PART I

Introduction

In the world of commerce, organizations incur costs to produce and sell their products or services. These costs run the gamut: labor, taxes, advertising, occupancy, raw materials, research and development, and, yes, fraud and abuse. The latter cost, however, is fundamentally different from the former: the true expense of fraud and abuse is hidden, even if it is reflected in the profit-and-loss figures.

For example, suppose a company's advertising expense is $1.2 million. But unknown to the company's executives, the marketing manager is colluding with an outside ad agency and has accepted $300,000 in kickbacks to steer business to that firm. That means the true advertising expense is overstated by at least the amount of the kickbacks – if not more. The result, of course, is that $300,000 comes directly off the bottom line, out of the pockets of the investors and the workforce. Similarly, if a warehouse foreman is stealing inventory or an accounting clerk is skimming customer payments, the company suffers a loss – one it likely does not know about, but one that must be absorbed somewhere.

The truth is, fraud can occur in virtually any organization. If an organization employs individuals, at some point one or more of those individuals will attempt to lie, cheat, or steal from the company for personal gain. So this hidden cost – one that offers no benefit to the company and, in fact, causes numerous kinds of damage to the company even beyond the direct financial consequence – is one that all organizations, in all countries, in all industries, and of all sizes, will encounter. However, the risk of fraud is most significant – that is, it has the potential to cause the most damage – for organizations that are unaware of, ignore, or underestimate whether and how fraud can occur within their operations.

The risk is also evolving due to changes in technology, globalization, regulatory environments, and other factors. These changes can present challenges to those charged with preventing, detecting, investigating, and responding to fraud. Nonetheless, the concepts behind fraud remain timeless – the perpetrators seek to trick victims out of financial or other resources for personal gain. As a result, the foundational concepts in fighting fraud are still effective.

WHAT IS FRAUD?

The term *fraud* is commonly used to encompass a broad range of schemes: employee embezzlement, identity theft, corrupt government officials, cybercrimes, fraud against the elderly, health care schemes, loan fraud, bid rigging, credit card skimming, counterfeit goods, and dozens of others. While the range of schemes that fall under the

Portions of this chapter are adapted from the following Association of Certified Fraud Examiners (ACFE) publications: *Ten Common External Threats to Your Organization*, the materials for the *Auditing for Internal Fraud* and *Controlling the Risk of Asset Misappropriation* seminars, and the "Financial Transactions" and "Fraud Schemes" sections of the *Fraud Examiners Manual*.

umbrella of fraud is extensive, a general definition and an understanding of the common elements of these schemes are useful in preventing and detecting these acts.

Fraud can be generally defined as any crime for gain that uses deception as its principal modus operandi. Consequently, fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means. As such, all types of fraud have the following common elements:

- A material false statement (i.e., a misrepresentation)
- Knowledge that the statement was false when it was uttered (i.e., intent)
- The victim's reliance on the false statement
- Damages resulting from the victim's reliance on the false statement

Components of Fraud

An act of fraud normally involves three components, or steps:

1. The act
2. The concealment
3. The conversion

To successfully perpetrate a fraud, offenders generally must complete all three steps: they must commit the act, conceal the act, and convert the proceeds for their personal benefit or the benefit of another party.

The Act

The fraud act is normally the theft or deception – the action that leads to the gain the perpetrator is seeking.

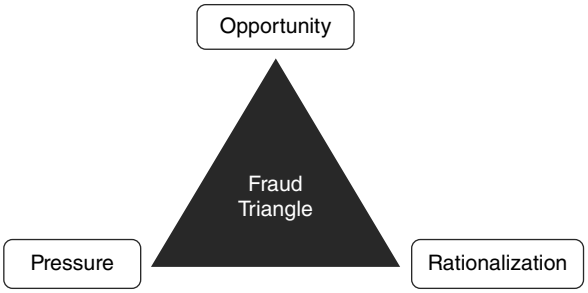
The Concealment

Once the perpetrator accomplishes the act, the individual typically makes efforts to conceal it. Concealment is a cornerstone of fraud. As opposed to traditional criminals, who make no effort to conceal their crimes, fraud perpetrators typically take steps to keep their victims ignorant. For example, in the case of the theft of cash, falsifying the balance in the cash account would constitute concealment. Although some individuals commit fraud without attempting to conceal it (e.g., taking cash from a register drawer with no attempt to cover the theft), fraud investigations generally uncover such schemes quickly, reducing the perpetrator's chances of repeating the offense and increasing the likelihood of being caught.

The Conversion

After completing and concealing the fraudulent act, the perpetrator must convert the ill-gotten gains for the individual's own benefit or the benefit of another party. In the case of the theft of petty cash, conversion generally occurs when the perpetrator deposits the funds into the individual's own account or makes a purchase with the stolen funds.

Exhibit 1.1 The Fraud Triangle



WHAT FACTORS LEAD TO FRAUD?

Individuals and groups perpetrate frauds to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage. However, most people who commit fraud against their employers are not career criminals. In fact, the vast majority are trusted employees who have no criminal history and who do not consider themselves to be lawbreakers. So the question is: What factors cause these otherwise normal, law-abiding individuals to commit fraud?

The Fraud Triangle

The best and most widely accepted model for explaining why people commit fraud is the Fraud Triangle. (See Exhibit 1.1.) Dr. Donald Cressey, a criminologist whose research focused on embezzlers (whom he called *trust violators*), developed this model.

According to Cressey, three factors must be present at the same time for an ordinary person to commit fraud:

1. Pressure
2. Perceived opportunity
3. Rationalization

Pressure

The first leg of the Fraud Triangle represents *pressure*. This is what motivates the crime in the first place. The individuals might have a financial problem they are unable to solve through legitimate means, so they begin to consider committing an illegal act, such as stealing cash or falsifying a financial statement. The pressure can be personal (e.g., too deep in personal debt) or professional (e.g., job or business in jeopardy).

Examples of pressures that commonly lead to fraud include:

- Inability to pay one's bills
- Drug or gambling addiction
- Need to meet earnings forecast to sustain investor confidence
- Need to meet productivity targets at work
- Desire for status symbols, such as a bigger house or nicer car

Opportunity

The second leg of the Fraud Triangle is *opportunity*, sometimes referred to as *perceived opportunity*, which defines the method by which an individual can commit the crime. The person must see some way to use (abuse) a position of trust to solve a financial problem with a low perceived risk of getting caught.

It is critical that fraud perpetrators believe they can solve their problem in secret. Many people commit white-collar crimes to maintain their social status. For instance, they might steal to conceal a drug problem, pay off debts, or acquire expensive cars or houses. If perpetrators are caught embezzling or falsifying financial information, it hurts their status at least as much as the underlying problem they were trying to conceal. So the fraudster has to not only be able to steal funds, but also be able to do it in such a way that the person is unlikely to be caught and the crime itself will go undetected.

Rationalization

The third leg of the Fraud Triangle is *rationalization*. The majority of fraudsters are first-time offenders with no criminal past. They do not view themselves as criminals. They see themselves as ordinary, honest people caught in a bad set of circumstances. Consequently, fraudsters must justify their crime to themselves in a way that makes it an acceptable or justifiable act; that is, they must be able to rationalize their scheme. Common rationalizations include the following:

- "I was only borrowing the money."
- "I was entitled to the money."
- "I had to steal to provide for my family."
- "I was underpaid; my employer cheated me."
- "My employer is dishonest to others and deserved to be defrauded."

Limitations of the Fraud Triangle

The Fraud Triangle applies to most embezzlers and occupational fraudsters, but it does not apply to the *predatory employees* – those who take a job with the premeditated intent of stealing from their employer.

Also, while a rationalization is necessary for most people to begin a fraud, perpetrators often abandon rationalization after committing the initial act. Most frauds are not one-time events. They usually start as small thefts or misstatements and gradually increase in size and frequency. As the perpetrator repeats the act, it becomes easier to justify, until eventually there is no longer a need for justification.

Why Sanctions Alone Don't Deter Fraud

The Fraud Triangle also implies that simply punishing people who are caught committing fraud is not an effective deterrent. There are several reasons why:

- Fraud perpetrators commit their crimes when there is a perceived opportunity to solve their problems in secret. In other words, they do not anticipate getting caught.

The threat of sanctions does not carry significant weight because they never expect to face them.
- Fraud perpetrators rationalize their conduct so that it seems legal or justified. Thus, they do not see their actions as something that warrants sanctioning.
- Because status is frequently the motivation for individuals to commit fraud, the greatest threat they face is the detection of their crime, which would result in loss of status. Any formal sanctions that follow are a secondary consideration.

Control Weaknesses

On the organizational side, control weaknesses create the opportunity for fraud to occur. While this is only one factor in the Fraud Triangle, it is the element of fraud that organizational leaders typically have the greatest ability to control, and thus tend to focus most of their efforts and resources on. However, deficiencies in such controls are a notable factor in many frauds that occur. According to the 2018 *Report to the Nations on Occupational Fraud and Abuse*, published by the Association of Certified Fraud Examiners (ACFE), nearly half of all occupational fraud cases occur primarily due to a lack of internal controls or an override of existing controls. (Specific control activities to prevent and detect fraud are discussed in detail in Chapters 3 and 4.)

THE IMPACT OF FRAUD

All Organizations Are Susceptible to Fraud

Fraud is an uncomfortable risk to address. Most directors, executives, and managers would much rather believe that their organization's employees would never steal from the company. However, companies with management that is least attentive to the potential for fraud are at the greatest risk.

The truth is that fraud occurs in all organizations, regardless of size, industry, or location. No entity is immune. The fundamental reason for this is that fraud is a human problem, not an accounting problem. As long as organizations are employing individuals to perform the business functions, the risk for fraud exists. Only by recognizing and proactively and continually addressing this risk can organizations mitigate the potentially devastating impact.

The High Cost of Occupational Fraud

In its 2018 *Report to the Nations on Occupational Fraud and Abuse*, the ACFE analyzed data from 2,690 cases of occupational fraud that were investigated worldwide between January 2016 and October 2017. To compile this information, the ACFE surveyed the Certified Fraud Examiners (CFEs) who investigated those cases about the costs, methods, victims, and perpetrators involved in the frauds. The fraud cases in the study came from 125 nations – with more than half of the cases occurring in countries outside the US – providing a truly global view into the plague of occupational fraud.

Survey participants estimated that the typical organization loses 5% of its annual revenue to fraud. Applied to the estimated 2016 gross world product,[1] this figure translates to a potential total fraud loss of nearly US $4 trillion worldwide. Further, the median loss caused by the occupational fraud cases in the study was US $130,000, with 22% of the frauds resulting in losses of at least US $1 million.

The Indirect Costs

The impact of a fraud extends well beyond the actual dollar amount stolen by the perpetrator or the amount of the financial statement manipulation. In the wake of a fraud, employees might lose confidence in the security of their jobs, leading to loss of productivity. Moreover, the company's image is tarnished, decreasing its reputation in the eyes of existing and potential customers and vendors. In some instances, competitors have even used reports of fraud as a recruiting advantage in attracting top talent away from the victim company.

TYPES OF FRAUD AFFECTING ORGANIZATIONS

Occupational Fraud

Occupational fraud, also called *internal fraud*, is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets." Simply stated, occupational fraud occurs when an employee, manager, or executive commits fraud against the employer. *Occupational fraud* is commonly synonymous with terms like *employee fraud* or *embezzlement*, although the term *occupational fraud* is broader and better reflects the full range of employee misconduct through which organizations lose money.

Although perpetrators are increasingly embracing technology and new approaches in committing and concealing these types of schemes, the methodologies used in such frauds generally fall into clear, time-tested categories. To identify and delineate the schemes, the ACFE developed the *Occupational Fraud and Abuse Classification System*, also known as the *Fraud Tree*. (See Exhibit 1.2.) This organization of schemes is especially helpful in designing, implementing, and assessing internal controls and other activities undertaken to manage the risk of fraud.

As illustrated in the Fraud Tree, there are three primary types of occupational fraud: asset misappropriation, corruption, and financial statement fraud; each of these types also has several distinct categories of subschemes.

The ACFE's 2018 *Report to the Nations* shows that, of the three primary categories of occupational fraud, asset misappropriation schemes are by far the most common and the least costly. In contrast, financial statement fraud schemes cause the greatest damage, but occur in just 10% of occupational fraud schemes. Corruption schemes fall in the middle in terms of both frequency and financial impact. (See Exhibits 1.3 and 1.4.)

Asset Misappropriation

Asset misappropriation schemes are frauds in which an employee misappropriates the organization's resources (e.g., cash, inventory, or proprietary information) for personal

Exhibit 1.2 The Fraud Tree

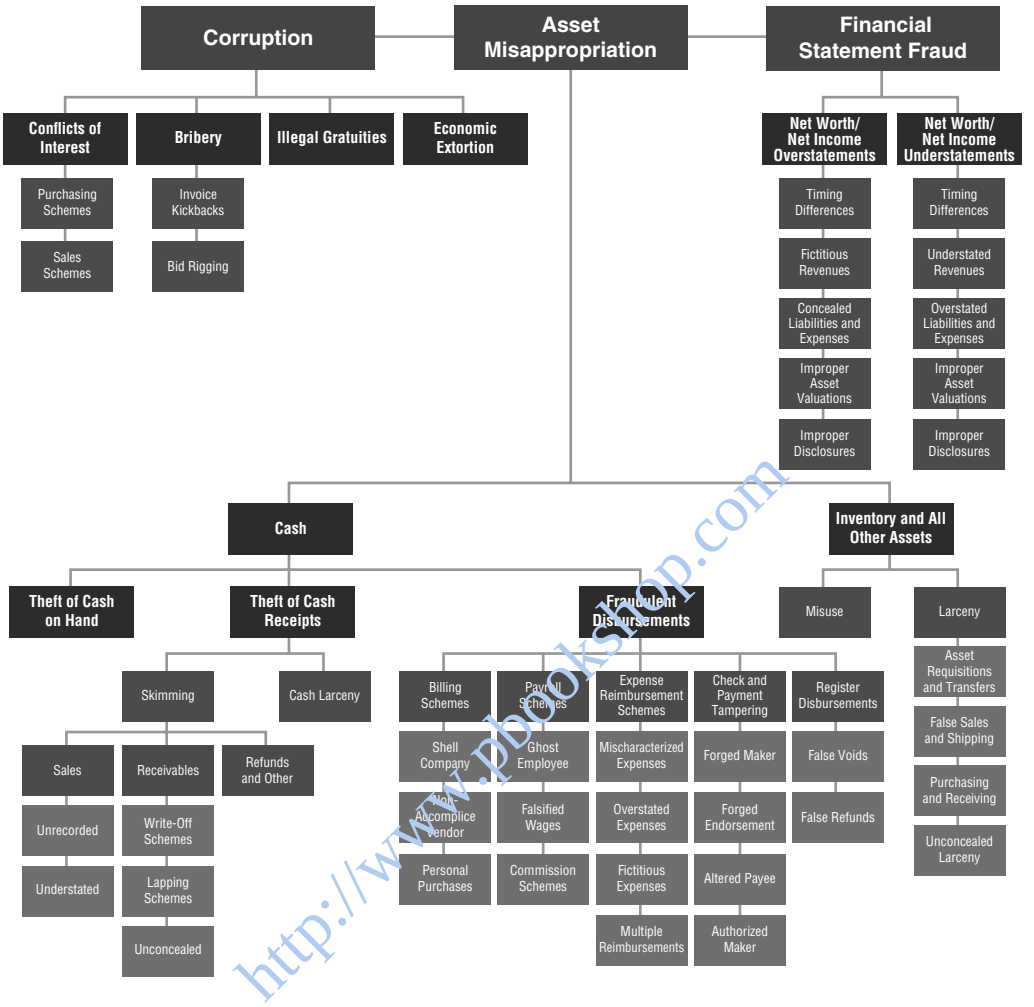


Exhibit 1.3 Occupational Frauds by Category – Frequency

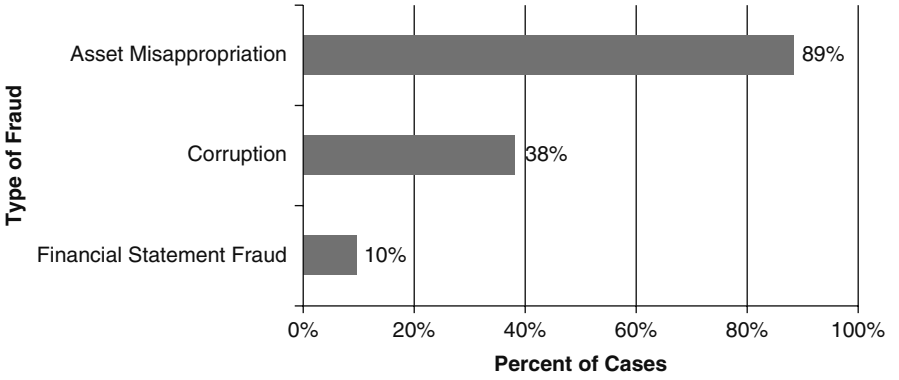
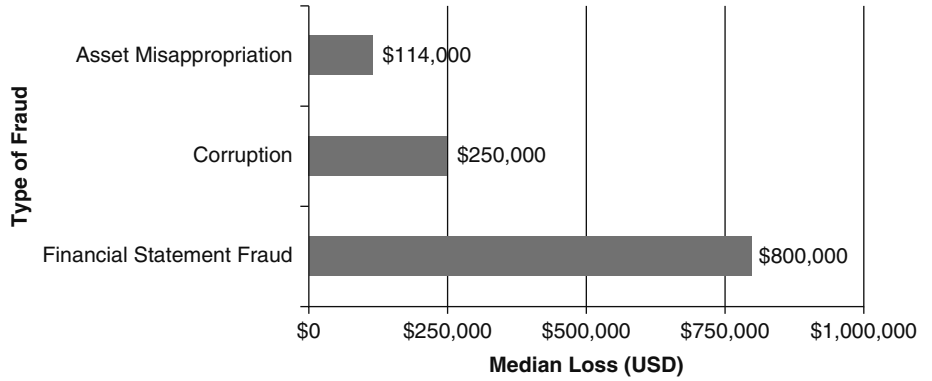


Exhibit 1.4 Occupational Frauds by Category – Median Loss



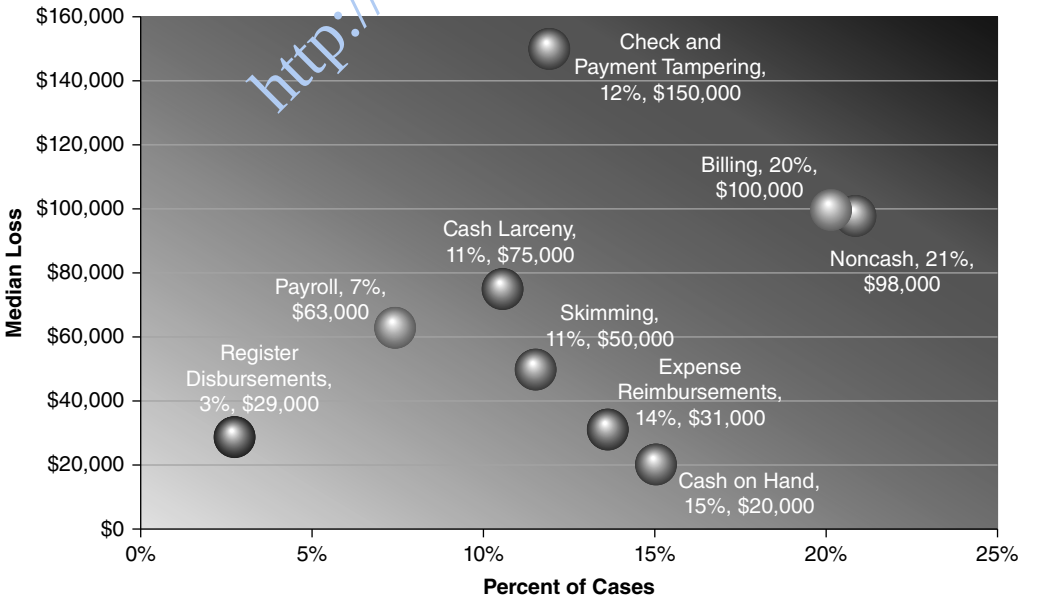
gain. These schemes include both the *theft* of company assets (such as stealing inventory from the warehouse) and the *misuse* of company assets (such as using a company car for a personal trip).

Exhibit 1.5 shows the frequency and median loss of the various forms of asset misappropriation as noted in the ACFE's 2018 *Report to the Nations*.

Theft of Cash on Hand

Theft of cash on hand refers to cash that resides in a secure, central location, such as a vault or safe. These schemes usually involve a perpetrator who has authorized access to monies in the safe or vault.

Exhibit 1.5 Frequency and Median Loss of Asset Misappropriation Subschemes



Theft of Cash Receipts

Perpetrators often target incoming cash payments, whether from sales, payments on customer accounts, or some other source. These schemes can take the form of skimming or cash larceny, depending on when the cash is stolen.

Skimming

Skimming is the theft of incoming cash before an employee records it in the accounting system; thus, it is an *off-book scheme*, meaning these schemes leave no direct audit trail. Because the stolen funds are never recorded, the victim organization might not be aware that the cash was ever received.

Skimming can occur at any point where money enters a business, so almost anyone who deals with the process of receiving incoming payments might be in a position to skim money. However, the most common places for skimming schemes to occur are in sales and accounts receivable.

Sales Skimming

Most skimming schemes involve the theft of incoming payments received from sales. This is probably because money skimmed from sales can remain completely unrecorded, whereas skimmed receivables might leave warning signs in the form of aged account balances.

Example

Johannes is a sales associate at a men's clothing store. One afternoon, a customer approaches the cash register with three shirts that he would like to purchase. Johannes charges the customer for all three shirts, but rings up the sale for only two of the shirts. When the customer hands over cash as payment for the purchase, Johannes puts the money for the two shirts he rang up in the register drawer and puts the money for the other shirt in his pocket.

Receivables Skimming

It is generally more difficult to hide the skimming of receivables than the skimming of sales because receivables payments are expected. When receivables are skimmed, the missing payment is shown on the books as a delinquent account. To conceal a skimmed receivable, the perpetrator must somehow account for the payment that was due to the company but never received. Consequently, schemes in which the fraudster skims receivables usually involve one of the following concealment methods:

- Lapping, in which one customer's payment is used to cover the theft of another customer's payment
- Account write-offs
- Falsified discounts, allowances, or other account adjustments

Example

Marjorie worked in the accounts receivable department of XYZ Corp. When Marjorie's personal debts grew larger than her income, she began embezzling incoming payments from XYZ's customers to finance the shortfall. After stealing Customer A's payment, Marjorie hid the documentation for that payment until the following day, when she took money from Customer B's payment to cover it. Then she used a payment from Customer C to cover the shortage in Customer B's payment. The cycle continued, with Marjorie repeatedly taking some of the incoming payments for herself, until a customer noticed a discrepancy between the payments and the account statement and called the accounting manager to complain.

Cash Larceny

Cash larceny involves the theft of money *after* an employee records it in the accounting system; thus, it is an *on-book scheme*. Accordingly, these schemes leave an audit trail on the company's books and are thus much harder to get away with than skimming schemes. Like skimming schemes, cash larceny can take place anywhere an employee has access to cash, but the most common schemes are:

- Theft of cash from the register
- Theft of cash from the deposit

Theft of Cash from the Register

The register is a popular place for cash larceny schemes for one reason – that's where the money is. In a scheme involving theft of cash from the register, an employee opens the register and simply removes the cash. The fraudster might do so while a sale is rung up or by opening the cash drawer with a "no sale" transaction. Unlike skimming schemes, cash larceny results in an imbalance in the register because the remaining cash in the drawer is less than the amount indicated on the register transaction log.

Example

A manager at a retail store signed onto a coworker's register when that person was on break, rang a "no sale" transaction, and took cash from the drawer. Over a period of two months, the manager took approximately $6,000 through this simple method. The resulting cash shortage therefore appeared in an honest employee's register, deflecting attention from the true thief.

Theft of Cash from the Deposit

When a company receives cash, someone must deposit it into a financial institution. In this scheme, an employee steals currency or checks before depositing them into the

company's account but after recording the payment as received. This causes an out-of-balance condition, unless the thief alters the deposit slip after it has been validated.

Example

Soon after being given the responsibility of taking his company's deposit to the bank (and knowing that his employer's record keeping was less than effective), Gregory began a scheme involving theft of cash from the deposit. He simply took money from the deposit and altered the deposit slip to reflect the amount he actually deposited. His scheme worked well until the company hired a new employee in the accounting department who immediately began reconciling the bank account with the recorded cash receipts.

Fraudulent Disbursements

In a fraudulent disbursement scheme, an employee uses falsified documentation or other misstatements to induce the organization to disburse company funds for a dishonest purpose. Examples of fraudulent disbursements include submitting false invoices, altering time cards, and falsifying expense reports. On their face, the fraudulent disbursements do not appear any different from valid cash disbursements. Someone might notice the fraud based on the amount, recipient, or destination of the payment, but the method of payment is legitimate.

Common forms of fraudulent disbursements include:

- Check and payment tampering schemes
- Billing schemes
- Cash register disbursement schemes
- Expense reimbursement fraud
- Payroll fraud

Check and Payment Tampering Schemes

Check and payment tampering is a form of fraudulent disbursement scheme in which an employee either prepares a fraudulent payment (whether by check or by electronic funds transfer) for personal benefit or intercepts a payment intended for a third party. While the use of checks for business payments has declined dramatically over recent decades – and is almost nil in some countries – these schemes still proliferate. According to the 2018 *Report to the Nations*, check and payment tampering schemes, including those involving checks, were involved in 12% of occupational frauds and caused a median loss of US $150,000.

Check and payment tampering schemes include:

- Forged maker schemes
- Forged endorsements
- Altered checks
- Authorized maker schemes
- Electronic payment schemes

Forged Maker Schemes In a forged maker scheme, the perpetrator steals blank company checks, fills them out, and negotiates them at a bank, check-cashing store, or other establishment. Commonly, the perpetrator finds unsecured checks and takes several from the bottom of the stack. The theft of the checks might not be discovered until much later (i.e., when the checks would have been issued), when someone notices that the check numbers do not match up with the check register. A variation of this scheme involves stealing checks from an inactive bank account, filling them out, and then cashing them.

Forged maker schemes can be easily concealed if the person who steals the checks also reconciles the bank account upon which the checks are drawn. In this case, the fraud will probably not be caught as long as there is money in the account.

Example

An accountant for a small organization was highly trusted and had responsibility over all accounting functions. She also had unrestricted access to blank checks, and she began writing checks to herself from the company account. To conceal the scheme, she would let large sales go unrecorded in the company's books, then write fraudulent checks in the amount of the unrecorded sales. Since the perpetrator was also the sole recipient of the company's bank statement, she could destroy the fraudulent checks and adjust the reconciliation to show the account as being in balance.

Forged Endorsements Forged endorsements occur when an employee fraudulently negotiates a check written to someone else. The perpetrator might forge the recipient's signature or double-endorse the check.

Example

A manager stole and converted approximately $130,000 worth of company checks that had been returned to the company due to noncurrent addresses for the recipients. The nature of his company's business was such that the recipients of the rerouted checks were often not aware that the victim company owed them money, so 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 the book balance matched when, in fact, they did not.

Altered Checks Rather than forging a signature, the fraudster might change the payee on a previously written check by manually altering the payee or by using a computer to change the payee. One way to alter a check is by adding letters or words at the end of the payee. For example, a check made payable to "ABC" could be changed to "ABCollins" and probably wouldn't be detected when negotiated. Alternatively, if the fraudster has responsibility for check creation, the individual might write the check in pencil to allow for easy alteration later.

Example

An administrative employee misappropriated funds from her organization by preparing checks for fraudulent expenses. The employee would draw a manual check for a miscellaneous expense, have the check approved and signed by an authorized employee, and then alter the check by inserting her own name as the payee. The employee was in charge of the bank statement and would destroy the altered checks when they were returned to the company after payment. Bank staff detected the fraud during a review of manual checks on the account. One check appeared to be irregular, so a bank employee contacted the victim organization, and the perpetrator was interviewed. She admitted to having "borrowed" funds on one occasion. In fact, she had written more than 10 fraudulent checks totaling approximately $50,000.

Authorized Maker Schemes In an authorized maker scheme, an employee with signature authority on a company account writes fraudulent checks for his own benefit and signs his name as the maker. Because the perpetrator is authorized to sign checks, there is no need to forge signatures or intercept signed checks. The perpetrator simply writes and signs the instruments in the same manner as with any legitimate check.

The perpetrator of an authorized maker scheme can conceal a fraud the same way a forged maker does. Additionally, since perpetrators of authorized maker schemes are usually high-level employees, they can use their influence to discourage employees from asking questions when they override controls. Intimidation can play a large part in the concealment of any type of occupational fraud where powerful individuals are involved.

Example

The manager of a sales office stole approximately $150,000 from his employer over a two-year period. The manager had primary check-signing authority and abused this power by writing company checks to pay his personal expenses. Certain members of his staff knew about the fraud, but he had control over their careers. Fear of losing their jobs, plus the lack of a proper whistle-blowing structure, prevented these employees from reporting his fraud.

Electronic Payment Tampering As businesses moved to using electronic payments – such as automated clearinghouse (ACH) payments, online bill payments, and wire transfers – in addition to or instead of traditional checks, fraudsters have adapted their methods to manipulate these payments as well. Some of these fraudsters abuse their legitimate access to their employer's electronic payment system; these schemes are similar to traditional check tampering frauds carried out by authorized makers. Others gain access through social engineering or password theft, or by exploiting weaknesses in their employer's internal control or electronic payment system. Regardless of how they log in to the system, dishonest employees use this access to fraudulently initiate or divert electronic payments to themselves or their accomplices.

As with other schemes, after making a fraudulent payment, employees must cover their tracks. However, the lack of physical evidence and forged signatures can make concealment of fraudulent electronic payments less challenging than other forms of check and payment tampering schemes. Some fraudsters attempt to conceal their schemes by altering the bank statement, miscoding transactions in the accounting records, or sending fraudulent payments to a shell company with a name similar to that of an existing vendor. Others rely on the company's failure to monitor or reconcile its accounts.

Billing Schemes

Billing schemes are those in which the fraudster manipulates the organization's purchasing and accounts payable functions to generate a fraudulent payment. The purchases used by the fraudster to generate the payment might be real or fictitious.

The following are common categories of billing schemes:

- False invoicing through shell companies
- Overbilling schemes involving existing vendors
- Making personal purchases with company funds

False Invoicing through Shell Companies False invoicing occurs when a fraudulent invoice is set up for payment through the normal processing channels. The perpetrator creates fictitious backup documentation for the transaction (e.g., a purchase order or requisition) and attaches an invoice to generate the fraudulent payment. The perpetrator might either be the purchasing agent or be from a user area.

These schemes often involve the use of *shell companies*, which are business entities that typically have no physical presence (other than a mailing address) and no employees, and generate little, if any, independent economic value. Such companies might be nothing more than a fabricated name and a post office box that the fraudster uses to collect disbursements from the false billings. However, because the payments generated are made out in the name of the shell company, the perpetrator normally sets up a corresponding bank account in the shell company's name to deposit and cash the fraudulent checks.

To successfully commit a shell company scheme, the fraudster needs to be able to do all of the following:

- Form the shell company.
- Obtain the victim organization's approval of the shell company as a vendor.
- Submit an invoice from the shell company.
- Collect and convert the payment.

Example

A purchasing manager set up a dummy company using his residence as the mailing address. Over a two-year period, he submitted more than $250,000 worth of false invoices. Eventually, the scheme was detected by an accounts payable clerk when she was processing an invoice and noticed that the address of the vendor was the same as the purchasing manager's address. Had the perpetrator used a post office box instead of his home address on the invoices, his scheme might have continued indefinitely.

Overbilling through Existing Vendors Billing schemes sometimes involve the use of legitimate vendors. In these cases, the perpetrator uses an existing vendor to bill the victim organization for goods or services that are nonexistent or overpriced.

The perpetrator might manufacture a fake invoice for a vendor that regularly deals with the victim organization, or might resubmit an invoice that has already been paid and then intercept the new payment. Because the bill is fictitious, the existing vendor is not out any money. The victim is the organization, which pays for goods or services that it does not receive.

A variation of these schemes, called a *pay-and-return scheme*, involves an employee intentionally mishandling legitimate payments that are owed to existing vendors. A perpetrator might do this by purposely double-paying an invoice, then requesting and intercepting the refund for overpayment. Alternatively, the fraudster might intentionally pay the wrong vendor. The perpetrator tells the vendor to return the check to the perpetrator's attention, intercepts the returned check, and then runs the vouchers through the accounts payable system a second time so the correct vendor eventually gets paid.

Example

A co-owner of a privately held company generated several hundred thousand dollars' worth of fraudulent income through false invoicing. The perpetrator submitted falsified invoices from one of the victim company's regular suppliers. The invoices were prepared with the help of an employee of the supplier. The fraudulent bills were paid on the perpetrator's authority, and the payments were intercepted by the employee of the supplier, who split the proceeds with the company co-owner.

Personal Purchases with Company Funds Some frauds involve employees purchasing goods or services for personal use and billing the purchase to their employer. Fraudsters might use company funds to buy items for themselves, their businesses, their families, or their friends. Instead of generating cash, the perpetrator reaps the benefit of the purchases. From the victim organization's perspective, the loss is the same. In either case, the victim ends up expending funds on something that it does not receive.

In some of these schemes, the fraudster purchases the personal items but has the invoice sent to the organization's accounts payable department for payment. Another variation involves the purchase of personal items using a corporate credit card.

Example

A purchasing supervisor started a company for his son and had his employer purchase all the materials and supplies necessary for the son's business. In addition, the supervisor purchased materials through his employer that were used to add a room to his own house. The perpetrator used company money to buy nearly $50,000 worth of supplies and materials for himself.

Cash Register Disbursement Schemes

Register disbursement schemes involve removing cash from the register during a transaction, but they differ from skimming schemes because there is a record of the transaction on the register transaction log. And unlike cash larceny schemes, these frauds do not result in an imbalanced register. The most common methods are false refunds and false voids.

False Refunds When a customer returns merchandise, an employee generates a refund and gives the customer the funds. Two types of false refunds are included in this category. The first involves refunds made for the entire amount of purchase without a customer actually returning the merchandise. The second involves overstated refunds in which part of the refund is legitimate, but the sales associate rings up a larger refund than the customer is owed and keeps the difference in cash. Another variation of this scheme is a refund through a credit card – the sales associate rings up a refund on the associate's own credit card.

Although false refund schemes are most common in the retail industry, they also occur in the service industry. Often in such frauds, the customer is in collusion with the fraudster. In a typical scheme, a customer receives the services requested, an employee at the service provider bills the customer, the customer submits a payment and it is processed, but then the employee issues a refund based on "unperformed" or "unsatisfactory" services. The two conspirators then split the fraudulent refund.

False Voids False voids are similar to false refunds, except the sales clerk withholds the customer's receipt in anticipation of the fraud. Knowing that most establishments require a receipt to void a purchase, the perpetrator rings up the legitimate sale, keeps the customer's receipt, and then voids the transaction and pockets the sale amount. The sales clerk later submits the customer's receipt to the supervisor to justify the void.

Expense Reimbursement Schemes

Another common form of fictitious disbursements involves employees submitting falsified claims for expense reimbursement. There are four basic types of fraudulent expense reports:

1. Fictitious expenses
2. Altered or overstated expenses
3. Mischaracterized expenses
4. Duplicate reimbursements

Fictitious Expenses Fictitious expenses are expenses that never occurred. The following are examples of common ways that employees fabricate expense report items:

- Claiming mileage that was never incurred
- Claiming lodging charges that were never incurred
- Submitting air travel receipts for trips that were never taken
- Requesting reimbursement for taxi fare when the hotel provided free service from the airport or the employee was picked up by a friend or relative without charge

- Submitting small items, such as tips and parking, that were never incurred
- Claiming meals that were paid for by other parties
- Claiming business trips that were never taken

Example

On his expense report, an employee claimed hotel expenses that his client had actually paid. He attached photocopies of legitimate hotel bills to the expense report as though he had paid for his own room.

Altered or Overstated Expenses Employees might also alter documentation for legitimate expenses to fraudulently increase the amount of reimbursement received. Common altered expense schemes include:

- Altering the amount or date of the expense incurred
- Sharing a taxi with someone but submitting the full fare
- Submitting reimbursement for expensive meals by indicating that more than one person dined
- Altering the identities of individuals entertained so that the expense is reimbursable
- Submitting air travel for first class but flying coach

Mischaracterized Expenses Mischaracterized expenses are expenses incurred by the employee but that are not eligible for reimbursement. Examples include:

- Disguising alcohol as meals
- Paying for personal meals and expenses, such as a family outing, and disguising them as business-related entertainment
- Claiming mileage for personal errands
- Claiming nonallowed entertainment expenses as meals
- Claiming gifts as meals
- Paying for personal vacations and claiming them as business trips

Example

Two midlevel managers ran up $1 million in inappropriate expenses over a two-year period. Their executive supervisors did not properly oversee their travel or expense requests, allowing them to spend large amounts of company money on international travel, lavish entertainment of friends, and the purchase of expensive gifts. They claimed they incurred these expenses entertaining corporate clients.

Duplicate or Multiple Reimbursements Duplicate reimbursements occur when a legitimate expense is paid more than once. For example, an airline trip might be reimbursed

from the passenger receipt as well as from the credit card receipt. The same might be true for meals; both the actual receipt and the credit card receipt are submitted for reimbursement.

Example

In one case of duplicate expense reimbursements, the perpetrator was an executive in a company that another organization purchased. The acquired company continued to operate in a fairly independent manner, and the books of the two companies were maintained separately. The perpetrator held a credit card in the name of the smaller, acquired company, which he used for business expenses. He would retain receipts for expenses charged to this credit card and submit them for reimbursement to the accounting office of the acquiring company. Thus, the perpetrator was able to receive a double reimbursement for his expenses.

Payroll Schemes

Payroll schemes occur when employees fraudulently generate more compensation than they are owed. These schemes are similar to billing schemes in that the perpetrator typically produces a false document or makes a false claim for distribution of funds by the employer. In billing schemes, the false claim typically comes in the form of a fraudulent invoice. In payroll schemes, the false claim generally occurs when the fraudster falsifies payroll records, timekeeping records, or other types of documents related to payroll or personnel functions. The most common forms of payroll fraud schemes are:

- Ghost employees
- Overpayment of wages
- Commission schemes

Ghost Employees A perpetrator might use a fictitious employee placed on the payroll – called a *ghost employee* – to generate fraudulent paychecks. The ghost employee might be an ex-employee kept on the payroll after termination; a newly hired employee put on the payroll before employment begins; an accomplice, such as a friend or relative who does not work for the organization; or a fictitious person.

For a ghost employee scheme to work, the following things must happen:

- The ghost must be added to the payroll.
- Timekeeping information must be collected (if the ghost is set up as an hourly employee).
- A paycheck must be issued to the ghost.
- The check must be delivered to the perpetrator or an accomplice and converted for personal use.

Example

A high-ranking school employee added several fictitious employees to the school district's payroll. The scheme succeeded principally because of a lack of segregation of duties. The perpetrator had the authority to hire new employees and approve payroll expenditures. The bookkeepers for the school district relied on the perpetrator's authority in processing and recording payroll transactions. Payroll checks were distributed through the perpetrator's office, under his supervision. The perpetrator always took direct responsibility for distributing the paychecks to the fictitious employees.

Overpayment of Wages The most common method of misappropriating funds from the payroll involves overpayment of wages. These schemes involve the fraudsters inducing the victim organization into paying them more than they are owed for a pay period.

For employees who are paid on an hourly basis to fraudulently increase the amounts of their paychecks, they must either falsify the number of hours worked or change their wage rates. Because salaried employees do not receive compensation based on hours worked, they usually generate fraudulent wages by increasing their rates of pay. Thus, schemes involving the overpayment of wages include:

- Falsified hours reported (hourly)
- Overtime abuses (hourly)
- Falsified pay rate (hourly and salaried)
- False reporting of paid time off (hourly and salaried)
- Retroactive pay increases (hourly and salaried)

Example

An individual who worked for a government agency committed fraud by falsely claiming overtime. The perpetrator was employed at a remote location and was the only individual who worked in this office, so no one was overseeing her activities. The employee would fill out false time cards, crediting herself with an average of 10 hours of overtime per week. Because there was no supervisor in the office, the perpetrator simply signed the time cards and forwarded them to headquarters.

Commission Schemes Employees who are paid on commission might falsify the amount of sales made – and thus inflate their pay – by creating fictitious sales, altering the pricing list on sales documents or claiming the sales of other employees. Alternatively, they might fraudulently increase their own commission rates. However, to do so, they (or an accomplice) must obtain access to the payroll records, enter the change in the system, and save it.

Noncash Asset Schemes

In addition to stealing cash from an employer, an employee might steal or misuse other assets. These schemes range from taking a box of pencils home to stealing millions of dollars' worth of company equipment or misappropriating proprietary information from the company.

Misappropriation of Physical Assets

Employees can misappropriate a physical noncash asset through two basic methods: misuse and outright theft.

Misuse of Physical Assets Asset misuse is the less egregious of the two categories of noncash misappropriation of physical assets. Misuse typically occurs with fixed assets such as company vehicles, computers, and other office equipment. In such schemes, these assets are not stolen; they are simply used by employees for nonbusiness purposes.

Employees might also use office supplies, computers, and other office equipment to perform personal work on company time. For instance, they might use their computers at work to write letters, print invoices, or complete other work connected with a business they run on the side. In many cases, these side businesses are of the same nature as the employer's business, so the employee is essentially using the employer's equipment to compete with the employer.

Example

An employee used his employer's machinery to run his own snow removal and excavation business. He generally performed this work on weekends and after hours, falsifying the logs that recorded mileage and usage on the equipment. The employee had formerly owned all the equipment but had sold it to his current employer to avoid bankruptcy. As a term of the sale, he agreed to operate the equipment for his current employer, but he also never stopped running his old business.

Theft of Inventory, Supplies, and Fixed Assets While the misuse of company property might be a problem, the theft of company property is of greater concern because it deprives the organization of the ability to use and profit from the assets completely. The most common methods of stealing noncash assets are:

- Unconcealed larceny
- Fraudulent requisitions and transfers
- Falsified receiving reports
- Fraudulent shipments of merchandise
- Theft of scrap inventory

Unconcealed Larceny The most basic method for stealing noncash assets is unconcealed larceny, where an employee takes inventory, supplies, or other assets from the

victim organization's premises without attempting to conceal the theft in the victim's books and records.

Example

A warehouse manager stole merchandise from his employer and resold it for his own profit. The perpetrator was taking inventory on weekends when the company was closed for business. He would enter the warehouse, load a company truck with various types of merchandise, and drive to a commercial storage facility where he kept the stolen items. From there, the fraudster ran his illicit business, selling the merchandise at discounted rates.

Fraudulent Requisitions and Transfers Some employees falsify internal documents pertaining to the requisition or internal movement of noncash assets in order to steal those assets. They use these documents to justify the transfer or reallocation of inventory, supplies, or fixed assets by enabling access to items that they otherwise might not be able to reach. Examples of this type of scheme include overstating the amount of materials required for a project, requesting merchandise for an improper purpose, and fraudulently transferring inventory from one site to another within the victim organization.

Example

An employee of a telecommunications company used false project documents to request approximately $100,000 worth of computer chips, allegedly to upgrade company computers. Knowing that this type of requisition required verbal authorization from another source, the employee set up an elaborate phone scheme to get the project approved. The fraudster used her knowledge of the company's phone system to forward calls from four different lines to her own desk. When the confirmation call was made, it was the perpetrator who answered the phone and authorized the project.

Falsified Receiving Reports Another relatively common method for misappropriating noncash assets is to falsify receiving reports or skim goods from incoming deliveries. For example, a warehouse supervisor or clerk might falsify a receiving report to show that a shipment was short or that some of the goods in the shipment were defective. The perpetrator then steals the "missing" or "substandard" merchandise.

The problem with this kind of scheme is that the receiving report does not reconcile to the vendor's invoice. If the vendor bills for 1,000 units of merchandise, but the receiving report only shows receipt of 900 units, someone has to explain the missing 100 units. This kind of scheme can be avoided by matching up support documents before paying invoices.

Example

Two employees conspired to misappropriate incoming merchandise by marking shipments as short. The fraudsters concealed the theft by falsifying only one copy of the receiving report. The copy that was sent to accounts payable indicated receipt of a full shipment so that the vendor would be paid without any questions. The copy used for inventory records indicated a short shipment so that the assets on hand would equal the assets in the perpetual inventory.

Fraudulent Shipments of Merchandise Some employees misappropriate inventory by creating false sales orders or other shipping documents. These false documents might indicate sales made to fictitious persons or companies, real customers who are unaware of the scheme, or accomplices of the perpetrator. The victim organization's shipping department sends the inventory as if it had been sold; however, there is no sale, and the merchandise is delivered to the perpetrator or an accomplice.

Example

A warehouse employee misappropriated inventory from his employer's distribution center by creating fraudulent shipments. This individual had access to the organization's inventory control and shipping/receiving programs. He created shipments of inventory to an accomplice who worked for a competitor of the victim company. He also had merchandise delivered to a commercial storage facility he had leased. The victim organization had recently relaxed its controls over the shipping and inventory control processes to meet deadlines and improve efficiency. Consequently, the fraudster was able to enter shipping information into the victim's computer system, wait until the shipment was sent, and then cancel the orders and delete all the files associated with the transaction.

Theft of Scrap Inventory Assets are sometimes written off *before* they are stolen, making them susceptible to theft. If a fraudster can have the target assets designated as scrap, it can be easier to conceal their misappropriation. Fraudsters might be able to take the supposedly useless assets for themselves, sell them to an accomplice at a greatly reduced price, or simply give them away.

Example

A warehouse foreman abused his authority to declare inventory obsolete. The foreman wrote off perfectly good inventory as scrap, and then transferred it to a shell corporation that he secretly owned. Using this scheme, the fraudster took more than $200,000 worth of merchandise from his employer.

Concealing Shrinkage When a fraudster steals inventory, supplies, or fixed assets, the key concealment issue is usually shrinkage. *Shrinkage* is the unaccounted-for reduction in an organization's inventory that results from theft. Shrinkage is one of the red flags of noncash asset misappropriation. The goal of the fraudster is to avoid detection and prevent anyone from looking for missing assets. This means concealing the shrinkage that occurs from inventory theft. Common ways fraudsters attempt to conceal inventory shrinkage include:

- Altering inventory records
- Padding the physical inventory
- Recording fictitious sales and accounts receivable
- Writing off the missing assets

Misappropriation of Intangible Assets

Any valuable information that an organization collects, creates, develops, or stores is susceptible to theft or misappropriation.

Types of Intangible Assets That Are Misappropriated The two intangible assets most susceptible to misappropriation are intellectual property and personally identifiable information.

INTELLECTUAL PROPERTY The World Intellectual Property Organization defines *intellectual property* as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names, and images used in commerce."[2] The term encompasses many different forms of subject matter, which in some cases might overlap through copyrights, patents, trademarks, industrial design rights, and trade secrets.

Of these, trade secrets are particularly susceptible to theft because they are the most likely to confer a competitive advantage when misappropriated. The potential for theft and abuse increases as management invests time, money, and energy into developing information, processes, techniques, and other forms of trade secrets that provide an edge over competitors. The precise definition of a *trade secret* tends to vary by jurisdiction, but three elements are common to most:

1. The information is not generally known to the relevant portion of the public.
2. It confers an economic benefit on its holder (derived specifically from its not being generally known, not just from the value of the information itself).
3. It is the subject of reasonable efforts to maintain its secrecy.

Consequently, trade secrets can include a variety of confidential information used by an organization to gain a competitive advantage in its market, including:

- Business processes (e.g., those used in manufacturing, sales, or marketing)
- Sales information, such as customer data, historical sales, and cost and pricing information
- Research findings
- Methodologies

- Business plans and strategic plans
- Unreleased marketing information
- Source code and algorithms
- Documents and forms

Personally Identifiable Information *Personally identifiable information* (PII) is information that can be used on its own or with other information to identify, contact, or locate a person, or to identify an individual in context. PII includes but is not limited to:

- Full name, maiden name, mother's maiden name, or alias
- Street address or email address
- Government identification number, passport number, driver's license number, taxpayer identification number or financial account, or credit card numbers
- Information about an individual that is linked or linkable to one of the previously listed items (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, and financial information)

Organizations often have databases of PII for employees and customers. Such information can be extremely valuable to fraudsters because it can be used to commit identity theft, obtain fraudulent credit cards, or hack into individuals' bank accounts.

How Do Employees and Other Insiders Misappropriate Information?
Gaining access to sensitive information can be a complex feat for an outsider, but an employee might already have access to the targeted information. Even employees who do not have access are likely to know who does and how get to the information. Departing employees are often the greatest source of concern regarding information theft because they might see an opportunity to use company information to help get ahead at a new job or to get revenge on an organization they believe has wronged them.

As technology evolves, so do the methods used to misappropriate information. Ranging from crude to sophisticated, the methods used by insiders have a commonality: They serve a different – and usually legitimate – purpose within the business's normal operations. The following are some mechanisms that fraudsters might use to transfer the valuable information they are misappropriating:

- Email
- Removable media (e.g., USB drives, CDs, hard disks, and external drives)
- Smart phones and other mobile devices
- Printed documents and files
- Images and screen captures
- Instant messaging
- Social media
- File transfer protocols (e.g., FTP and SFTP)
- Peer-to-peer file-sharing programs
- Cloud storage

Corruption

Corruption involves employees' use of their influence in business transactions in a way that violates their duty to the employer and for the purpose of obtaining a benefit for themselves or someone else. These schemes create an unhealthy situation for businesses.

Corruption is a significant problem for organizations, particularly due to the drive for growth in international markets. As a result, many countries have enacted laws specifically designed to combat this risk. (Information about these country-specific laws is contained in Part II of this handbook.) Despite the multitude of anti-corruption legislation and increased enforcement efforts around the world, corruption is still prevalent.

Corruption can be broken down into the following four scheme types:

1. Bribery and kickbacks
2. Illegal gratuities
3. Economic extortion
4. Conflicts of interest

Bribery and Kickbacks

Bribery can be defined as "the offering, giving, receiving, or soliciting of corrupt payments (i.e., items of value paid to procure a benefit contrary to the rights of others) to influence an official act or business decision." At its heart, a bribe is a business transaction, albeit an illegal or unethical one. A person "buys" influence over the recipient of the bribe to procure a benefit that is contrary to the duty or the rights of others. Thus, bribery involves collusion between at least two parties – typically one inside and one outside the organization.

Bribery often takes the form of kickbacks, a form of negotiated bribery in which a commission is paid to the bribe taker in exchange for the services rendered. Thus, *kickbacks* are improper, undisclosed payments made to obtain favorable treatment. In the government setting, kickbacks refer to the giving or receiving of anything of value to obtain or reward favorable treatment in relation to a government contract. In the commercial sense, kickbacks refer to the giving or receiving of anything of value to influence a business decision without the employer's knowledge and consent.

Usually, kickback schemes are similar to the billing schemes described previously. They involve the submission of invoices for goods and services that are either overpriced or fictitious. However, kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and third parties.

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 this assistance, the employee receives a kickback payment from the vendor.

Most kickback schemes attack the purchasing function of the victim organization; therefore, these frauds are often undertaken by employees with purchasing responsibilities. Purchasing employees usually have direct contact with vendors and therefore have an opportunity to establish a collusive relationship.

Example

A purchasing agent redirected a number of orders to a company owned by a supplier with whom the agent was conspiring. In return for the additional business, the supplier paid the purchasing agent more than half the profits from the additional orders.

Illegal Gratuities

Illegal gratuities are something of value given to reward a decision *after* it has been made, rather than to influence it before the decision is made. Illegal gratuities are similar to bribery schemes except that, unlike bribery schemes, illegal gratuity schemes do not necessarily involve an intent to influence a particular decision before the fact; it is enough to show that the employee accepted an award based on the employee's performance. For example, instead of paying an employee to make a decision (i.e., award a contract), the vendor pays the employee because a favorable decision was made.

In the typical illegal gratuities scenario, a decision is made that 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 is merely offered as a thank-you for something that has been done.

Example

A city commissioner negotiated a land development deal with a group of private investors. After the deal was approved, the private investors rewarded the commissioner and his wife with a free, all-expenses-paid, international vacation.

At first glance, it might seem that illegal gratuity schemes are harmless as long as the business decisions in question are not influenced by the promise of payment. But most organizations' ethics policies forbid employees from accepting unreported gifts from vendors. One reason for such blanket prohibitions is that illegal gratuity schemes can (and frequently do) evolve into bribery schemes. Once an employee has been rewarded for an act such as directing business to a particular supplier, the employee might reach an understanding with the gift giver that future decisions will also be made to benefit the gift giver. Additionally, even though no outright promise of payment has been made in an illegal gratuity, employees might direct business to certain companies in the hope that they will be again rewarded with money or gifts.

Economic Extortion

An extortion scheme is often the other side of a bribery scheme. Economic extortion is present when an employee or official, through the wrongful use of actual or threatened force or fear, demands money or some other consideration to make a business decision. A demand for a bribe or kickback, coupled with a threat of adverse action if the payment

is not made, might constitute extortion. For example, a government official might refuse to pay a legitimate invoice from a contractor unless the contractor pays the official a percentage.

Example

A plant manager for a utility company started a business on the side. The manager forced vendors who wanted to do work for the utility company to divert some of their business to the manager's side business. Those that did not agree to the manager's terms lost their business with the utility company.

Conflicts of Interest

Conflicts of interest occur when an employee or agent of the organization (or a spouse or close family member) has an undisclosed financial interest in a matter that could influence the person's professional role. As with other corruption frauds, conflict of interest schemes involve the exertion of an employee's influence to the principal's detriment. In contrast to bribery schemes, in which fraudsters are paid to exercise their influence on behalf of a third party, conflict of interest cases involve self-dealing by employees or agents.

Conflicts of interest frequently arise in the procurement process. These conflicts usually involve employees who make decisions that would allow them to give preference or favor to a vendor or contractor in exchange for anything of personal benefit to themselves or their friends and families.

Conflicts of interest can occur in various ways. For example, they often arise when an employee:

- Buys goods or services through a broker or intermediary that the employee controls
- Is involved in other business ventures with a vendor or contractor or its employees
- Has an interest in a business that competes with the employer
- Accepts inappropriate gifts, favors, travel, entertainment, or "fees" (kickbacks) from a vendor or contractor
- Engages in unapproved employment negotiations or accepts employment with current or prospective vendors or contractors

Most conflicts of interest occur because the fraudster has an undisclosed economic interest in a transaction, but a conflict can exist when the fraudster's hidden interest is not economic. In some scenarios, employees act in a manner detrimental to their employer to provide a benefit for a friend or relative, even though the fraudster receives no direct financial benefit.

Conflicts of interest do not necessarily constitute legal violations, as long as they are properly disclosed. Thus, 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 the 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.

Financial Statement Fraud

Financial statement fraud is the deliberate misrepresentation of the financial condition of an enterprise accomplished through the intentional misstatement or omission of amounts or disclosures in the financial statements to deceive financial statement users. Like all types of fraud, financial statement fraud involves an intentional act. As stated in the International Standard on Auditing (ISA) 240, *The Auditor's Responsibility Relating to Fraud in an Audit of Financial Statements*, "misstatements in the financial statements can arise from error or fraud. The distinguishing factor between error and fraud is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional."[3]

The financial statements are the responsibility of the organization's management. Accordingly, financial statement fraud is unique in that it almost always involves upper management. Also, in contrast to other frauds, the motivation for financial statement fraud is not only personal gain. Most commonly, financial statement fraud is used to make a company's reported earnings look better than they actually are. Specifically, some of the more common reasons people commit financial statement fraud are:

- To demonstrate increased earnings per share or partnership profits interest, thus allowing increased dividend/distribution payouts
- To cover inability to generate cash flow
- To avoid negative market perceptions
- To obtain financing, or to obtain more favorable terms on existing financing
- To encourage investment through the sale of stock
- To receive higher purchase prices for acquisitions
- To demonstrate compliance with financing covenants
- To meet company goals and objectives
- To receive performance-related bonuses

Most financial statement schemes involve one or more of the following:

- Overstatement of assets or revenues
- Understatement of liabilities or expenses
- Improper disclosures[4]

Overstated Assets or Revenues

One of the most direct ways to improve the organization's financial appearance is to artificially inflate the reported revenues, assets, or both. However, recording revenue or assets in a way that is not in accordance with generally accepted accounting principles can result in fraudulent financial statements.

Common schemes used to overstate asset or revenue include:

- Fictitious revenues
- Timing differences
- Improper asset valuation

Fictitious Revenues

Fictitious revenue schemes involve recording sales that never occurred. The purpose of fictitious sales is to overstate or inflate reported revenue to make the organization appear more profitable than it is. Fictitious revenues can be recorded for fake sales of both goods and services.

Fictitious revenue schemes most often involve fake or phantom customers, but can also involve legitimate customers. For example, an invoice is prepared for a legitimate customer and then the goods are not shipped or the services are not rendered. At the beginning of the next accounting period, the sale is reversed. Another method involves altering (e.g., artificially inflating) invoices to legitimate customers so that they reflect higher amounts or quantities than were actually sold.

Timing Differences

Financial statement fraud can involve timing differences (i.e., recognizing revenue or expenses in improper periods). In general, revenue should be recognized in the accounting records when the sale is complete; for the sale of goods, this generally is when title is passed from the seller to the buyer. In the case of services, revenue is typically recognized when the services have been rendered.

Examples of schemes that involve fraudulent timing differences include:

- Improper matching of revenues and expenses
- Early revenue recognition

Improper Matching of Revenues and Expenses In general, under the accounting concept of the *matching principle*, revenues and their corresponding expenses should be recorded in the same period. An example of improper matching of revenues and expenses occurs when a company accurately records sales for an accounting period, but then fails to simultaneously record the expenses corresponding to those sales. This mismatch of income and expenditures has the effect of overstating net income in the period the sales occurred, and subsequently understating net income when the expenses are recorded.

Early Revenue Recognition Generally, revenue should be booked when the sale is complete – when the title has passed from the buyer to the seller or when services have been rendered. However, intentionally booking revenue before it is earned results in overstated income. For example, a company receives fees from a customer for management services that it has not yet rendered. If the company reports the fees as revenue in the period received, the financial statements for the period will be misstated. The same is true for the sale of merchandise that is booked but not shipped. In addition, the income for the reporting period in which the sales are finally complete

will be lower than it should be due to the cost of goods sold recorded in that period without matching revenue to offset it.

Improper Asset Valuation

The cost principle in generally accepted accounting principles requires that assets be recorded at their original cost. Some assets are reported at the lower of cost or market value, but asset values are generally not increased to reflect current market value. Even so, it is still sometimes necessary to use estimates in valuing and accounting for assets. For example, estimates are used in determining the salvage value and useful life of a depreciable asset. Whenever estimates are used, there is an opportunity for fraud. For this reason, some assets are especially susceptible to manipulation.

While any asset can be manipulated for financial reporting purposes, the most common assets subject to improper valuation are:

- Inventory
- Accounts receivable
- Fixed assets

Inventory Inventory can be overstated by manipulating the physical inventory count, failing to relieve inventory for costs of goods sold, and many other methods. One of the most popular methods of overstating inventory is by reporting fictitious (phantom) inventory. Fictitious inventory schemes usually involve the creation of fake documents, such as inventory count sheets and receiving reports. In some instances, a co-conspirator claims to be holding inventory for the company in question. Alternatively, some fraudsters insert fake count sheets or change the quantities recorded on the count sheets during the inventory observation.

Accounts Receivable Accounts receivable are subject to manipulation in the same manner as sales and inventory, and in many cases the schemes are conducted together. The two most common schemes involving accounts receivable are:

- Fictitious receivables (which usually accompany fictitious revenues)
- Failure to write down accounts receivable as bad debts or the failure to establish adequate reserves for future collectability problems

Fixed Assets Fixed asset values can be falsified through several different schemes. Some of the more common schemes are:

- Fictitious fixed assets
- Misrepresenting valuations of fixed assets

Understated Liabilities and Expenses

Understating liabilities and expenses is another way financial statements can be manipulated to make a company appear more profitable than it is. Liability understatement

has a positive effect on the balance sheet in that the company appears to owe less to creditors than it actually does. Furthermore, the reported amount of either assets or equity increases by the amount of understated liabilities to keep the books in balance. Understating expenses, conversely, has the effect of artificially inflating net income. Both actions make the financial statements more attractive to the user.

Concealed liabilities and expenses can be difficult to detect because frequently there is no audit trail to follow. If there is nothing in the books, it makes the manipulation difficult to uncover using normal audit and review techniques.

Common methods of concealing liabilities and expenses involve:

- Liability or expense omissions
- Improper capitalizing of costs

Liability or Expense Omissions

The easiest method of concealing liabilities and expenses is to simply fail to record them. Liability omissions are probably one of the hardest schemes to detect. A thorough review of all transactions after the financial statement date, such as increases and decreases in accounts payable, might help uncover any liabilities that management omitted from the financial statements. Also, a review and analysis of the company's contractual obligations might reveal contingent liabilities that were intentionally omitted.

Improper Capitalizing of Costs

All organizations incur costs. However, it is not always clear how an organization should record those costs. Suppose ABC Company has a piece of property in need of some repairs. If the work performed simply fixes any problems and brings the property back to its original state, then the costs associated with the repair would appear as an expense on the income statement in the year they were incurred. Net income would be reduced by this amount, and the balance sheet would remain unaffected.

However, suppose work is done that not only repairs but increases the value of the property. Any expenditures made that increase the book value of the property would need to be capitalized – that is, added to the company's assets reported on the balance sheet. In other words, these costs would be added to the asset value on ABC's balance sheet and then depreciated as an expense over time.

Either way, the costs associated with repairs or improvements are on ABC's income statement as an expense. The difference is in the timing. Capitalizing an expenditure and depreciating it over a number of years makes a significant difference in the bottom line of the financial statements in the year the work was done. Conversely, expensing the same amount of costs in the same year results in a much lower net income that year.

Improperly capitalizing expenses is another way to increase income and assets and make the entity's financial position appear stronger. If expenditures are capitalized as assets and not expensed during the current period, both income and assets will be overstated. As the assets are depreciated, income in following periods will be understated.

Improper Disclosures

Generally accepted accounting principles require that financial statements and notes include all the information necessary to prevent a reasonably discerning user of the financial statements from being misled. The most common fraud schemes resulting from improper disclosures involve:

- Related-party transactions
- Liability omissions
- Subsequent events
- Management fraud
- Accounting changes

Related-Party Transactions

Related-party transactions occur when a company does business with another entity whose management or operating policies can be controlled or significantly influenced by the company or by some other party in common. The financial interest that a company official has might not be readily apparent. For example, common directors of two companies that do business with each other, any corporate general partner and the partnerships with which it does business, and any controlling shareholder of the corporation with which it does business could be related parties. Family relationships can also be considered related parties, such as all direct descendants and ancestors, without regard to financial interests.

Related-party transactions are sometimes referred to as *self-dealing*. While these transactions are sometimes conducted at arm's length, often they are not. There is nothing inherently wrong with related-party transactions, as long as they are fully disclosed. If the transactions are not fully disclosed, the company might injure shareholders by engaging in economically harmful dealings without their knowledge.

Liability Omissions

Improper disclosures related to liability omissions include the failure to disclose loan covenants or contingent liabilities. Loan covenants are agreements, in addition to or as part of a financing arrangement, that a borrower has promised to keep as long as the financing is in place. The agreements can contain various types of covenants, including certain financial ratio limits and restrictions on other major financing arrangements. Contingent liabilities are potential obligations that will materialize only if certain events occur in the future. A corporate guarantee of personal loans taken out by an officer or a private company controlled by an officer is an example of a contingent liability.

Subsequent Events

Events occurring or becoming known after the close of the period that could have a significant effect on the entity's financial position must be disclosed. Fraudsters typically avoid disclosing court judgments and regulatory decisions that undermine the reported values of assets, that indicate unrecorded liabilities, or that adversely reflect upon management's integrity. A review of subsequent financial statements, if available, might reveal whether management improperly failed to record a subsequent event that it had knowledge of in the previous financial statements.

Management Fraud

Management has an obligation to disclose to the shareholders information about significant fraud committed by officers, executives, and others in a position of trust. When management is aware that fraud has occurred and the subjects are under criminal proceedings, disclosure is required.

Accounting Changes

In general, three types of accounting changes must be disclosed to avoid misleading the user of financial statements: changes in accounting principles, estimates, and reporting entities. Although the required treatment for these accounting changes varies for each type and across jurisdictions, they are all susceptible to manipulation. For example, fraudsters might fail to retroactively restate financial statements for a change in accounting principles if the change causes the company's financial statements to appear weaker. Likewise, they might fail to disclose significant changes in estimates such as the useful lives and estimated salvage values of depreciable assets, or the estimates underlying the determination of warranty or other liabilities. They might even secretly change the reporting entity by adding entities owned privately by management or by excluding certain company-owned units to improve reported results.

External Fraud

External fraud against a company covers a broad range of schemes committed by a broad range of parties. While management often places considerable attention on the potential for employee fraud, it must ensure that the organization's leaders are aware of the ways the organization can be defrauded by outside parties and that anti-fraud measures address the risks posed by these threats as well.

Many external fraud schemes are dependent upon the relationship the perpetrator has with the organization, and thus the opportunities presented to commit the fraud.

Fraud Committed by Vendors and Contractors

Dishonest vendors and contractors might engage in schemes to defraud the organization of cash or other resources. Common examples of fraud committed by vendors include:

- Billing the company for goods or services not provided
- Submitting inflated or duplicate billings for payment
- Bribing company employees to gain or keep the company's business
- Delivering goods or services that do not meet the specified requirements, but not disclosing the substitution

Colluding with Other Vendors or Contractors

Some contractors might seek to circumvent the competitive bidding process – and thus to defraud the company – by colluding with their competitors. In these schemes, competitors in the same market collude to defeat competition or to inflate the prices of goods

and services artificially. When competitors commit such schemes, the procuring entity is cheated out of its right to the benefits of free and open competition.

The most common forms of collusion between competitors involve the following types of schemes:

- *Complementary bidding* (also known as *protective*, *shadow*, or *cover bidding*) occurs when competitors submit token bids that are not serious attempts to win the contract (e.g., are too high or deliberately fail to meet other requirements). These bids give the appearance of genuine bidding but are actually intended only to influence the contract price and who is awarded the contract.
- *Bid rotation* (also known as *bid pooling*) occurs when two or more contractors conspire to alternate the business between/among themselves on a rotating basis. Instead of engaging in competitive contracting, the bidders exchange information on contract solicitations to guarantee that each contractor will win a share of the purchasing entity's business.
- *Bid suppression* occurs when two or more contractors enter into an illegal agreement whereby at least one of the conspirators refrains from bidding or withdraws a previously submitted bid. The goal of this type of scheme is to ensure that a particular competitor's bid is accepted.
- *Market division* occurs when competitors agree to divide and allocate markets and to refrain from competing in each other's designated portion of the market. The result of these schemes is that competing firms will not bid against each other, or they will submit only complementary bids when a solicitation for bids is made by a customer or in an area not assigned to them. The customer thereby loses the benefit of true competition and ends up paying a higher price than would be dictated by fair bidding under normal economic forces.

Colluding with Company Employees

In addition to bribing company employees to gain or keep the company's business, some dishonest vendors collude with company insiders to rig the procurement or contract bidding process. The manner in which these schemes are perpetrated generally depends on the corrupt employee's level of influence. The more power a person has over the process being manipulated, the more likely it is that the person can influence which entity is awarded the contract.

Fraud schemes involving collusion between the contractor and the purchasing entity's employees generally include the following:

- *Need recognition schemes*, in which a company employee receives a bribe or kickback for convincing the employer to recognize a need for a particular product or service
- *Bid tailoring* (also known as *specifications schemes*), in which an employee with procurement responsibilities, often in collusion with a contractor, drafts bid specifications in a way that gives an unfair advantage to a certain contractor
- *Bid manipulation schemes*, in which a procuring employee attempts to influence the selection of a contractor by restricting the pool of competitors from which

bids are sought, thereby improving the collusive vendor's chances of winning the contract
- *Leaking bid data*, in which an employee of a procuring entity leaks confidential information from competing bidders to a favored bidder, giving that bidder an unfair advantage in the bidding process
- *Bid splitting*, in which a dishonest employee breaks up a large project into several small projects that fall below the mandatory bidding level and awards some or all of the component jobs to a contractor with whom the employee is conspiring

Fraud Committed by Customers

Likewise, dishonest customers might take advantage of company sales and return policies for personal gain or might attempt to obtain company goods or services for free. Examples of frauds committed by customers include:

- Placing orders on other customers' accounts (account takeover fraud)
- Submitting bad checks or falsified account information for payment
- Paying for purchases with stolen or counterfeit credit cards
- Attempting to return stolen, broken, or counterfeit products for a refund
- Claiming goods were never received (even though they were) and requesting a refund or replacement order
- Overpaying for a product or service using a fraudulent payment method (e.g., counterfeit check or stolen credit card) and then requesting the organization to wire the difference between the overpayment and the true cost to the fraudster or a third party
- Manipulating customer loyalty and reward programs to obtain benefits the fraudster isn't entitled to
- Making multiple warranty claims or claims for issues not covered by the warranty

Fraud Committed by Agents, Brokers, and Fiduciaries

Other parties, such as financial and legal advisers, might also have the opportunity to defraud organizations. For example, an investment adviser might steal an organization's funds or undertake transactions on the organization's behalf simply to generate excess fees and commissions. Such schemes are similar to schemes perpetrated against consumers, but organizations can fall victim to dishonest agents, brokers, and fiduciaries as well.

Fraud Committed by Unrelated Third Parties

In addition to watching for schemes perpetrated by parties known to the organization, management must also be aware of threats from unknown outside parties.

Business ID Theft

While individuals are the usual targets of identity theft, identity thieves sometimes target businesses. *Business identity theft* occurs when a fraudster impersonates a business

to commit financial fraud. For identity thieves, there are a number of reasons to target businesses instead of individuals:

- The potential rewards are greater, as businesses tend to have larger bank account balances, easier access to credit, and higher credit limits than individuals.
- Employees are less likely to notice new or unusual financial transactions, because businesses tend to engage in more transactions than individuals.
- The information necessary to commit business identity theft (e.g., business or tax identification numbers) is often publicly available online or in government records.

Methods of Business ID Theft

To operate legally in most jurisdictions, company owners must file certain documents with the appropriate government agency. Such documents might include business registration forms, organizational documents (e.g., articles of incorporation), governance agreements (e.g., shareholder agreements), and tax forms. Fraudsters often commit business identity theft by changing the information in these government filings. In addition to impersonating an existing business, identity thieves can use those government filings to reinstate or revive a closed or dissolved business. Identity thieves tend to target companies that recently closed, because there is usually a legal time limit for reinstatement (e.g., two years from closure). Once they find a suitable company, the identity thieves can reinstate the company by filing the required reinstatement documents and paying a filing fee. The owners of the closed or dissolved company generally do not discover the fraud until creditors of the reinstated company contact them.

Fraudsters also commit business identity theft by creating a new business with a name similar to an existing business. For example, identity thieves could impersonate a company named Windsor Homes, Inc., by creating a new company named "Windsor Homes, LLC" or "Windsor Home, Inc." In such cases, the fraudsters attempt to trick careless third parties (e.g., creditors, vendors, customers) into doing business with the similarly named company.

In one of the more audacious and risky schemes, fraudsters sometimes commit business identity theft by renting office space in the same building as the targeted company.

Example

Barney, Cooper, & Smith (BCS) is a large law firm that occupies the ninth and tenth floors of an office building. After researching BCS for months, a fraudster rents a suite on the eighth floor of the same building, calls several of BCS's vendors, and orders $50,000 worth of computers and office equipment. The fraudster pretends to represent BCS and gives the address of his suite. Because his address is the same as that of BCS (except for the suite number), the vendors deliver the goods to the fraudster's suite. The fraudster then vacates the building. BCS discovers the fraud a month later when it receives invoices from the vendors.

Data Breaches

External fraudsters are increasingly attacking organizations' networks and systems to steal sensitive information. In these data breach schemes, the fraudster exploits weaknesses stemming from default configurations and passwords, design flaws, coding issues, and software vulnerabilities. Wide-ranging and often sophisticated techniques, such as SQL injection, malware, automated attack tools, exploit kits, and other hacking tools can be used by ambitious fraudsters. Conversely, many data breaches are accomplished using simple social engineering techniques, such as phishing schemes, tech support impersonation schemes, or schemes targeting the customer contact center.

Upon gaining access to systems, the attackers search to identify the valuable information before misappropriating it from the organization's controls. These attacks can be either obvious or unnoticeable to the victim organization, depending on the attackers' skill levels.

While many data breaches are committed by unrelated third parties, the possible perpetrators – and the specific motivations for the attacks – vary. Such schemes might be perpetrated or assisted by:

- Contractors or vendors, which often have access to the same information as employees but without the same controls
- Competitors, which are seeking to misappropriate trade secrets, ideas, processes, blueprints, or source code, or to acquire commercial information such as client lists, pricing, or bid information to gain an undue advantage
- Nation-state actors, who have become extremely active in industrial and commercial ventures so their industries can perform at a higher level than those of competing nations
- Organized crime groups, who seek personally identifiable information in support of criminal endeavors

Ransomware

Ransomware is a type of malicious software (malware) that locks a computer's operating system and restricts access to data until the victim pays a ransom to the perpetrator. Fraudsters use ransomware to extort money from businesses. A typical ransomware attack on a business involves the following three steps:

1. *A company computer or network is infected with ransomware*. The infection usually occurs when an employee clicks on a malicious link in an email, opens or downloads an infected file, or visits a compromised website. Ransomware can also infect mobile devices through links in text messages. Some ransomware spreads automatically through the Internet, infecting computers without the need for any action by computer users. However, this method of infection is uncommon; most ransomware infections occur because a user unwittingly downloads it. After infecting one computer, the ransomware often spreads throughout the company's computer network, endangering all data residing on the network.

2. *The ransomware encrypts or blocks access to data on the infected computer or the entire network.* Some ransomware programs also encrypt the targeted data so that the victim cannot access the data without a decryption key provided by the fraudster. Other ransomware programs simply delete the data and then falsely claim that it has been encrypted, thus tricking the victim into paying a ransom for data that no longer exists.
3. *A ransom demand is displayed on the computer screen*. Generally, the ransomware disables the infected computer and displays a message on the computer screen stating that the victim's data will be deleted unless a ransom is paid by a specified date. To intimidate victims, the message might contain threatening accusations that the victim has viewed illegal videos, downloaded pirated media, or otherwise accessed forbidden content. The message might also include police insignia or an official-looking government logo. Other ransomware messages are more direct and make no effort to conceal their obvious attempts at extortion. Increasingly, such messages demand payment in bitcoin, the most popular type of cryptocurrency. Historically, fraudsters have kept the ransom amount relatively low to encourage more victims to pay, especially in ransomware campaigns that are widespread and indiscriminate. However, the ransom amount tends to be higher when a specific company is targeted. In addition, many companies do not recover their data after paying the ransom. Some fraudsters destroy the ransomed data regardless of management's response, and others raise the ransom amount after receiving an initial payment.

Business Email Compromise

In a traditional *business email compromise* scheme, a fraudster uses a fake email from a company executive (e.g., CEO, CFO, president) to trick an employee into sending money or other information to the fraudster. Business email compromise schemes are also commonly known as *BEC scams* or *CEO fraud*.

How BEC Scams Work

Social engineering refers to the psychological manipulation of people to trick them into revealing information or taking some action. After researching a victim, social engineers often impersonate someone the victim trusts, such as an authority figure or a business associate.

One common social engineering method is *phishing*, which involves the use of emails to impersonate trusted persons or entities. In traditional phishing schemes, fraudsters send out thousands of emails indiscriminately. Only a small percentage of recipients fall for the scheme, but the fraudsters rely on the sheer volume of their emails to achieve results. By contrast, *spear phishing* schemes target specific individuals or businesses. BEC scams are a type of spear phishing scheme. They generally require more preparation than a traditional phishing scheme, but the rewards can be great.

Prior to initiating the BEC scam, fraudsters generally perform extensive research on the company, the executive they will impersonate, and the employee who will receive the fake email. Fraudsters can gather much of this information from public sources,

such as the company's website and social media accounts. In addition, fraudsters might use phishing or other social engineering methods, malware, and hacking to learn about the company's employees, organizational structure, and payment procedures. Some victims have reported being the target of a ransomware attack prior to a BEC scam.

The fake emails used in BEC scams are often well written, and they sometimes mimic language used by the executive in prior emails. Fraudsters can compromise the executive's email account through social engineering or computer intrusion techniques (e.g., malware). Additionally, fraudsters sometimes spoof emails by adding, removing, or changing characters in the email address. For example, if a CEO's email address is John.Smith@ABCINC.com, the fake email might come from John.Smit@ABCINC.com (the "h" in "Smith" is missing) or John.Smith@ACBINC.com (the letters "B" and "C" in "ABCINC" are transposed). This makes it difficult to spot the fake email address.

Types of BEC Schemes

Although BEC scams can take numerous forms, the FBI has identified five common scenarios by which BEC scams are perpetrated.[5]

1. Fraudsters posing as a company's longstanding supplier (often a foreign supplier) send an email to an employee of the company and request that funds be transferred to an alternate account controlled by the fraudsters. The scenario is sometimes known as the bogus invoice scheme, supplier swindle, or invoice modification scheme.
2. The compromised email account of a high-level executive is used to ask an employee to transfer funds to the fraudsters' account. This scenario is sometimes known as CEO fraud, business executive scam, masquerading, or financial industry wire fraud.
3. Fraudsters use an employee's hacked personal email account to identify the company's vendors or business contacts and ask them to transfer funds to the fraudsters' account.
4. Fraudsters posing as the company's attorney contact an employee and request a transfer of funds to the fraudsters' account. The fraudsters often insist that the employee act quickly and secretly.
5. The compromised email account of a high-level executive is used to contact the company's human resources department and request employees' payroll data, tax information, or other personally identifiable information. Unlike traditional BEC schemes, this scheme seeks to obtain information about employees instead of money. Fraudsters then use the employee information to commit identity theft or one of the other BEC schemes described earlier.

NOTES

1. Estimated 2016 gross world product of US $79.58 trillion (www.cia.gov/library/publications/the-world-factbook/geos/xx.html), retrieved January 22, 2018.
2. www.wipo.int/about-ip/en/index.html
3. www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf

4. Because financial reporting standards can vary by jurisdiction, the details of those standards – and intentional violations thereof – are beyond the scope of this discussion. Consequently, the schemes discussed in this section reflect high-level accounting principles and the general approaches used to manipulate the financial statements; experts in applicable financial reporting standards should be consulted if financial statement fraud is suspected.
5. www.ic3.gov/media/2017/170504.aspx