GLOBAL EDITION

Accounting Information Systems

FIFTEENTH EDITION

Marshall B. Romney
Paul John Steinbart
Scott L. Summers
David A. Wood

Ppbig/123RF

Stephen VanHorn/Shutterstock

FuzzBones/Shutterstock

Accounting Information Systems

white-collar criminals - Typically, businesspeople who commit fraud. White-collar criminals usually resort to trickery or cunning, and their crimes usually involve a violation of trust or confidence.

corruption - Dishonest conduct by those in power which often involves actions that are illegitimate, immoral, or incompatible with ethical standards. Examples include bribery and bid rigging.

investment fraud - Misrepresenting or leaving out facts in order to promote an investment that promises fantastic profits with little or no risk. Examples include Ponzi schemes and securities fraud.

misappropriation of assets - Theft of company assets by employees.

better able to commit and conceal a fraud. The controls used to protect corporate assets make it more difficult for an outsider to steal from a company. Fraud perpetrators are often referred to as **white-collar criminals**.

There are a great many different types of frauds. We briefly define and give examples of some of those and then provide a more extended discussion of some of the most important ones to businesses.

Corruption is dishonest conduct by those in power and it often involves actions that are illegitimate, immoral, or incompatible with ethical standards. There are many types of corruption; examples include bribery and bid rigging.

Investment fraud is misrepresenting or leaving out facts in order to promote an investment that promises fantastic profits with little or no risk. There are many types of investment fraud; examples include Ponzi schemes and securities fraud.

Two types of frauds that are important to businesses are misappropriation of assets (sometimes called employee fraud) and fraudulent financial reporting (sometimes called management fraud). These two types of fraud are now discussed in greater depth.

MISAPPROPRIATION OF ASSETS

Misappropriation of assets is the theft of company assets by employees. Examples include the following:

- Albert Milano, a manager at *Reader's Digest* responsible for processing bills, embezzled $1 million over a five-year period. He forged a superior's signature on invoices for services never performed, submitted them to accounts payable, forged the endorsement on the check, and deposited it in his account. Milano used the stolen funds to buy an expensive home, five cars, and a boat.
- A bank vice president approved $1 billion in bad loans in exchange for $585,000 in kickbacks. The loans cost the bank $800 million and helped trigger its collapse.
- A manager at a Florida newspaper went to work for a competitor after he was fired. The first employer soon realized its reporters were being scooped. An investigation revealed the manager still had an active account and password and regularly browsed its computer files for information on exclusive stories.
- In a recent survey of 3,500 adults, half said they would take company property when they left and were more likely to steal e-data than assets. More than 25% said they would take customer data, including contact information. Many employees did not believe taking company data is equivalent to stealing.

The most significant contributing factor in most misappropriations is the absence of internal controls and/or the failure to enforce existing internal controls. A typical misappropriation has the following important elements or characteristics. The perpetrator:

- Gains the trust or confidence of the entity being defrauded.
- Uses trickery, cunning, or false or misleading information to commit fraud.
- Conceals the fraud by falsifying records or other information.
- Rarely terminates the fraud voluntarily.
- Sees how easy it is to get extra money; need or greed impels the person to continue. Some frauds are self-perpetuating; if perpetrators stop, their actions are discovered.
- Spends the ill-gotten gains. Rarely does the perpetrator save or invest the money. Some perpetrators come to depend on the "extra" income, and others adopt a lifestyle that requires even greater amounts of money. For these reasons, there are no small frauds—only large ones that are detected early.
- Gets greedy and takes ever-larger amounts of money at intervals that are more frequent, exposing the perpetrator to greater scrutiny and increasing the chances the fraud is discovered. The sheer magnitude of some frauds leads to their detection. For example, the accountant at an auto repair shop, a lifelong friend of the shop's owner, embezzled ever-larger sums of money over a seven-year period. In the last year of the fraud, the embezzler took more than $200,000. Facing bankruptcy, the owner eventually laid off the accountant and had his wife take over the bookkeeping. When the company immediately began doing better, the wife hired a fraud expert who investigated and uncovered the fraud.

- Grows careless or overconfident as time passes. If the size of the fraud does not lead to its discovery, the perpetrator eventually makes a mistake that does lead to the discovery.

FRAUDULENT FINANCIAL REPORTING

The National Commission on Fraudulent Financial Reporting (the Treadway Commission) defined **fraudulent financial reporting** as intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements. Management falsifies financial statements to deceive investors and creditors, increase a company's stock price, meet cash flow needs, or hide company losses and problems. The Treadway Commission studied 450 lawsuits against auditors and found undetected fraud to be a factor in half of them.

fraudulent financial reporting - Intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements.

Through the years, many highly publicized financial statement frauds have occurred. In each case, misrepresented financial statements led to huge financial losses and a number of bankruptcies. The most frequent "cook the books" schemes involve fictitiously inflating revenues, holding the books open (recognizing revenues before they are earned), closing the books early (delaying current expenses to a later period), overstating inventories or fixed assets, and concealing losses and liabilities.

The Treadway Commission recommended four actions to reduce fraudulent financial reporting:

1. Establish an organizational environment that contributes to the integrity of the financial reporting process.
2. Identify and understand the factors that lead to fraudulent financial reporting.
3. Assess the risk of fraudulent financial reporting within the company.
4. Design and implement internal controls to provide reasonable assurance of preventing fraudulent financial reporting.[1]

The ACFE found that an asset misappropriation is 17 times more likely than fraudulent financial reporting but that the amounts involved are much smaller. As a result, auditors and management are more concerned with fraudulent financial reporting even though they are more likely to encounter misappropriations. The following section discusses an auditors' responsibility for detecting material fraud.

SAS NO. 99 (AU-C SECTION 240): THE AUDITOR'S RESPONSIBILITY TO DETECT FRAUD

Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit*, became effective in December 2002. SAS No. 99 requires auditors to:

- ***Understand fraud.*** Because auditors cannot effectively audit something they do not understand, they must understand fraud and how and why it is committed.
- ***Discuss the risks of material fraudulent misstatements.*** While planning the audit, team members discuss among themselves how and where the company's financial statements are susceptible to fraud.
- ***Obtain information.*** The audit team gathers evidence by looking for fraud risk factors; testing company records; and asking management, the audit committee of the board of directors, and others whether they know of past or current fraud. Because many frauds involve revenue recognition, special care is exercised in examining revenue accounts.
- ***Identify, assess, and respond to risks.*** The evidence is used to identify, assess, and respond to fraud risks by varying the nature, timing, and extent of audit procedures and by evaluating carefully the risk of management overriding internal controls.
- ***Evaluate the results of their audit tests.*** Auditors must evaluate whether identified misstatements indicate the presence of fraud and determine its impact on the financial statements and the audit.

[1]Copyright ©1987 by the National Commission on Fraudulent Financial Reporting.

- ***Document and communicate findings.*** Auditors must document and communicate their findings to management and the audit committee.
- ***Incorporate a technology focus.*** SAS No. 99 recognizes the impact technology has on fraud risks and provides commentary and examples recognizing this impact. It also notes the opportunities auditors have to use technology to design fraud-auditing procedures.

Through the years there have been improvements to and reorganizations of auditing standards. The fraud standards are now referred to as AU-C Section 240.

Who Perpetrates Fraud and Why

When researchers compared the psychological and demographic characteristics of white-collar criminals, violent criminals, and the public, they found significant differences between violent and white-collar criminals. They found few differences between white-collar criminals and the public. Their conclusion: Many fraud perpetrators look just like you and me.

Some fraud perpetrators are disgruntled and unhappy with their jobs and seek revenge against employers. Others are dedicated, hard-working, and trusted employees. Most have no previous criminal record; they were honest, valued, and respected members of their community. In other words, they were good people who did bad things.

Computer fraud perpetrators are typically younger and possess more computer experience and skills. Some are motivated by curiosity, a quest for knowledge, the desire to learn how things work, and the challenge of beating the system. Some view their actions as a game rather than as dishonest behavior. Others commit computer fraud to gain stature in the hacking community.

A large and growing number of computer fraud perpetrators are more predatory in nature and seek to turn their actions into money. These fraud perpetrators are more like the blue-collar criminals that look to prey on others by robbing them. The difference is that they use a computer instead of a gun.

Many first-time fraud perpetrators that are not caught, or that are caught but not prosecuted, move from being "unintentional" fraudsters to "serial" fraudsters.

Malicious software is a big business and a huge profit engine for the criminal underground, especially for digitally savvy hackers in Eastern Europe. They break into financial accounts and steal money. They sell data to spammers, organized crime, hackers, and the intelligence community. They market malware, such as virus-producing software, to others. Some work with organized crime. A recently convicted hacker was paid $150 for every 1,000 computers he infected with his adware and earned hundreds of thousands of dollars a year.

Cyber-criminals are a top FBI priority because they have moved from isolated and uncoordinated attacks to organized fraud schemes targeted at specific individuals and businesses. They use online payment companies to launder their ill-gotten gains. To hide their money, they take advantage of the lack of coordination between international law enforcement organizations.

THE FRAUD TRIANGLE

For most predatory fraud perpetrators, all the fraudster needs is an opportunity and the criminal mind-set that allows him/her to commit the fraud. For most first-time fraud perpetrators, three conditions are present when fraud occurs: a pressure, an opportunity, and a rationalization. This is referred to as the fraud triangle, and is the middle triangle in Figure 8-1.

pressure - A person's incentive or motivation for committing fraud.

PRESSURES A **pressure** is a person's incentive or motivation for committing fraud. Three types of pressures that lead to misappropriations are shown in the Employee Pressure Triangle in Figure 8-1 and are summarized in Table 8-2.

Financial pressures often motivate misappropriation frauds by employees. Examples of such pressures include living beyond one's means, heavy financial losses, or high personal debt. Often, the perpetrator feels the pressure cannot be shared and believes fraud is the best way out of a difficult situation. For example, Raymond Keller owned a grain elevator where he stored grain for local farmers. He made money by trading in commodities and built a lavish house overlooking the Des Moines River. Heavy financial losses created a severe cash

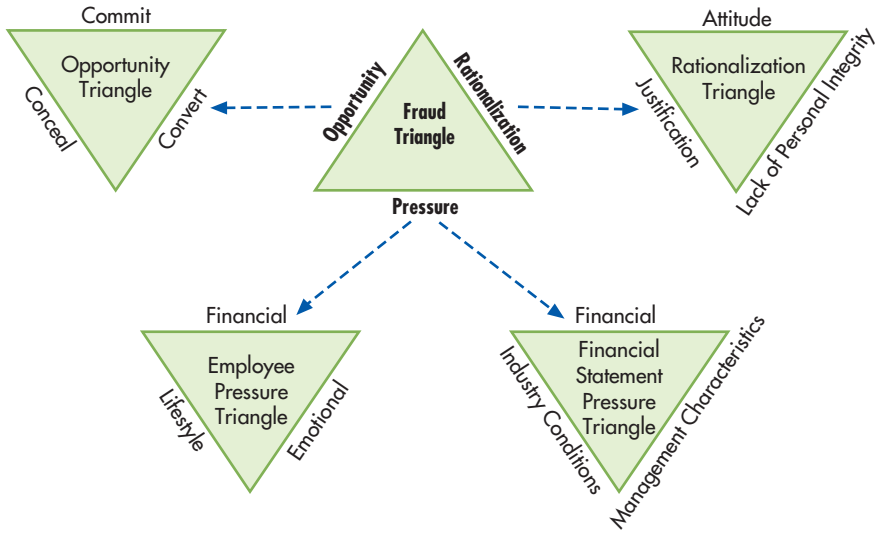

FIGURE 8-1
Fraud Triangle

shortage and high debt. He asked some farmers to wait for their money, gave others bad checks, and sold grain that did not belong to him. Finally, the seven banks to which he owed more than $3 million began to call their loans. When a state auditor showed up unexpectedly, Raymond took his life rather than face the consequences of his fraud.

A second type of pressure is emotional. Many employee frauds are motivated by greed. Some employees turn to fraud because they have strong feelings of resentment or believe they have been treated unfairly. They may feel their pay is too low, their contributions are not appreciated, or the company is taking advantage of them. A California accountant, passed over for a raise, increased his salary by 10%, the amount of the average raise. He defended his actions by saying he was only taking what was rightfully his. When asked why he did not increase his salary by 11%, he responded that he would have been stealing 1%.

Other people are motivated by the challenge of "beating the system" or subverting system controls and breaking into a system. When a company boasted that its new system was impenetrable, a team of individuals took less than 24 hours to break into the system and leave a message that the system had been compromised.

Some people commit fraud to keep pace with other family members or win a "who has the most or best" competition. A plastic surgeon, making $800,000 a year, defrauded his clinic of $200,000 to compete in the family "game" of financial one-upmanship.

TABLE 8-2 Pressures That Can Lead to Employee Fraud

Financial	Emotional	Lifestyle
Living beyond one's means	Excessive greed, ego, pride, ambition	Gambling habit
High personal debt/expenses	Performance not recognized	Drug or alcohol addiction
"Inadequate" salary/income	Job dissatisfaction	Sexual relationships
Poor credit ratings	Fear of losing job	Family/peer pressure
Heavy financial losses	Need for power or control	
Bad investments	Overt, deliberate nonconformity	
Tax avoidance	Inability to abide by or respect rules	
Unreasonable quotas/goals	Challenge of beating the system	
	Envy or resentment against others	
	Need to win financial one-upmanship competition	
	Coercion by bosses/top management	

Other people commit fraud due to some combination of greed, ego, pride, or ambition that causes them to believe that no matter how much they have, it is never enough. Thomas Coughlin was a vice-chairman of Walmart and a personal friend of founder Sam Walton. Even though his annual compensation exceeded $6 million, over a five-year period he had subordinates create fictitious invoices so that Walmart would pay for hundreds of thousands of dollars of personal expenses. These expenses included hunting vacations, a $2,590 pen for Coughlin's dog, and a $1,400 pair of alligator boots. Dennis Kozlowski and Mark Swartz, the CEO and CFO of Tyco International, were convicted of stealing $170 million from Tyco by abusing the company's loan program and by granting themselves unauthorized bonuses.

A third type of employee pressure is a person's lifestyle. The person may need funds to support a gambling habit or support a drug or alcohol addiction. One young woman embezzled funds because her boyfriend threatened to leave her if she did not provide him the money he needed to support his gambling and drug addictions.

Three types of organizational pressures that motivate management to misrepresent financial statements are shown in the Financial Statement Pressure triangle in Figure 8-1 and summarized in Table 8-3. A prevalent financial pressure is a need to meet or exceed earnings expectations to keep a stock price from falling. Managers create significant pressure with unduly aggressive earnings forecasts or unrealistic performance standards or with incentive programs that motivate employees to falsify financial results to keep their jobs or to receive stock options and other incentive payments. Industry conditions such as new regulatory requirements or significant market saturation with declining margins can motivate fraud.

opportunity - The condition or situation that allows a person or organization to commit and conceal a dishonest act and convert it to personal gain.

OPPORTUNITIES As shown in the Opportunity Triangle in Figure 8-1, **opportunity** is the condition or situation, including one's personal abilities, that allows a perpetrator to do three things:

1. ***Commit the fraud***. The theft of assets is the most common type of misappropriation. Most instances of fraudulent financial reporting involve overstatements of assets or revenues, understatements of liabilities, or failures to disclose information.
2. ***Conceal the fraud***. To prevent detection when assets are stolen or financial statements are overstated, perpetrators must keep the accounting equation in balance by inflating

TABLE 8-3 Pressures That Can Lead to Financial Statement Fraud

Management Characteristics	Industry Conditions	Financial
Questionable management ethics, management style, and track record	Declining industry	Intense pressure to meet or exceed earnings expectations
Unduly aggressive earnings forecasts, performance standards, accounting methods, or incentive programs	Industry or technology changes leading to declining demand or product obsolescence	Significant cash flow problems; unusual difficulty collecting receivables, paying payables
Significant incentive compensation based on achieving unduly aggressive goals	New regulatory requirements that impair financial stability or profitability	Heavy losses, high or undiversified risk, high dependence on debt, or unduly restrictive debt covenants
Management actions or transactions with no clear business justification	Significant competition or market saturation, with declining margins	Heavy dependence on new or unproven product lines
Oversensitivity to the effects of alternative accounting treatments on earnings per share	Significant tax changes or adjustments	Severe inventory obsolescence or excessive inventory buildup
Strained relationship with past auditors		Economic conditions (inflation, recession)
Failure to correct errors on a timely basis, leading to even greater problems		Litigation, especially management vs. shareholders
High management/employee turnover		Impending business failure or bankruptcy
Unusual/odd related-party relationships		Problems with regulatory agencies
		High vulnerability to rise in interest rates
		Poor or deteriorating financial position
		Unusually rapid growth or profitability compared to companies in same industry
		Significant estimates involving highly subjective judgments or uncertainties

other assets or decreasing liabilities or equity. Concealment often takes more effort and time and leaves behind more evidence than the theft or misrepresentation. Taking cash requires only a few seconds; altering records to hide the theft is more challenging and time-consuming.

One way for an employee to hide a theft of company assets is to charge the stolen item to an expense account. The perpetrator's exposure is limited to a year or less, because expense accounts are zeroed out at the end of each year. Perpetrators who hide a theft in a balance sheet account must continue the concealment.

Another way to hide a theft of company assets is to use a lapping scheme. In a **lapping** scheme, an employee of Company Z steals the cash or checks customer A mails in to pay the money it owes to Company Z. Later, the employee uses funds from customer B to pay off customer A's balance. Funds from customer C are used to pay off customer B's balance, and so forth. Because the theft involves two asset accounts (cash and accounts receivable), the cover-up must continue indefinitely unless the money is replaced or the debt is written off the books.

lapping - Concealing the theft of cash by means of a series of delays in posting collections to accounts receivable.

An individual, for his own personal gain or on behalf of a company, can hide the theft of cash using a check-kiting scheme. In **check kiting**, cash is created using the lag between the time a check is deposited and the time it clears the bank. Suppose an individual or a company opens accounts in banks A, B, and C. The perpetrator "creates" cash by depositing a $1,000 check from bank B in bank C and withdrawing the funds. If it takes two days for the check to clear bank B, he has created $1,000 for two days. After two days, the perpetrator deposits a $1,000 check from bank A in bank B to cover the created $1,000 for two more days. At the appropriate time, $1,000 is deposited from bank C in bank A. The scheme continues—writing checks and making deposits as needed to keep the checks from bouncing—until the person is caught or he deposits money to cover the created and stolen cash. Electronic banking systems make kiting harder because the time between a fraudster depositing the check in one bank and the check being presented to the other bank for payment is shortened.

check kiting - Creating cash using the lag between the time a check is deposited and the time it clears the bank.

3. ***Convert the theft or misrepresentation to personal gain***. In a misappropriation, fraud perpetrators who do not steal cash or use the stolen assets personally must convert them to a spendable form. For example, employees who steal inventory or equipment sell the items or otherwise convert them to cash. In cases of falsified financial statements, perpetrators convert their actions to personal gain through indirect benefits; that is, they keep their jobs, their stock rises, they receive pay raises and promotions, or they gain more power and influence.

Table 8-4 lists frequently mentioned opportunities. Many opportunities are the result of a deficient system of internal controls, such as deficiencies in proper segregation of duties, authorization procedures, clear lines of authority, proper supervision, adequate documents and records, safeguarding assets, or independent checks on performance. Management permits fraud by inattention or carelessness. Management commits fraud by overriding internal controls or using a position of power to compel subordinates to perpetrate it. The most prevalent opportunity for fraud results from a company's failure to design and *enforce* its internal control system.

Companies who do not perform a background check on potential employees risk hiring a "phantom controller." In one case, a company president stopped by the office one night, saw a light on in the controller's office, and went to see why he was working late. The president was surprised to find a complete stranger at work. An investigation showed that the controller was not an accountant and had been fired from three jobs over the prior eight years. Unable to do the accounting work, he hired someone to do his work for him at night. What he was good at was stealing money—he had embezzled several million dollars.

Other factors provide an opportunity to commit and conceal fraud when the company has unclear policies and procedures, fails to teach and stress corporate honesty, and fails to prosecute those who perpetrate fraud. Examples include large, unusual, or complex transactions; numerous adjusting entries at year-end; questionable accounting practices; pushing accounting principles to the limit; related-party transactions; incompetent personnel, inadequate staffing, rapid turnover of key employees, lengthy tenure in a key job, and lack of training.