11

CHAPTER

Security, Fraud, and Ethics

©CORBIS

skills that pay dividends

Convey a Professional Image

PHOTODISC

Strong relationships are fundamental to successful banking. Ongoing courteous, professional relationships between customers and bank representatives help maintain customer loyalty. Fair, prompt, and proactive service helps cement the relationship between businesses and banks. How do customers form their initial and ongoing impressions of a bank? What sways customers and businesses to select one bank over another? What can bankers do to put clients' minds at ease that the bank will carefully and thoughtfully handle their money?

A professional appearance of bank personnel helps influence customers' decision-making. Seeing bank staff look and act professional helps customers feel assured that their finances will be handled carefully and thoughtfully. Components of a professional appearance include personal grooming, clothing, and demeanor.

Each day you should go to work freshly showered. Hair should be neat. Fingernails should be well groomed. Remember, if you and a customer are exchanging forms or if you are counting out money to give to a customer, your hands will be quite visible. Perfume or cologne should be used moderately. Teeth should be brushed and your breath should be fresh. If you have body piercings or tattoos in nontypical, visible locations, you should consider how seeing those will influence customers' opinion of both you and your bank.

The banking industry tends to be conservative. You should select outfits that are appropriate to the industry. Trendy outfits that may make you a fashion leader in social situations may not be appropriate for the workplace. Classic, conservative styles are a better long-term wardrobe investment. Classic styles do not look dated as quickly as trendy styles. You can still inject your own personal or creative touches in a professional outfit through careful accessory selection. A well-coordinated scarf or tie can add some pizzazz to your outfit.

Match your clothing selection to the specific requirements of your job, your customer, and your agenda for the day. For example, if you are going to your customer's worksite to do a presentation on services your bank can offer to employees, a suit is probably most appropriate. If you are participating in a golf outing with the same customer on another day, then golf attire would be appropriate.

Your demeanor toward customers should be cheerful, respectful, and helpful. In most situations, sticking to the professional facts pertaining to the business situation is appropriate. Personal discussions regarding religion or politics should be avoided. You should demonstrate a knowledge of your industry and of current events that extends beyond the particular transaction you are conducting with the customer.

Develop Your Skill

Visit three workplaces in different industries. Observe the appearance of various staff members. Take notes on how the job duties of staff members affected their appearance. Reflect on how the appearance of staff members impacted your opinion of not only the employees, but of the business. Be prepared to share your observations with the class.

11.1

goals

- Discuss how security measures can prevent bank robbery.
- Describe what bank employees should do during a robbery.

terms

- bandit barrier

Robbery Prevention and Response

Banking Scene

Cheyenne Rainwater has read about the recent increase in bank robberies in her city and is concerned. She knows that her money is protected, but she doesn't want to be present for one of these terrible events, which have resulted in harm to bystanders from time to time. What are some things she should look for that indicate her bank is trying to prevent robberies?

Security as Prevention

When asked why he robbed banks during the 1930s and 1940s, notorious bank robber Willie Sutton simply replied, "Because that's where the money is." You might think that bank robbery in today's world is merely a plot line for television and movies, but it is a reality and actually occurs all too often. Armed robbery is an inherent risk associated with financial institutions. According to the Federal Bureau of Investigation, 7,175 bank robberies—which are federal offenses—occurred in the United States during the year 2007, a 5 percent decrease over the number in the previous year. Every bank is a potential temptation to would-be robbers. Despite all of the expensive and state-of-the-art measures banks have invested in to prevent robberies, make them unprofitable, and enhance the capture and conviction of the perpetrator, robberies are a persistent problem.

Physical Security

Ensuring the security of assets, employees, and customers is a major concern for financial institutions. Physically securing the bank is an important deterrent to robbery. It's easy to picture vaults and safe-deposit boxes when you think of physical security at banks. Locking devices are certainly part of the business, but physical security includes other considerations sometimes less obvious.

- **Building design plays a role in physical security.** Everything from resistance to attack to placement of sprinklers is a consideration in facility design. Planning the facility for technology, control of physical access to the building, location and security of records, and even the types and placement of furniture are part of an integrated security plan. The bank should be well lit with the lights positioned so that they do not interfere with processing images of perpetrators captured on security video or film. The view of tellers by other employees should be unobstructed.

- **Surveillance and alarm technology continues to evolve.** Increasingly sophisticated devices with higher and higher resolution are appearing in banks. From closed-circuit television (CCTV) systems to monitoring software for all phases of processing operations, forms of surveillance are becoming increasingly complex. Surveillance cameras should be placed so they are seen by possible robbers and positioned to ensure a full front photograph of the robber.
- **Safety devices can be used.** Bandit barriers, which are bulletproof plastic shields, can be positioned in front of each teller's station. Popup security screens, which rise in a fraction of a second out of the counter to protect the teller, may also be used. Time-delay locks that require a PIN and allow access to the safe only during specific hours can be installed.
- **Transportation security is a part of physical security.** With the necessity of safeguarding cash and checks in transit, transportation security involves screening of employees involved in transportation. Companies providing this service are liable for the actions of employees.

Best Practices Recommendations

It is wise for a bank to adopt a list of "best practices" to help deter bank robberies and to aid in the apprehension of bank bandits. Some measures prevent robberies, some protect staff and customers during a robbery, some help apprehend the criminal, and some accomplish a combination of these objectives. Training is a critical factor in carrying out the best practices.

Training is the core of preventing robbery. For this reason, banks invest a lot of resources in teaching their employees how to recognize and what to do in an emergency. These procedures both lessen the risk of harm for staff and customers and minimize financial loss to the institution.

Most banks are required by law to install surveillance cameras and alarms, and properly trained staff can aid in ensuring that security devices work accurately and are used during a robbery. Security guards, customer service representatives, or others should engage customers as they enter the bank to present a plain view of the security presence and make potential robbers aware that they could be recognized later.

PHOTODISC/GETTY IMAGES

tech talk

Taking Technology To the Limits To Prevent Robberies

In the early 1990s in Los Angeles, as the number of bank robberies, particularly violent ones, soared, FBI and financial institutions worked together to address this problem. Subsequently, banks deemed "robbery-prone" constructed bullet-resistant "bandit barriers" or access control units (ACUs). The clear, bullet-resistant, Plexiglas partitions completely enclose the teller and adjacent cash storage areas from the top of the counter to the ceiling or from the floor to the ceiling at the entrance. The ACUs consist of an electronically controlled, double-door entrance and adjacent exit. Customers access the inside of the bank, one at a time, by entering through the entry's outer door. When the outer door closes, a device conducts an automatic magnetometer-type search for weapons. If the search proves negative, the inner door automatically unlocks, allowing entry into the facility. If the search yields a positive result, indicating a possible weapon, the bullet-resistant second door remains locked, and the person must retreat from the entry.

Think Critically How would you feel about doing your banking in a bank that uses "bandit barriers" and ACUs?

✔ checkpoint

What factors do you believe are responsible for bank robberies?

Robbery Preparation

Just as tellers are usually the first to do business with customers, they are the first line of defense during a robbery. It is critical that teller training include what to do and *not* to do during a holdup. Training should emphasize that physical resistance is dangerous, not helpful. Tellers should do nothing that would risk their safety or that of others on the premises. Training should also include these instructions:

- Remain calm. Knowing what to do through training eliminates the need to make decisions during the crisis.
- Obey the robber's instructions. Employees should be assured that this is bank policy.
- Trigger foot-pedal or bill trap alarms and security cameras as soon as possible both to protect the safety of customers and employees and to help apprehend the robber. A *bill trap* is a device that sets off a security

system when a bill or switch is pulled.

PHOTODISC/GETTY IMAGES

- Use decoy or marked money or specially prepared packs that contain an exploding device with a dye to mark the cash. Drop a satellite-tracking device into the bag of money.
- Call 911 as soon as reasonably possible to provide a detailed description of the perpetrator and the direction he or she seemed to be heading after fleeing the bank.
- Keep anything, such as a demand note, when possible for fingerprint identification, and minimize contamination of evidence and the crime scene. Countertops are ideal places on which bandits leave fingerprints.
- Note the robber's physical characteristics, particularly any outstanding feature. Also, if possible, note any characteristics of the get-away vehicle, such as the make, model, color, and license plate number.
- Write a description of the robber as soon as possible because memory fades quickly, especially in crisis situations. A robbery description form, such as the one below, can be used to help authorities gather information.

ROBBERY DESCRIPTION FORM (Sample)

Sex ______________ Age ______ Race ______________ Height _______ Weight ______

Build ___________________ Complexion (light, dark, etc.) ___________________

Hair ___________ Eye Color ______ Facial Hair Beard _____ Mustache _____ Goatee, etc. ____

CLOTHING

Hat ___________________________________

Shirt __________________________________

Coat or jacket (length and color) ___________

Trousers (color and style) _________________

Tie ____________________________________

Shoes __________________________________

Other __________________________________

MISCELLANEOUS

Weapon _______ Type ____________________

Speech ________________________________

____

Mannerisms _____________________________

____

Physical characteristics __________________

(limp, deformities, etc.) __________________

It is not uncommon for tellers to become paralyzed with fright during a robbery, leading them to forget procedures for safety and suspect identification. To avoid this situation, some banks provide training at teller schools several times per month and at high-risk banks at least annually. Individual branches reinforce the lessons through practice drills and at staff meetings. By doing so, the tellers are more likely to remember how to react during a robbery without endangering customers or employees.

Other employees at the bank play a critically important role by being sensitive to a tellers' body language and demeanor. For example, a change in a teller's voice tone or pitch could indicate that a holdup is in process. A normally relaxed teller who tenses up or a chatty one who becomes quiet could indicate trouble. In one Seattle bank, for instance, a coworker who noticed that sounds from a normally lively teller had become stiff realized that a robbery was occurring and triggered an alarm.

Types of Bank Robberies

Although bank employees can never be fully prepared for a bank robbery, it may be helpful for them to know the different types of robberies that commonly occur to help plan the appropriate actions to take.

Morning glory robberies take place prior to opening the bank for the day. The morning glory robber could break in and wait for employees to arrive, seize the employees outside the bank as they arrive, use a ruse tactic to attempt to enter the bank, or even seize an employee en route to or from work or at the employee's home. In a *takeover* bank robbery, two or more robbers carry weapons and invade the bank. This is the least common type of robbery. The most common type of bank robbery committed involves *note passing*. In this case, the robber enters the bank and passes a note to a bank employee. The note demands money. The robber may issue a verbal demand instead of passing a note. Weapons may be displayed in all types of robberies as a means of intimidating and coercing bank employees.

The FDIC as a Safety Net

When robberies occur, it is important that consumers understand that the Federal Deposit Insurance Corporation (FDIC) insures deposits in banks and thrift institutions for up to $100,000 per depositor in the event of failure. As part of the Emergency Economic Stabilization Act of 2008, FDIC insurance coverage per depositor was increased to $250,000 through 2009. Although it is unlikely that a robbery could result in bank failure, FDIC provides safety for individual accounts.

✓ checkpoint

Why is it important that bank employees not resist a robbery attempt?

assessment 11.1

Think Critically

1. How does the building facility design contribute to the physical security of a bank?

2. Closed-circuit television systems and security cameras are part of the technology that can identify suspects in bank robbery cases. What role do they play in preventing robberies?

3. Why are robbery training and preparation critical for bank employees, especially tellers?

4. In your opinion, what is the best deterrent in preventing robberies?

Make Academic Connections

5. **Communication** Visit a local bank to find out what types of security measures it uses and employee training/preparation for robberies it offers. Present your findings in an oral report.
6. **Research** Internet banking presents new security challenges for financial institutions. Use the Internet to investigate what the most important issues are and how they are being resolved. Prepare a two-page report summarizing your findings.
7. **History** Study the bank robberies during the Great Depression. Why did the Secret Service become involved instead of leaving the crimes to local law enforcement?

11.2 Ethics in Banking

goals

- Explain how ethics applies to financial institutions.
- Identify ethical dilemmas that occur in banking.

terms

- ethics
- code of ethics
- conflict of interest

Banking Scene

Recent scandals related to unethical and illegal activities have rocked the corporate world. Several banks have been involved. What can Cheyenne Rainwater do to determine whether her bank seeks to emphasize ethical behavior among its employees?

Ethical Behavior

Ethics can be defined as the process of determining standards and procedures for dealing with judgmental decisions affecting other people. Ethics refers to beliefs that distinguish right from wrong. An *ethical dilemma* involves a situation that is problematic and makes a person question what is the "right" or "wrong" thing to do. Ethical dilemmas make individuals think about their obligations, duties, or responsibilities. These dilemmas can be highly complex and difficult to resolve. Easier ones involve a right versus wrong answer. Most people will agree, for example, that it is unacceptable to pretend that someone else's work is your own. However, complex ethical dilemmas involve a decision between "right" and "right." An example might occur if you uncover a colleague's error. To whom are you obligated—your colleague or your employer? "There is only one way for a business to convince the public that it is ethical," says Gerald H. Lipkin, chairman, president, and CEO of Valley National Bancorp, "and that is to build a record of dealing fairly with its customers, communities, shareholders, and employees."

A **code of ethics** is a statement adopted by the management and board of directors of businesses to guide employees in taking appropriate actions in critical situations that could reflect on the organization. A code can help employees answer questions about a bank's policy on matters such as receiving gifts from customers and taking outside jobs. Most banks require employees to read the code regularly and certify that they are in compliance with its provisions. KPMG, the international accounting firm, found in its 2000 Organizational Integrity Survey that the ethical behavior of top executives affects employees' perception of their companies. Overall, 69 percent of the 2,390 employees of the companies surveyed believed that their current customers would recommend their company to others. But when employees believed management would uphold the company's stated ethical standards, that number shot up to 80 percent.

Important Elements in a Code of Ethics

Most banking codes of ethics include the following.

PHOTODISC/GETTY IMAGES

- **Confidentiality** Banking business is confidential, so only authorized individuals can receive information.
- **Dishonesty and fraudulent behavior** Such behavior will not be tolerated.
- **Representation of the institution** The behavior of employees must positively reflect the bank's integrity.
- **Gifts** Accepting gifts or money given to influence employees' performance of duties is strictly prohibited.
- **Financial management** All employees should practice wise financial management. Customers won't trust a bank to take care of their funds if its employees can't take care of their own money.
- **Conflict of interest** Employees must act with honesty and integrity, avoiding any personal activity, investment, or association that could appear to interfere with good judgment concerning the bank's best interests. A **conflict of interest** occurs when two interests are at cross-purposes. Employees are strictly prohibited from exploiting their position or relationship with the bank for personal gain.
- **Compliance with laws and regulations** Employees are required to provide full, fair, accurate, timely, and understandable disclosure in reports and documents that the bank files. Employees must perform their duties in accordance with all applicable laws and regulations.
- **Responsibility for violations** The conduct of employees can reinforce an ethical atmosphere and positively influence the conduct of their colleagues. Employees who are unable to stop suspected misconduct or discover it after it has occurred are required to report it immediately to the appropriate management.

When a bank develops its code of ethics, it must decide what it wants to stand for and then put appropriate information in writing (often in the company handbook or on the company website), discuss it with its employees, and then enforce it. This policy reflects the values that the bank has determined to be important.

✓ checkpoint

What is the purpose of a code of ethics?

Ethical Issues in Banking and the Corporate World

At the beginning of the twenty-first century, a wave of corporate scandals broke out in the United States. A number of leading companies admitted that they had violated numerous regulations, including misstating their accounts, in order to project a positive impression of their status. In public companies, this type of "creative" accounting can be considered fraud. These companies violated both regulatory rules and accepted ethical practices. Unfortunately, the list could go on.


PHOTODISC/GETTY IMAGES

- PNC Financial Services Group Inc. reached a resolution with the Securities and Exchange Commission regarding charges that in violation of generally accepted accounting principles, PNC transferred from its financial statements approximately $762 million of volatile, troubled, or underperforming loans and venture capital assets. In addition, PNC issued a materially false and misleading press release that, among other things, overstated its 2001 full-year earnings per share by 52 percent.
- U.S. Bancorp settled a lawsuit brought by the Attorney General of Minnesota over the bank's sales of customer data to MemberWorks, a telemarketing company, for $4 million and a 22 percent commission on sales to those customers. The bank promised to end third-party sharing of information for marketing of nonfinancial products and provide customers the opportunity to opt out of affiliate-sharing of information for the purposes of selling additional company services.
- Citigroup Inc. agreed to pay $215 million to resolve charges that its Associates First Capital Corporation and Associates Corporation of North America had engaged in systematic and widespread deceptive practices designed to encourage borrowers to unknowingly purchase optional credit insurance products. It also participated in abusive lending practices.
- Enron Corporation, the energy trading and communications company based in Houston, Texas, used fraudulent accounting techniques that, when uncovered, caused it to become one of the largest corporate failures in history. It has become the symbol of institutionalized and well-planned corporate fraud.

- Merrill Lynch & Co., Inc., an investment banking company recognized as one of the world's leading financial management and advisory companies, reached an agreement in 2003 with New York State's attorney general on charges the firm's investment advice was influenced by conflicts of interest.
- Arthur Andersen, founded in 1913 and one of the Big Five U.S. accounting firms, was forced to cease business after accounting scandals involving Waste Management, Sunbeam, and Enron. Revelations of fraud in presenting Enron's financial statements and its felony conviction for obstructing justice for shredding tons of Enron documents led to the firm's demise.

Sarbanes-Oxley Act of 2002

On July 30, 2002, the *Public Company Accounting Reform and Investor Protection Act of 2002* (the *Sarbanes-Oxley Act of 2002*), also called SOX, was signed into law. It established a new Public Company Accounting Oversight Board with the power to set rules, investigate suspected wrongdoing, punish violators, and conduct regular inspections of accounting firms. The act gives broad new protections to corporate whistle blowers—employees who publicly report illegal activities occurring inside their company—and makes security fraud a criminal offense. A chief executive officer or chief financial officer who certifies false financial reports could get 20 years in prison and be fined $5 million. Shredding documents could result in a 20-year sentence. This act also places restrictions on loans by corporations to their executives. These restrictions strive to eliminate the interest-free loans that became a popular form of compensation for executives.

Ethics in Action

Billionaire-populist Warren Buffett is one of the richest men in the world and is chairman of the board and chief executive officer of Berkshire Hathaway Inc. In his 1998 letter to company shareholders, Mr. Buffett stated that "a significant and growing number of otherwise high-grade managers … have come to view that it's okay to manipulate earnings to satisfy what they believe are Wall Street's desires. Indeed, many CEOs think this kind of manipulation is not only okay, but actually their duty. They also argue that in using accounting shenanigans to get the figures they want, they are doing only what everybody else does."

Think Critically

What ethical responsibility do employees at firms whose managers share this view owe to the company, the business community, and the public in general?

PHOTODISC/GETTY IMAGES

Everyday Ethical Dilemmas in Banking

The Sarbanes-Oxley Act addresses the behavior of corporate executives, but all bank employees, including tellers, accountants, loan officers, marketing directors, and customer service representatives, also face ethical dilemmas. Consider the ethical dilemmas in the following scenarios and the proper ethical action to take in each case.

- Luisa Sillas realizes that her immediate supervisor, who orders the bank's supplies, is taking kickbacks to order from several suppliers.
- Jerry Cappocci is a teller who processed the deposit of a rather confused customer for $1,600. The customer actually gave him $1,600 in checks and $75 in cash without realizing it.
- Several years ago while working with a client, Tanisha Higgins learned confidential information about the company's research. It is now planning to go public, and the information she learned indicates that purchase of its stock will be an excellent investment.
- Susan Issacs works for the marketing director of a large bank. She is sure that the facts of a new advertising campaign for bank loans are misleading but was told things were "okay."

Ethical Behavior as the Final Decision

Banking is an essential service like the supply of water, electricity, and police protection. As a result, ethics should be the ultimate factor in making decisions in the financial world. Banks must provide safe and convenient places for customers to take care of their financial needs. In providing essential services, bankers must be dedicated to giving advice based on the particular customer's financial position and situation in general, including loan and investment choices, willingness to take risks, and ability to assess the impact of the advice provided. Bankers should ensure that sufficient information about the bank's products and services is available to customers.

✓ checkpoint

What is it necessary to provide special protection to corporate whistle-blowers?

assessment 11.2

Think Critically

1. Discuss how ethical dilemmas could involve making decisions between "right" and "right."
2. Why is confidentiality a critical element in banking?
3. Discuss the ethical implications of the ability of a bank to determine the interest rate for a loan.
4. Why did Congress and the President see the need for the Sarbanes-Oxley Act?

Make Academic Connections

5. **Technology** Use the Internet to find out about ethical issues regarding online banking that are of concern to bank regulators. Present your findings to the class orally.
6. **Research** Locate the websites of three commercial banks that have a code of ethics. List any elements not covered in this chapter.
7. **Problem Solving** As a supervisor, you must decide what to do about a loyal, honest employee who tries really hard but can't perform up to par, forcing coworkers to pick up the slack. You know that the employee is a single parent whose child has serious medical problems. What do you do?

11.3 Fraud and Scams

goals

- Identify types of fraud that are committed against banks.
- Discuss mortgage-based scams.

terms

- fraud
- check kiting
- forgery
- check counterfeiting
- scam
- house flipping
- straw buyer

Banking Scene

Cheyenne Rainwater has learned from the news media that several people in her city have been victims of checking account scams. What can she do to protect herself from these crimes?

Fraud Related to Banking

Although robbery is a concern for banks, far larger dollar values are lost through computer crime, vandalism, and various forms of fraud. **Fraud** is a deception deliberately practiced to secure unfair or unlawful gain. During 2007, it was estimated that the total amount of online fraud in the U.S. was about $240 million. The average victim lost about $2,500. The sheer volume of check and credit card transactions presents many opportunities for the unscrupulous. Various forms of fraud, some simple and some sophisticated, cost banks and consumers billions of dollars a year. Fighting and preventing these crimes is a never-ending part of the banking industry.

Fraud prevention occupies more resources of the banking industry than any other activity except routine processing. Bank administration is an important part of fraud prevention. Adhering to established procedures, including technology security rules, insisting on careful record keeping, conducting audits, and investigating suspicious activities of employees or customers are all part of an overall plan for security and fraud prevention.

Employee training may be the best return on investment for fraud prevention. Detailed checklists for ways to identify questionable or counterfeit checks, identification verification procedures, and frequent updates on new types of counterfeit and fraud schemes all help combat fraud on the front lines. Tellers, operations personnel, technicians, investment counselors, loan officers, and other personnel require training.

Consumer education is an effort that banks see as increasingly worthwhile. Most frauds are crimes of opportunity, and if consumers protect their checks, credit cards, identities, and account information more carefully, committing fraud becomes a more difficult task.

Counterfeit Currency and New Design

Counterfeiting money has been a crime throughout the history of the United States. It was a serious problem during the nineteenth century when banks issued their own currency. At the time of the Civil War, it was estimated that one-third of all currency in circulation was counterfeit. The adoption of a national currency in 1863 did not, as expected, solve the counterfeiting problem. On July 5, 1865, the United States created the Secret Service to suppress counterfeiting. More recently, in 2006, an estimated $62 million dollars was lost in the U.S. due to counterfeiting. Nearly 4,000 people were arrested for crimes relating to the counterfeiting.


BUREAU OF ENGRAVING & PRINTING

To address the continuing "funny money" problem, in 2003 the Federal Reserve began issuing redesigned bills. To date, the $5, $10, $20, and $50 bills have been redesigned. The most noticeable difference in the new $20 notes is the use of subtle green, peach, and blue colors featured in the background. The new $20 note design retains three important security features:

- The watermark, the faint image similar to the large portrait, which is part of the paper itself and is visible from both sides when the bill is held up to the light.
- The vertical strip of plastic making up the security thread—also visible from both sides when held up to the light—is embedded in the paper. "USA TWENTY" and a small flag are visible on the thread.
- The color-shifting ink—the numeral "20" in the lower-right corner on the face of the note—changes from copper to green when the note is tilted. The color shift is more dramatic and easier to see on the new notes.

Check Fraud

Statistics indicate the seriousness of check fraud. In a recent eight-month period, postal inspectors seized more than $2 billion of fake checks. The advancement of computer technology has made it increasingly easy for criminals, either individually or in organized groups, to manipulate checks to deceive unknowing victims. Desktop publishing and copying to create or duplicate an actual financial document are responsible for a significant amount of check fraud today. In most cases, these crimes begin with the theft of a financial document, such as a blank check, taken from your home or vehicle during a burglary, a canceled or old check you threw away, or a check you just put in your mailbox. Two of the most common schemes directed at banks are check kiting and money laundering. Other check fraud includes forgery, counterfeiting or alteration, and paperhanging.

Check Kiting The fraud of **check kiting** requires opening accounts at two or more institutions and using "the float time" of available funds to create fraudulent balances. A person draws a check for an amount that exceeds the account balance at one bank and then deposits it at another bank. Before that deposit can be processed, the individual draws a check on the second bank to deposit at the first bank. Although neither bank account has

interesting *facts*

The National Consumers League is America's oldest nonprofit consumer group. In 1996 it launched Internet Fraud Watch to prevent online and Internet fraud by helping people recognize possible scams. The most common fraud signs on the Internet are incredibly low prices, extravagant promises of profits, guarantees of credit regardless of bad credit histories, or prizes that require payment to obtain.

enough money to cover the checks, the person may withdraw more than the collected balance from the first account.

Check kiting has become easier in recent years due to the Expedited Funds Availability Act of 1987, which requires banks to make funds available sooner. The Check 21 Act passed in October 2003 has probably helped counteract this problem. Instead of requiring physical possession of a paper check by the issuing bank before funds are transferred, the Check 21 Act allows the receiving bank to treat an electronic image of the check, called an Image Replacement Document (IRD), the same as the check itself. This significantly reduces the check clearing process time and has the power to help eliminate check kiting.

Money Laundering The scheme of money laundering received its name because criminals use it to make money "clean." Criminals use the process to conceal illicitly acquired funds by converting them into seemingly legitimate income. Originally used to refer to the proceeds of organized crime, the term is now often associated with financial activities of drug dealers who seek to launder the large amounts of cash they generate from the sale of narcotics. Money laundering does not cause financial institutions a loss, but it makes large sums of money difficult to trace.

To help combat money laundering, Congress has passed several laws. The Bank Secrecy Act requires financial institutions to report suspicious transactions that may be a possible violation of law. This act creates a paper trail for currency so that money can not be deposited, invested, or exchanged in a way that conceals its illegal source. This discourages the use of banks to hide transfers or deposits of money derived from criminal activity.

The Patriot Act of 2001 prohibits financial relationships with banks that have no physical presence in their host county. Under this act, banks must use

Banking Math *Connection*

Many insurance policies currently will protect for losses caused by the acceptance in good faith of counterfeit money. Most pay from $500 to $1,000 for a loss. During a garage sale, a family unfortunately accepted $500 in counterfeit bills for a purchase. The family's insurance policy covered losses from counterfeit money up to $700 with a $200 deductible. Did the family experience a loss from this transaction? If so, how much?

Solution

Because the loss is less than the $700 ceiling, the formula for determining loss is

Amount of loss − Deductible = Amount covered
$500 − $200 = $300

The insurance covers $300, so the actual out-of-pocket loss is $200 ($500 loss − $300).

due diligence to determine the identity and source of transactions. The Patriot Act seeks to curtail the financing of terrorism with laundered money.

Forgery Check **forgery**, or counterfeiting a check or other document with the intent to defraud, is difficult to spot. Criminals steal a check, endorse it with a forged or unauthorized signature, and, using fake identification, present it for payment at a retail location or a bank.

Counterfeiting and Alteration **Check counterfeiting** can mean either entirely creating a check with desktop publishing equipment (personal computer, scanner, cutting-edge software, and top-grade laser printer) or simply duplicating a check with advanced color photocopiers. *Alteration* removes or modifies handwriting and information on the check with chemicals and solvents such as acetone, brake fluid, and household bleach.

Paperhanging The act of purposefully writing checks on closed accounts or reordering checks for closed accounts is *paperhanging*. It is also known as *closed account fraud*.

Signs of Counterfeit Checks

Several signs can indicate a bad check. Telling signs are lack of perforations, a low number (such as 101 through 400 on personal checks or 1001-1500 on business checks), or no address for the customer or the bank. Stains or discoloration perhaps caused by erasures or alterations are other signs. Be alert to the Magnetic Ink Character Recognition coding number printed along the bottom: if it is shiny, if it does not match the check number, or if it is missing.

The first and probably most important line of defense against counterfeit checks is teller training. Knowing how to verify a check and what to look for on a suspicious one is the focus of training efforts.

Consumer Tips for Preventing Check Fraud

Checks are the most common negotiable instrument and should be treated as carefully as cash. Here are some steps to prevent check fraud.

- Use checks that have built-in security features. Many of these checks have a padlock icon on them to indicate the presence of enhanced security features such as watermarking and microprinting.
- Don't have your social security number imprinted on checks. Your SSN is enough for a criminal to get a credit card, bank account, or fake loan.
- Don't endorse a check until just before you cash or deposit it. It is better, in fact, if you sign the check in a teller's presence.
- Don't leave spaces on checks. Draw horizontal lines to fill any blank spaces, and write words close together, especially on amount lines.
- Reconcile your account regularly. Call your bank immediately if you notice any suspicious transactions on your statement.
- Shred statements, canceled checks, ATM slips, and credit card receipts, rather than just throwing them in the trash.

"communicate"

Conduct a poll of at least 10 people in your community about checking account scams. Have they experienced any attempts to obtain their checking account information that they thought were suspicious? If so, what were the circumstances?

- Be careful on the phone, in person, and on the Web. Never give out account information or numbers to anyone you don't know or of whom you are not certain. Don't be afraid to contact authorities.

checkpoint

How has computer technology affected counterfeit checking scams?

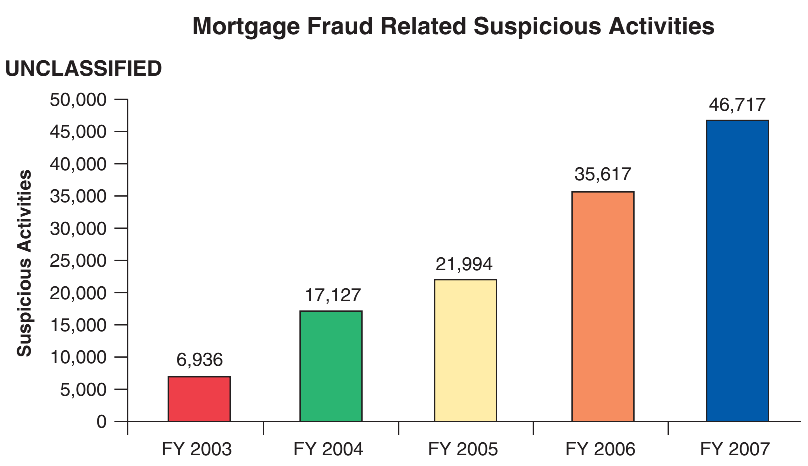
Mortgage-Based Scams

Scam is a slang term for something that is fraudulent or a swindle. When a scam is perpetrated, trickery is used to intentionally dupe an individual or business into a transaction for the financial benefit of the thief. Available scams are limited only by the creativity of the thief.

Illegal Mortgage Practices

The recent mortgage and financial crisis put a lot of pressure on people throughout the economy. Businesses affected ranged from those who supply the raw materials to build a house through those that provide the décor for a finished home. Increased pressure to compensate for lost income due to tightened credit and reduced home sales has made many participants in the housing industry vulnerable to illegal schemes.

The FBI's *2007 Mortgage Fraud Report* highlighted common schemes. According to their research, between 2003 and 2007, reported instances of mortgage fraud rose from about 7,000 cases to about 47,000 cases. The graph provides a detailed overview of the increased incidents of fraud. Successful schemes resulted in financial losses to financial institutions. Some of the schemes are summarized below.



Source: *Federal Bureau of Investigation 2007 Mortgage Fraud Report*

Illegal House Flipping **House flipping** commonly refers to the practice of buying a house for below market value and selling the house at or above market value. Oftentimes an increased sale price is obtained either because renovations were made to the home or because a distressed seller originally sold the house at below market value. This process becomes illegal if a fraudulent appraisal, which artificially inflates the value of the house, is used to secure a loan by a second buyer. In some schemes, a straw buyer is used to help with

flat world...

Scam Targets New Zealanders

In 2003, a slick online banking scam fooled New Zealanders into losing large sums of money. A website with a professional look and claiming to be business partners with all leading New Zealand banks was customized for New Zealand readers. The scam worked by convincing people to accept deposits into their bank accounts and then to send the funds minus a transaction fee to a third party. Of course, the initial deposit is then canceled. For example, a scam "associate" might deposit $14,000 into the account of a New Zealander, who then sends $13,500 on to someone else as soon as possible on the same day. The scammer then quickly cancels the $14,000 deposit. The result: The unlucky New Zealander has lost his or her own $13,500 sent to its perpetrators.

Think Critically What do you think can be done to protect people from scams such as the one in New Zealand?

the scheme. A **straw buyer** is someone who agrees to use their personal information to buy the home at a falsely inflated price. The straw buyer agrees to state that they intend to live in the home even though their actual intent is to flip the home. Sometimes a straw buyer knows that they are participating in a fraudulent scheme and sometimes they themselves are victims.

Profits from illegal house flipping can be obtained by intentionally defaulting on a loan. For example, Buyer A purchases a house for $30,000 and then has it fraudulently appraised for $100,000. Buyer A solicits the help of Buyer B, a straw buyer, to purchase the house for $100,000 by obtaining a bank loan for $80,000. Buyer B does not plan to move in to the house and plans to default on the loan. An illegal profit of $50,000 is available to be shared between Buyer A and Buyer B. (An $80,000 loan minus the initial $30,000 investment in the house.) The bank is then left with a loss of $50,000. This loss arises because the bank has an $80,000 mortgage on a house that has a true value of $30,000. According to the FBI, if the loan was FHA-insured, then the loss is absorbed by the government.

Other Mortgage-Based Schemes A variety of other schemes exploit the same concepts of illegally inflating the value of a house, obtaining financing to pay for the inflated value, and defaulting on loans for personal gain. Names of some of these schemes include *Builder-Bailout Schemes*, *Seller Assistance Scams*, *Short-Sale Schemes*, and *Foreclosure Rescue Scams*.

✓ checkpoint

What is the necessary step in the process to ensure that an illegal house flipping scheme achieves a profit?

assessment 11.3

Think Critically

1. How have $20 bills been redesigned to prevent counterfeit scams?

2. Discuss how a person could commit check fraud on your account. When are you likely to first be aware that you've been a victim of the scam?

3. How does mortgage fraud generate a profit for participants?

4. Why have mortgage-based schemes been rising over the last few years?

Make Academic Connections

5. **Communication** Talk to a local bank official about check fraud. Does the bank use any technological devices to identify counterfeit checks? If so, explain them in a one-page report.

6. **Banking Math** If you accept counterfeit bills in payment for a $650 antique you sell at a flea market, what will be your actual loss if your insurance has a $900 limit and a $225 deductible?

Identity Theft

11.4

goals

- Explain the concept of identity theft.
- Describe various identity theft methods.
- Discuss identity theft prevention.

terms

- spam
- phishing
- war driving
- sniffer program
- fraud alert
- credit freeze

Banking Scene

Cheyenne was puzzled and embarrassed. While pumping gas, the attendant had said, over the loud speaker where everyone could hear, that her credit card had been declined. As she paid her bill in full and on time each month, she did not know why her credit card was declined. When she got home, Cheyenne called her bank. She was informed that her credit card had been closed due to suspicious activity that included charges in two separate states within hours of each other. Cheyenne then regretted not checking her voice mails promptly, as the bank had left her a message to call. Apparently, someone had obtained access to Cheyenne's account information and illegally used her identity. What should she do? Could she have prevented this?

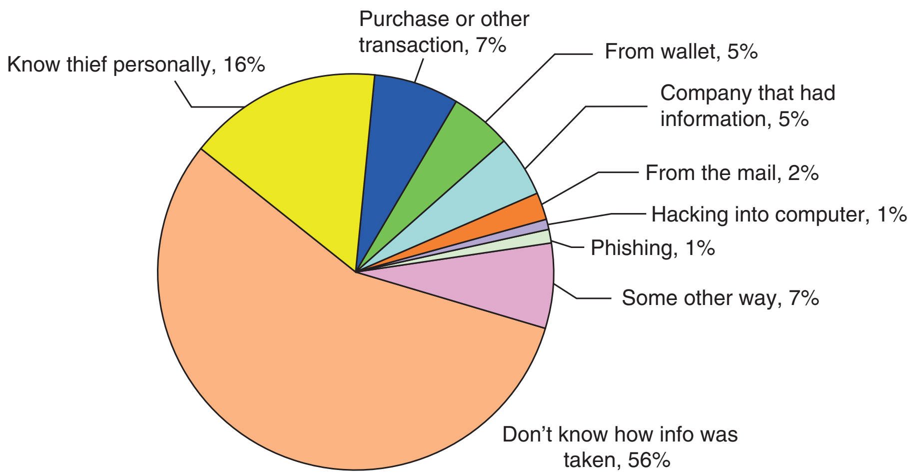
An Overview of Identity Theft

Identity theft occurs when someone intentionally obtains your personal information to use that information for personal gain. By illegally identifying themselves as you, they engage in financial transactions that enable them to receive goods and services that are charged to your accounts.

Categories of Identity Theft

In November, 2007, the Federal Trade Commission (FTC) released the *2006 Identity Theft Survey Report*. This report categorized identity theft by the severity of the harm caused by the identity thief. The *Existing Credit Card Only* categorization occurs when the thief only misuses one or more existing credit cards. It is the least serious category. The *Existing Non-Credit Card Account* categorization occurs when the thief accesses an existing account, like a checking or savings account, that is not a credit card account. The most serious category is *New Accounts and Other Frauds*. In this instance, the thief opens new accounts using the victim's identity. This type of identity theft can be difficult for the victim to catch. One way to catch this is to do an annual review of your credit report.

How Identity Theft Information Is Obtained



Source: Federal Trade Commission — *2006 Identity Theft Survey Report*

Costs of Identity Theft

When identity theft occurs, victims experience financial costs, emotional costs, and loss of productive time. They have to use their time to resolve the many issues that arise from the identity theft.

According to the FTC's report, $500 was the median value of goods and services obtained by identity thieves. However, 5 percent of victims indicated that the thieves obtained at least $13,000 of products.

Fortunately, over half of the victims incurred no out-of-pocket expenses. Some victims, however, had expenses of $5,000 or more. Attorney fees, loss of salary, and paying for any charges attributed to the thief are among the potential costs. There is a variety of laws designed to protect consumers from out-of-pocket losses that result from identity theft.

Although the median amount of time victims spent resolving the identity theft was four hours, some victims spent at least 130 hours resolving the identity theft. The feelings of identity theft victims range from vulnerability to violation of personal privacy to anger to sadness. The emotional stress caused by identity theft adds to the overall fatigue victims experience when dealing with what can be a long process to thoroughly resolve all issues stemming from the theft.

✓ checkpoint

What are the three general categories of identity theft?

Methods for Stealing Identities

There is a variety of methods available for stealing identities. As technology evolves and as customer payment systems change, new methods of obtaining personal information become available. Some theft methods are manual and other methods are electronic.

Manual Ways to Commit Identity Theft

Identity thieves can be fairly creative. They have found ways to steal personal information through telephone scams, by using information from employment records, through stealing mail in residential mailboxes, by going through the trash, and through in-person observation. Once these methods are used to construct a false identity, the thief either steals the individual's funds or obtains credit in the name of the victim.

Telephone Scams Many scams are committed using the telephone. The scam may begin with a postcard advertising easy credit approval or low credit card interest rates. When consumers call these phone numbers, someone asks for their checking account number, supposedly as part of a "verification process." Other scams involve con artists that call and claim to be from the person's bank, saying they need to verify certain information about the checking account for various reasons. Another common scam is to call people to tell them that they have won a prize. After a few minutes of pleasant chat, the thief requires the person to read the numbers off the bottom of a check to "confirm" that he or she "qualifies" for the prize. With checking account information, the con artist can issue a bank draft on the person's checking account.

©TYLER OLSON 2008/USED UNDER LICENSE FROM SHUTTERSTOCK.COM

Mail Theft Some identity thieves steal mail from residential mailboxes. As about 700 million pieces of mail are delivered daily, thieves have ample opportunity to steal mail. Personal information, including credit card numbers and bank account numbers, can be obtained this way. Offers addressed to the resident for new credit or new loans can also be stolen. Once the thief obtains these documents, the information can be used to illegally establish accounts, apply for a loan, or access funds in existing accounts.

The U.S. Postal Inspection service works hard to prevent mail theft. According to their website, in 2007 they arrested more than 9,000 suspects for crimes relating to the mail. More than half of those arrests related to mail theft or identity crimes.

interesting *facts*

The Identity Theft Enforcement and Restitution Act of 2007 is an act that developed in response to increased occurrences of identity theft and increased losses due to identity theft. The Act would increase the ways in which identity theft could be prosecuted. The status of the Act is still pending.

NET Bookmark

The Federal Trade Commission (FTC) is dedicated to helping individuals and businesses avoid becoming victims of identity theft. Access www.cengage.com/school/pfinance/banking and click on the link for Chapter 11. Go to the Federal Trade Commission website. Review the content in the Hot Links section. What are some new identity theft schemes? How can you and your employer work to avoid them?

www.cengage.com/school/pfinance/banking

Trash Retrieval Dumpster diving occurs when a thief goes through the trash of a business or individual with the specific intent of finding either personal identifying information or account information to construct a false identity.

Observation In this day and age, it's hard to know who is watching you. Discrete image-taking devices, ranging from cell phone cameras to pocket-sized video recorders with micro button cameras, can record you discretely. Thieves can record an image of a credit card left exposed on a restaurant table or can photograph a customer entering a PIN in a retail store.

Electronic Ways to Commit Identity Theft

The Internet has streamlined financial transactions. It has also streamlined identity theft. The Internet allows individuals or companies to communicate with tens of thousands of people without spending much time, effort, or money. The Securities and Exchange Commission says that **spam**, or junk e-mail, allows "the unscrupulous to target more potential investors than cold calling or mass mailing." Spammers can use a bulk e-mail program to send personalized messages to thousands of Internet users at a time. In addition, anyone can also reach a large audience by posting a message on an online bulletin board. Fraudsters use spam to find investors for bogus investment schemes. Electronic methods for stealing identities abound.

Phishing Common attacks on banks through the Internet include **phishing** ("fishing"), which is the act of sending a user an e-mail falsely claiming to be a legitimate enterprise in an attempt to solicit private information. The e-mail directs the users to visit a website onto which they are to update personal information, such as passwords and credit card, Social Security, and bank account numbers. The scammer commits identity theft using this information.

Hacking Computer hackers that gain access to records or systems pose another threat to consumers and banks. Banks should use tools such as antivirus software and *autobots*, programs that constantly monitor all transactions looking for abnormalities. *Firewalls*, programs that monitor and limit incoming and outgoing transmissions, have become increasingly important as banks allow access to records for online banking via the Internet. Banks must safeguard the technology that makes doing business possible.

Fraudelent HELOC Accounts A HELOC loan enables borrowers to borrow against a home equity line of credit. Withdrawals against the credit can be made by check or credit card. An identity thief can open an online HELOC account using a false identity and then methodically withdraw funds from the account.

Fake Websites There are multiple ways to extract personal information from fraudulent websites. One method is to develop a website that looks like an authentic business and prompt people to pay for a product or service from that website. When the victim enters identifying credit information, the thieves can use that information for their own purposes.

Another method exploits design weaknesses in the Domain Name System (D.N.S.). In the early 1980s, the D.N.S. was developed to provide Internet addresses. The system was not initially intended to safeguard transactions, like credit transactions, that required specific identity verification. Internet-savvy thieves can exploit the D.N.S. to redirect website visitors to nonlegititmate locations where their personal account information can be collected.


©MARK STOUT PHOTOGRAPHY 2008/USED UNDER LICENSE FROM SHUTTERSTOCK.COM

Personnel Data Theft In the age of laptops and flash drives, it is fairly easy for confidential employee information to be lost or stolen. In recent years, electronic versions of personnel data has been stolen from a diverse array of organizations including the United States Veteran Affairs, Equifax, the District of Columbia, and Google. In many instances, an employer will offer employees a one-year free subscription to an identity-theft monitoring service after a data theft occurs.

Looking for Opportunities Some thieves seek to abuse wi-fi systems used by stores to transmit customer credit information. **War driving** refers to the criminal practice of driving around to find retailers with weaknesses in their Internet security systems. Once a weakness has been found, **sniffer programs**, which are electronic programs that capture account numbers and PINs, can be installed.

One particularly effective example of this was widely reported during the summer of 2008. In this case, an international ring of thieves exploited weaknesses in the Internet security of major retailers including T.J. Maxx, Barnes & Noble, and OfficeMax. More than 41 million debit and credit card numbers were stolen. Sometimes the stolen numbers were sold online and sometimes they were used to manufacture fraudulent ATM cards. Cash could be withdrawn from victims' accounts with the fraudulent ATM cards.

✓ checkpoint

List six ways to steal identity information electronically.

Identity Theft Prevention

There are a number of ways to proactively protect your personal information to try to avoid being an identity theft victim.

Common Sense Precautions

Keep your radar up at all times regarding any suspicious activities or inquiries. If someone unfamiliar is walking around your neighborhood and looking into mailboxes, keep an eye on them. If you think they are stealing mail, contact law enforcement authorities. Never provide account access codes, Social Security numbers, or other personal identifying information over the phone or online unless you are absolutely certain of the validity of the parties with whom you are interacting. Shred all documents containing personal identifying information—including offers for new credit that arrive in the mail.

Electronic Precautions

A **fraud alert** is an electronic warning placed on your accounts to monitor for suspicious financial activity. According to the FTC, you are legally entitled to two free types of fraud alerts. An *initial fraud alert* is good for 90 days and could be put in place if you suspect you may soon be a victim of identity theft. (If perhaps, your wallet was recently stolen.) An *extended fraud alert* lasts for seven years. An extended alert is a good idea if you have been a victim of identity theft. A copy of the Identity Theft Report must be submitted before an extended fraud alert can be placed on your account. A **credit freeze** prohibits access to your credit report. These electronic protections provide a good first step, but they do not necessarily prevent all types of identity theft.

Commercially Sold Identity Protection Packages

Many private companies offer a variety of services to help combat identity theft. Some companies offer services, like fraud alerts, that are actually available for free. Some companies may help you resolve complications resulting from being an identity theft victim. Carefully evaluate the services and costs of such programs. Determine the true value they offer before purchasing them.

✔ checkpoint

Distinguish between the two types of fraud alerts.

assessment 11.4

Think Critically

1. Identify financial costs associated with identity theft.

2. Name four manual ways to commit identity theft.

3. How have electronic transactions and the Internet made identity thieves more efficient?

4. List some ways to prevent identity theft.

Make Academic Connections

5. **Law Enforcement** The postal service is actively involved in trying to catch criminals. Go to their website at http://postalinspectors.uspis.gov/. Review the information on consumer awareness. List and define the types of fraud on the website that are not covered in this section. Be prepared to discuss your answers with the class.

6. **Current Events** Recently the post office made 77 arrests that spanned three countries to stop the flow of 666,000 fake checks. Research other recent arrests for fraud. Summarize the nature of the crime, the amount of the damage, and the agency that caught the thieves. Be prepared to share your research with the class.

chapter 11 assessment

Chapter Summary

11.1 Robbery Prevention and Response

A. Robbery prevention involves installing security equipment and training employees how to behave during a robbery.

B. During a bank robbery, employees should be concerned with the twin goals of safety and identification.

11.2 Ethics in Banking

A. Many banks provide written codes of ethics to help their employees know how to choose the "proper" behavior in specified circumstances.

B. Making the correct ethical decision for a company has become clouded recently with the concern for the "bottom line." Banks must be especially careful to make ethical decisions.

11.3 Fraud and Scams

A. Banking fraud has always occurred, but methods of performing bank fraud have increased with technological advances.

B. Checking account scams seek to find ways to illegally obtain money from the accounts of unsuspecting victims.

11.4 Identity Theft

A. Existing Credit Card Only, Existing Non-Credit Card Account, and New Accounts and Other Frauds are categories of identity theft.

B. Identity theft can be prevented.

Vocabulary Builder

a. bandit barrier
b. check counterfeiting
c. check kiting
d. code of ethics
e. conflict of interest
f. credit freeze
g. ethics
h. forgery
i. fraud
j. fraud alert
k. house flipping
l. phishing
m. scam
n. sniffer program
o. spam
p. straw buyer
q. war driving

Choose the term that best fits the definition. Write the letter of the answer in the space provided. Some terms may not be used.

____ 1. Another term for junk e-mail

____ 2. Act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise to scam the user

____ 3. Process of determining standards and procedures for dealing with judgmental decisions affecting other people

____ 4. Situation in which two interests are at cross-purposes

____ 5. Using a fraudulent appraisal to extract value on a loan for a property you plan to default on

____ 6. Slang term for something that is fraudulent or a swindle

____ 7. Deception deliberately practiced to secure unfair or unlawful gain

____ 8. Name for bulletproof plastic shield at a teller's station

____ 9. Act of opening accounts at two or more institutions and using the "float time" of available funds to create fraudulent balances

____ 10. Statement adopted by management to guide employees in taking appropriate actions in critical situations that could reflect on the organization

Review Concepts

11. Discuss the way security can be described as robbery prevention.

12. Name several actions that should be part of a "best practices" list for a bank.

13. Why is training the key to preventing robbery?

14. Discuss some actions that tellers should take during a robbery to help identify a suspect afterward.

15. Explain how fraud related to banking may be committed.

16. How does a credit freeze help prevent identity theft?

17. Discuss the signs to look for that could identify counterfeit checks.

18. List and explain some steps to take to avoid becoming the victim of check fraud.

19. Describe what is involved in identity theft.

20. What is the relationship between war driving and sniffer programs?

21. What is the Sarbanes-Oxley Act? What behavior does it seek to prevent?

Apply What You Learned

22. Why are the services of an appraiser critical for an illegal mortgage flipping scheme?

23. Why do banks insist that employees not take any heroic measures during a robbery?

24. What aspects of currency design can help prevent counterfeiting?

25. How has computer technology affected bank fraud?

26. Give at least two examples of a conflict of interest or of a breach of confidentiality that could occur in banking.

27. What do you think caused the accounting scandals of the early twenty-first century?

28. Why should you be concerned about who is watching your financial transactions?

Make Academic Connections

29. **Criminology** Crooks can be quite clever. Use the Internet or other research materials to learn about some specific forms of fraud that are currently problematic. Present a report to the class about how they work and how they can be prevented.

30. **Problem Solving** As the head of the HR department in your bank, you must develop screening procedures to be used during the hiring process. Create a list detailing the background information required of prospective employees and the steps to take to verify the information.

31. **Ethics** Make a list of ethical dilemmas you have experienced during your daily life and describe how you handled each situation.

32. **Communication** Do you believe that fraud can ever be effectively eliminated from the banking system? Explain your answer.