an employee demands that a vendor pay him in order to make a decision in that vendor’s favor. If the vendor refuses to pay, he faces some harm such as a loss of business with
the extorter’s company. In any situation where an employee might accept bribes to favor a particular company or person, the situation could be reversed to a point where the employee extorts money from a potential purchaser or supplier.

**Illegal Gratuities**

Illegal gratuities are similar to bribery schemes except there is not necessarily intent to influence a particular business decision before the fact. In the typical illegal gratuities scenario, a decision is made which happens to benefit a certain person or company. The party who benefited from the decision then gives a gift to the person who made the decision. The gift could be anything of value. An illegal gratuity does not require proof of intent to influence.

At first glance, it may seem that illegal gratuities schemes are harmless as long as the business decisions in question are not influenced by the promise of payment. But most company ethics policies forbid employees from accepting unreported gifts from vendors. One reason is that illegal gratuities schemes can (and do) evolve into bribery schemes. Once an employee has been rewarded for an act such as directing business to a particular supplier, an understanding might be reached that future decisions beneficial to the supplier will also be rewarded. Additionally, even though an outright promise of payment has not been made, employees may direct business to certain companies in the hope that they will be rewarded with money or gifts.

**Methods of Making Illegal Payments:**

**Gifts, Travel, and Entertainment**

Most bribery (corruption) schemes begin with gifts and favors. Commonly encountered items include:

- Wine and liquor (consumable),
- Clothes and jewelry for the recipient or spouse,
- Sexual favors,
- Lavish entertainment,
- Paid vacations,
- Free transportation on corporate jets,
- Free use of resort facilities,
- Gifts of the briber’s inventory or services, such as construction of home improvements by a contractor.

**Cash Payments**

The next step usually involves cash payments. However, cash is not practical when dealing with large sums, because large amounts are difficult to generate, and they draw attention when they are deposited or spent. The use of currency in major transactions might itself be incriminating.

**Checks and Other Financial Instruments**

As the scheme grows, illicit payments are often made by normal business check, cashier’s check, or wire transfer. Disguised payments on the payer’s books appear as some sort of legitimate business expense, often as consulting fees. Payments can be made directly or through an intermediary.

**Hidden Interests**

In the latter stages of sophisticated schemes, the payer might give a hidden interest in a joint venture or other profit-making enterprise. The recipient’s interest might be concealed through a straw nominee, hidden in a trust or other business entity, or merely included by an undocumented verbal agreement. Such arrangements are very difficult to detect, and even if identified, proof of corrupt intent might be difficult to demonstrate.

**Loans**

Three types of “loans” often turn up in fraud cases:

- A prior outright payment falsely described as an innocent loan.
- Payments on a legitimate loan guaranteed or actually made by someone else.
- An actual loan made on favorable terms, such as interest-free.
Payment of Credit Card Bills
The recipient’s transportation, vacation, and entertainment expenses might be paid with the payer’s credit card, or the recipient might forward his own credit card bills to the payer for payment. In some instances, the payer simply lets the recipient carry and uses the payer’s card.

Transfers at Other than Fair Market Value
The corrupt payer might sell or lease property to the recipient at far less than its market value, or might agree to buy or rent property at inflated prices. The recipient might also “sell” an asset to the payer, but retain title or the use of the property.

Promises of Favorable Treatment
Promises of favorable treatment commonly take the following forms:
- A payer might promise a governmental official lucrative employment when the recipient leaves government service.
- An executive leaving a private company for a related government position might be given favorable or inflated retirement and separation benefits.
- The spouse or other relative of the intended recipient might also be employed by the payer company at an inflated salary or with little actual responsibility.

FINANCIAL STATEMENT FRAUD
Fraudulent financial statements typically takes the form of:
- Overstated assets or revenue
- Understated liabilities and expenses

Overstating assets and revenues falsely reflects a financially stronger company by inclusion of fictitious asset costs or artificial revenues.

Understated liabilities and expenses are shown through exclusion of costs or financial obligations.

Both methods result in increased equity and net worth for the company. This overstatement or understatement results in increased earnings per share or partnership profit interests, or a more stable picture of the company’s true situation. To demonstrate these over and understatements, the schemes typically used have been divided into five classes. Because the maintenance of financial records involves a double-entry system, fraudulent accounting entries always affect at least two accounts and, therefore, at least two categories on the financial statements. While the areas described below reflect their financial statement classifications, keep in mind that the other side of the fraudulent transaction exists elsewhere.

It is common for schemes to involve a combination of several methods. The five classifications of financial statement fraud schemes are as follows:
- Fictitious revenues
- Timing differences
- Improper asset valuations
- Concealed liabilities and expenses
- Improper disclosures

Fictitious Revenues
Fictitious or fabricated revenues involve the recording of sales of goods or services that did not occur. Fictitious sales most often involve fake or phantom customers, but can also involve legitimate customers. For example, a fictitious
Invoice can be prepared (but not mailed) for a legitimate customer although the goods are not delivered or the services are not rendered. At the beginning of the next accounting period, the sale might be reversed to help conceal the fraud, but this may lead to a revenue shortfall in the new period, creating the need for more fictitious sales. Another method is to use legitimate customers and artificially inflate or alter invoices reflecting higher amounts or quantities than are actually sold.

**Timing Differences (Including Premature Revenue Recognition)**

Financial statement fraud might also involve timing differences, that is, the recording of revenues or expenses in improper periods. This can be done to shift revenues or expenses between one period and the next, increasing or decreasing earnings as desired.

**Improper Asset Valuation**

Under the “lower of cost or market value” rule, where an asset’s cost exceeds its current market value (as happens often with obsolete technology), the asset must be written down to market value. With the exception of certain securities, asset values are generally not increased to reflect current market value. It is often necessary to use estimates in accounting. For example, estimates are used in determining the residual value and the useful life of a depreciable asset, the uncollectible portion of accounts receivable, or the excess or obsolete portion of inventory. Whenever estimates are used, there is an additional opportunity for fraud by manipulating those estimates.

Many schemes are used to inflate current assets at the expense of long-term assets. The net effect is seen in the current ratio.

**Concealed Liabilities and Expenses**

Understating liabilities and expenses is one of the ways financial statements can be manipulated to make a company appear more profitable than it actually is. Because pre-tax income will increase by the full amount of the expense or liability not recorded, this financial statement fraud method can have a significant impact on reported earnings with relatively little effort by the fraudster. It is much easier to commit than falsifying sales transactions.

Missing transactions can also be harder for auditors to detect than improperly recorded ones since the missing transactions leave no audit trail.

Common methods for concealing liabilities and expenses include:

- Liability/expense omissions
- Capitalized expenses

**Improper Disclosures**

Accounting principles require that financial statements include all the information necessary to prevent a reasonably discerning user of the financial statements from being misled. The notes should include narrative disclosures, supporting schedules, and any other information required to avoid misleading potential investors, creditors, or any other users of the financial statements.

Management has an obligation to disclose all significant information appropriately in the financial statements and in management’s discussion and analysis. In addition, the disclosed information must not be misleading. Improper disclosures relating to financial statement fraud may involve the following:

- Liability omissions
- Subsequent events
- Related-party transactions
- Accounting changes
ASSET MISAPPROPRIATIONS
These types of schemes are by far the most common of all occupational frauds. There are three major categories of asset misappropriation schemes:

- Cash receipts
- Fraudulent disbursements of cash
- Theft of inventory and other non-cash assets.

Cash Receipt Schemes
Cash is the focal point of most accounting entries. Cash, both on deposit in banks and on hand as petty cash, can be misappropriated through many different schemes. These schemes can be either on-book or off-book, depending on where they occur.

Cash receipts schemes fall into two categories, **skimming** and **larceny**. The difference in the two types of fraud depends completely on when the cash is stolen. Cash larceny is the theft of money that has *already appeared* on a victim organization’s books, while skimming is the theft of cash that has *not yet been recorded* in the accounting system. The way in which an employee extracts the cash may be exactly the same for a cash larceny or skimming scheme.

**Skimming:**
Skimming is the removal of cash from a victim entity prior to its entry in an accounting system. Employees who skim from their companies steal sales or receivables before they are recorded in the company books. Skimming schemes are known as “off-book” frauds, meaning money is stolen before it is recorded in the victim organization’s accounts. This aspect of skimming schemes means they leave no direct audit trail. Because the stolen funds are never recorded, the victim organization may not be aware that the cash was ever received. Consequently, it may be very difficult to detect that the money has been stolen. This is the prime advantage of a skimming scheme to the fraudster.

**Sales Skimming**
The most basic skimming scheme occurs when an employee sells goods or services to a customer, collects the customer’s payment, but makes no record of the sale. The employee simply pockets the money received from the customer instead of turning it over to his employer.

In Government Departments, sales may refer to fees and other collections from customers and clients charged by the Department for services provided:

This can be of two types:
1. Unrecorded Sales
2. Understated Sales

The Unrecorded Sales can be of the following types:

**Register Manipulation**
Some employees might ring a “no sale” or other non-cash transaction to mask the theft of sales. The false transaction is entered on the register so that it appears a sale is being rung up. The perpetrator opens the register drawer and pretends to place the cash he has just received in the drawer, but in reality he pockets the cash. To the casual observer it looks as though the sale is being properly recorded.
Skimming During Non-business Hours
Another way to skim unrecorded sales is to conduct sales during non-business hours. For instance, some employees will open stores on weekends or after hours without the knowledge of the owners. They can pocket the proceeds of all sales made during these times because the owners have no idea that their stores are even open for business.

Skimming of Off-Site Sales
Several industries rely on remote salespersons to generate revenue. The fact that these employees are largely unsupervised puts them in a good position to skim revenues.

Poor Collection Procedures
Poor collection and recording procedures can make it easy for an employee to skim sales or receivables.

Understated Sales
Understated sales work differently because the transaction in question is posted to the books, but for a lower amount than what the perpetrator actually collected. (See “Understated Sales” flowchart.) One way employees commit understated sales schemes is by altering receipts or preparing false receipts that misstate the amount of sales.

False Discounts
Those employees with the authority to grant discounts may utilize this authority to skim sales and receivables. In a false discount skimming scheme, an employee accepts full payment for an item, but records the transaction as if the customer had been given a discount.

Theft of Checks Received Through the Mail
Checks received through the mail are a frequent target of employees seeking illicit gains. Theft of incoming checks usually occurs when a single employee is in charge of opening the mail and recording the receipt of payments. This employee simply steals one or more incoming checks instead of posting them to customer accounts. When the task of receiving and recording incoming payments is left to a single person, it is all too easy for that employee to make off with an occasional check.

Check for Currency Substitutions
The intelligent criminal will generally prefer to steal currency rather than check if given the opportunity. The reasons why are obvious. First, currency is harder to trace than a check. A cashed check eventually returns to the person who wrote it and may provide evidence of who cashed it or where it was spent. Endorsements, bank stamps, and so forth may indicate the identity of the thief. Currency, on the other hand, disappears into the economy once it is stolen.

The second reason that currency is preferable to a check is the difficulty in converting the check. When currency is stolen it can be spent immediately. A check, on the other hand, must be endorsed and cashed or deposited before the thief can put his hands on the money it represents. To avoid this problem, employees who steal unrecorded check will frequently substitute them for receipted currency.

Skimming Receivables
It is generally more difficult to conceal the skimming of receivables than the skimming of sales because receivables payments are expected. The victim organization knows the customer owes money and it is waiting for the payment to arrive. When unrecorded sales are skimmed, it is as though the sale never existed. But when receivables are skimmed, the absence of the payment appears on the books as a delinquent account. In order to conceal a skimmed receivable, a perpetrator must somehow account for the payment that was due to the company but never received.
Forcing Account Balances or Destroying Transaction Records
Among the most dangerous receivables skimming schemes are those in which the perpetrator is in charge of collecting and posting payments. If a fraudster has a hand in both ends of the receipting process, he or she can falsify records to conceal the theft of receivables payments.

Lapping
Lapping customer payments is one of the most common methods of concealing receivables skimming. Lapping is the crediting of one account through the abstraction of money from another account. It is the fraudster’s version of “robbing Peter to pay Paul.”

Stolen Statements
When employees skim receivables, they may let the targeted accounts age instead of attempting to force the balances. In other words, they steal an incoming check intended as payment on a receivable, and they simply act as if the check never arrived. This method keeps the victim organization’s cash account in balance, because the stolen payment is never posted.

False Account Entries
Intercepting the customer’s statements will keep him in the dark as to the status of his account, but as long as the customer’s payments are being skimmed, his account is slipping further and further past due. The perpetrator must bring the account back up-to-date in order to conceal his crime. Lapping is one way to keep accounts current as the employee skims from them. Another way is to make false entries in the victim organization’s accounting system.

Debits to Expense Accounts
An employee might conceal the skimming of funds by making unsupported entries in the victim company’s books. If a payment is made on a receivable, for instance, the proper entry is a debit to cash and a credit to the receivable. Instead of debiting cash, the employee might choose to debit an expense account. This transaction still keeps the company’s books in balance, but the incoming cash is never recorded. In addition, the customer’s receivable account is credited, so it will not become delinquent.

Debits to Aging or Fictitious Receivables
The same method discussed above is used when employees debit existing or fictitious accounts receivable in order to conceal skimmed cash. For example, an employee who has skimmed one customer’s payments might add the stolen amounts to aging accounts which are soon to be written off as uncollectible or to very large accounts where a small debit might go unnoticed.

Some perpetrators also set up completely fictitious accounts and debit them for the cost of skimmed receivables. The employees then simply wait for the fictitious receivables to age and be written off as uncollectible. In the meantime, the fictitious receivables carry the cost of a skimming scheme where it will not be detected.

Write off Account Balances
Some employees cover their skimming by posting entries to contra revenue accounts such as “discounts and allowances.” If, for instance, an employee intercepts a $1,000 payment, he would create a $1,000 “discount” on the account to compensate for the missing money. Another account that might be used in this type of concealment is the bad debts expense account.
Inventory Padding
A problem for fraudsters in some skimming schemes is the victim organization’s inventory. Off-book sales of goods will always leave an inventory shortage and a corresponding rise in the cost of goods sold.

When a sale of goods is made, the physical inventory is reduced by the amount of merchandise sold. For instance, when a retailer sells a pair of shoes there is one less pair of shoes in the stock room. If this sale is not recorded, however, the shoes are not removed from the perpetual inventory records. Thus, there is one less pair of shoes on hand than in the perpetual inventory. A reduction in the physical inventory without a corresponding reduction in the perpetual inventory is known as “shrinkage.”

Cash Larceny
In the occupational fraud setting, a cash larceny may be defined as the intentional taking of an employer’s cash (the term cash includes both currency and checks without the consent and against the will of the employer.

A cash larceny scheme can take place in any circumstance in which an employee has access to cash. Every company must deal with the receipt, deposit, and distribution of cash, so every company is potentially vulnerable to a cash larceny scheme. While the circumstances in which an employee might steal cash are nearly limitless, most larceny schemes involve the theft of incoming cash, currency on hand (in a cash register, cash box, etc.), or theft of cash from the victim organization’s bank deposits.

Theft of Cash from the Register
A large percentage of cash larceny schemes occur at the cash register, and for good reason—the register is usually where the cash is. The register (or similar cash collection points like cash drawers or cash boxes) is usually the most common point of access to cash for employees, so it is understandable that this is where larceny schemes frequently occur.

Reversing Transactions
Some employees conceal cash larceny by processing reversing transactions, which cause the register tape to reconcile to the amount of cash on hand after the theft. By processing false voids or refunds, an employee can reduce the cash balance reflected on the register tape.

Register Manipulation
Instead of using reversing entries, an employee might manually alter the register tape. Again, the purpose of this activity is to force a balance between the cash on hand and the actual cash received. An employee might use white-out to cover up a sale whose proceeds were stolen, or he might simply cross out or alter the numbers on the tape so that the register total and the cash drawer balance. This type of concealment is not common because, in general, the alterations will be noticeable.

Altering Cash Counts
Another method for concealing cash larceny is to alter the cash counts on registers. When cash from a register is totaled and prepared for deposit, an employee simply records the wrong amount so that the cash on hand appears to balance with the total on the register tape. Obviously, employees who deal with the receipt of cash should not be charged with verifying the amount of cash on hand in their own register, but this control is often overlooked.

Destroying Register Tapes
If the fraudster cannot make the cash and the tape balance, the next best thing is to prevent others from computing the totals and discovering the imbalance. Employees who are stealing from the register sometimes destroy detail tapes that
would implicate them in a crime. When detail tapes are missing or defaced, it may be because someone is trying to conceal a fraud.

Other Larceny of Sales and Receivables
Not all receipts arrive via the cash register. Employees can just as easily steal money received at other points. One of the more common methods is to take checks received through the mail, post the payments to the accounting system, but steal the checks.

Cash Larceny from the Deposit
At some point in every revenue-generating business, someone must physically take the company’s currency and checks to the bank. This person or persons, left alone literally holding the bag, will have an opportunity to take a portion of the money prior to depositing it into the company’s accounts.

Deposit Lapping
One method that fraudsters sometimes use to conceal cash larceny from the deposit is lapping. Lapping occurs when an employee steals the deposit from day one and replaces it with day two’s deposit. Day two is replaced with day three, and so on. The perpetrator is always one day behind, but as long as no one demands an up-to-the-minute reconciliation of the deposits to the bank statement—and if daily receipts do not drop precipitously—he may be able to avoid detection for a period of time. Lapping is discussed in more detail in the Skimming section.

Deposits in Transit
A final strategy used to conceal stolen deposits is to carry the missing money as deposits in transit, which are a way of accounting for discrepancies between the company’s records and the bank statement.

Fraudulent Disbursements
In fraudulent disbursement schemes, an employee makes a distribution of company funds for a dishonest purpose. Examples of fraudulent disbursements include forging company checks, the submission of false invoices, doctoring timecards, and so forth. On their face, the fraudulent disbursements do not appear any different from valid disbursements of cash.

For instance, when an employee runs a bogus invoice through the accounts payable system, the victim organization cuts a check for the bad invoice right along with all the legitimate payments it makes. The perpetrator has taken money from his employer in such a way that it appears to be a normal disbursement of cash. Someone might notice the fraud based on the amount, recipient, or destination of the payment, but the method of payment is legitimate.

Register Disbursement Schemes
Fraudulent disbursements at the cash register are different from the other schemes that often take place at the register, such as skimming and cash larceny. When cash is stolen as part of a register disbursement scheme, the removal of the cash is recorded on the register tape. A false transaction is entered so it appears that the disbursement of money was legitimate.

There are two basic register disbursements schemes: false refunds and false voids. While the schemes are largely similar, there are a few differences between the two of them.
False Refunds
A refund is processed at the register when a customer returns an item of merchandise that was purchased from the store. The transaction that is entered on the register indicates the merchandise is being replaced in the store’s inventory and the purchase price is being returned to the customer. In other words, a refund shows cash being disbursed from the register to the customer.

Fictitious Refunds
In a fictitious refund scheme, an employee processes a transaction as if a customer were returning merchandise, even though there is no actual return.

False Voids
Fictitious voids are similar to refund schemes in that they make fraudulent disbursements from the register appear to be legitimate. When a sale is voided on a register, a copy of the customer’s receipt is usually attached to a void slip, along with the signature or initials of a manager indicating that the transaction has been approved.

Check Tampering Schemes
Check tampering is unique among the fraudulent disbursement schemes because it is the one group 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 organization such as an invoice or a timecard. The false document represents a claim for payment and causes the victim organization to issue a check that the perpetrator can convert.

Forged Maker Schemes
A forged maker scheme 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.

Forged Endorsement Schemes
Forged endorsements are those check tampering schemes in which an employee intercepts a company check intended to pay a third party and converts the check by endorsing it in the third party’s name. In some cases the employee also signs his own name as a second endorser.

Altered Payee Schemes
The second type of intercepted check scheme is the altered payee scheme. This is a form of check tampering 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 “Altered Payee Schemes” flowchart.) The employee inserts his own name, the name of an accomplice, or the name of a fictitious entity on the payee line of the check. The alteration essentially makes the check payable to the employee (or an accomplice), so there is no need to forge an endorsement and no need to obtain false identification.

Concealing Check Tampering Schemes
Most check tampering schemes do not consist of a single occurrence but instead continue over a period of time. Therefore, concealing the fraud is arguably the most important aspect of the scheme. If an employee 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, which make concealment the key to the crime.
Authorized Maker Schemes
The final check tampering scheme, the authorized maker scheme, may be the most difficult to defend against. An authorized maker scheme occurs when an employee with signature authority on a company account writes fraudulent checks for his own benefit and signs his own name as the maker.

Billing Schemes
The asset misappropriation schemes discussed up to this point—skimming, larceny, register schemes, and check tampering—all require the perpetrator of the scheme to physically take cash or checks from his employer. The next three sections will cover a different kind of asset misappropriation scheme, one which allows the perpetrator to misappropriate company funds without ever actually handling cash or checks while at work. These succeed by making a false claim for payment upon the victim organization. This group consists of billing schemes (which attack the purchasing function of a company), payroll schemes, and expense reimbursement schemes. The most common of these is the billing scheme.

Shell Company
Shell companies are fictitious entities created for the purpose of committing fraud. They may be nothing more than a fabricated name and a post office box that an employee uses to collect disbursements from false billings. However, since the checks received will be made out in the name of the shell company, the perpetrator will normally also set up a bank account in his new company’s name, so he can deposit and cash the fraudulent checks.

Invoicing Via Non-accomplice Vendors

Pay-and-Return Schemes
Instead of using shell companies in their over-billing schemes, some employees generate fraudulent disbursements by using the invoices of legitimate third-party vendors who are not a part of the fraud scheme. In pay-and-return schemes, employees intentionally mishandle payments which are owed to legitimate vendors. One way to do this is to purposely double-pay an invoice. For instance, a clerk might intentionally pay an invoice twice, then call the vendor and request that one of the checks be returned. The clerk then intercepts the returned check.

Personal Purchases on Credit Cards or Other Company Accounts
Instead of running false invoices through accounts payable, some employees make personal purchases on company credit cards or on running accounts with vendors. As with invoicing schemes, the key to getting away with a false credit card purchase is avoiding detection. Unlike invoicing schemes, however, prior approval for these purchases is not required. An employee with a company credit card can buy an item merely by signing his name (or forging someone else’s) at the time of purchase. Later review of the credit card statement, however, may detect the fraudulent purchase. Unfortunately, many high-level employees approve their own credit card expenses, making it very easy to carry out a purchasing scheme.

Payroll Fraud Schemes
Payroll schemes are similar to billing schemes. The perpetrators of these frauds produce false documents, which cause the victim company to unknowingly make a fraudulent disbursement. In billing schemes, the false document is usually an invoice (coupled, perhaps, with false receiving reports, purchase orders, and purchase authorizations). In payroll schemes, the perpetrator typically falsifies a timecard or alters information in the payroll records. The major difference between payroll schemes and billing schemes is that payroll frauds involve disbursements to employees rather than to external parties. The most common payroll frauds are ghost employee schemes, falsified hours and salary schemes, and commission schemes.
Ghost Employees
The term ghost employee refers to someone on the payroll who does not actually work for the victim company. Through the falsification of personnel or payroll records a fraudster causes pay checks to be generated to a ghost. The fraudster or an accomplice then converts these pay checks. The ghost employee may be a fictitious person or a real individual who simply does not work for the victim employer. When the ghost is a real person, it is often a friend or relative of the perpetrator.

In order for a ghost employee scheme to work, four things must happen: (1) the ghost must be added to the payroll, (2) timekeeping and wage rate information must be collected, (3) a pay check must be issued to the ghost, and (4) the check must be delivered to the perpetrator or an accomplice.

Falsified Hours and Salary
The most common method of misappropriating funds from the payroll is the overpayment of wages. For hourly employees, the size of a pay check is based on two factors: the number of hours worked and the rate of pay. It is therefore obvious that for an hourly employee to fraudulently increase the size of his pay check, he must either falsify the number of hours he has worked or change his wage rate. Since salaried employees do not receive compensation based on their time at work, in most cases these employees generate fraudulent wages by increasing their rates of pay.

Commission Schemes
Commission is a form of compensation calculated as a percentage of the amount of transactions a salesperson or other employee generates. It is a unique form of compensation that is not based on hours worked or a set yearly salary, but rather on an employee’s revenue output. A commissioned employee’s wages are based on two factors, the amount of sales he generates and the percentage of those sales he is paid. In other words, there are two ways an employee on commission can fraudulently increase his pay: (1) falsify the amount of sales made, or (2) increase his rate of commission.

Expense Reimbursement Schemes
Employees can manipulate an organization’s expense reimbursement procedures to generate fraudulent disbursements. Expense reimbursements are usually paid by the company in the following manner. An employee submits a report detailing an expense incurred for a business purpose, such as a business lunch with a client, airfare, hotel bills associated with business travel, and so forth. In preparing an expense report, an employee is usually required to explain the business purpose for the expense, as well as the time, date, and location in which it was incurred. Support documentation for the expense, typically a receipt, should be attached to the report. In some cases cancelled checks written by the employee or copies of a personal credit card statement showing the expense are allowed in lieu of receipts. The report must usually be authorized by a supervisor in order for the expense to be reimbursed.

The four most common types of expense reimbursement schemes are mischaracterized expenses, overstated expenses, fictitious expenses, and multiple reimbursements.

Mischaracterized Expense Reimbursements
Most companies only reimburse certain expenses of their employees. Which expenses a company will pay for depends to an extent upon policy, but in general, business-related travel, lodging, and meals are reimbursed. One of the most basic expense reimbursement schemes is perpetrated by simply requesting reimbursement for a personal expense by claiming that the expense is business related.
Overstated Expense Reimbursements
Instead of seeking reimbursement for personal expenses, some employees overstate the cost of actual business expenses.

Fictitious Expense Reimbursements
Employees sometimes seek reimbursement for wholly fictitious expenses. Instead of overstating a real business expense or seeking reimbursement for a personal expense, an employee just invents an expense and requests that it be reimbursed.

Multiple Reimbursements
The least common of the expense reimbursement schemes is the multiple reimbursements. This type of fraud involves the submission of a single expense several times. The most frequent example of a multiple reimbursement scheme is the submission of several types of support for the same expense.

Inventory and Other Assets
Employees target inventory, equipment, supplies, and other non-cash assets for theft in a number of ways. These schemes can range from stealing a box of pens to the theft of millions of dollars’ worth of company equipment. The term inventory and other assets are meant to encompass the misappropriation schemes involving any assets held by a company other than cash.

There are basically two ways a person can misappropriate a company asset. The asset can be misused or it can be stolen. Simple misuse is obviously the less egregious of the two.

Misuse:
Assets that are misused but not stolen typically include company vehicles, company supplies, computers, and other office equipment.

Theft of Inventory and Other Assets
While the misuse of company property might be a problem, the theft of company property is obviously of greater concern. Losses resulting from larceny of company assets can run into the millions of dollars. Most schemes where inventory and other non-cash assets are stolen fall into one of four categories: larceny schemes, asset requisition and transfer schemes, purchasing and receiving schemes, and false shipment schemes.

Larceny:
The term larceny is meant to refer to the most basic type of inventory theft, the schemes in which an employee simply takes inventory from the company premises without attempting to conceal the theft in the books and records.

The False Sale
In many cases, corrupt employees utilize outside accomplices to help steal inventory. The fake sale is one method that depends upon an accomplice. Like most inventory thefts, the fake sale is not complicated. The accomplice of the employee-fraudster pretends to buy merchandise, but the employee does not ring up the sale. The accomplice takes the merchandise without paying for it. To a casual observer, it will appear that the transaction is a normal sale. The employee bags the merchandise, and may act as though a transaction is being entered on the register, but in fact, the “sale” is not recorded. The accomplice may even pass a nominal amount of money to the employee to complete the illusion. A related scheme occurs when an employee sells merchandise to an accomplice at an unauthorized discount.
Asset Requisitions and Transfers
Asset requisitions and other documents that allow non-cash assets to be moved from one location in a company to another can be used to facilitate the theft of those assets. Employees use internal transfer paperwork to gain access to merchandise which they otherwise might not be able to handle without raising suspicion. These documents do not account for missing merchandise the way false sales do, but they allow a person to move the assets from one location to another. In the process of this movement, the thief steals the merchandise.

Purchasing and Receiving Schemes
Dishonest employees can also manipulate the purchasing and receiving functions of a company to facilitate the theft of inventory and other assets. It might seem that any purchasing scheme should fall under the heading of false billings, which were discussed earlier. There is, however, a distinction between the purchasing schemes that are classified as false billings and those that are classified as non-cash misappropriations.

Concealing Inventory Shrinkage
When inventory is stolen, the key concealment issue for the perpetrator is shrinkage. Inventory shrinkage is the unaccounted-for reduction in the company’s inventory that results from theft. For instance, assume a computer retailer has 1,000 computers in stock. After work one day, an employee loads ten computers into a truck and takes them home. Now the company only has 990 computers, but since there is no record that the employee took ten computers, the inventory records still show 1,000 units on hand. The company has experienced inventory shrinkage in the amount of 10 computers.