



2019 Fraud Review

CPE COURSE

CCH® PUBLICATIONS

2019 Fraud Review

CPE COURSE

Dr. Robert Minniti

DBA, CPA, CFE, CVA, CFF, MAFF, CrFA, CGMA, PI

CCH® PUBLICATIONS



Wolters Kluwer

Contributors

Technical Review: Kelen Camehl, CPA
Production Coordinator: Mariela de la Torre
Production: Sharon Sofinski

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

© 2019 CCH Incorporated and its affiliates. All rights reserved.
2700 Lake Cook Road
Riverwoods, IL 60015
800 344 3734
CCHCPELink.com

No claim is made to original government works; however, within this Product or Publication, the following are subject to CCH Incorporated's copyright: (1) the gathering, compilation, and arrangement of such government materials; (2) the magnetic translation and digital conversion of data, if applicable; (3) the historical, statutory and other notes and references; and (4) the commentary and other materials.

Course Objectives

One of the main reasons certified public accountants (CPAs) and other accountants often fail to detect fraud is that they are too honest. They find it difficult to think like a criminal. This course is designed for individuals who would like refresh their understanding of fraud schemes and to learn how to recognize the red flags for detecting fraud. Understanding how criminals commit fraud is the first step in preventing fraud. This course is designed to be a refresher course for CPAs, certified financial examiners (CFEs), and others in the accounting field and is appropriate to fulfill the four-hour fraud requirement for California CPAs.

At the completion of this course, the reader will be able to:

- Understand theories as to why people commit fraud
- Recognize the different types of fraud, including occupational fraud, cyber fraud, financial fraud, tax fraud, and identity theft
- Identify red flags for fraud
- Describe fraud schemes that affect businesses

Contents

Course Objectives	iii
¶100 Introduction to Fraud	1
¶200 Fraud Theories	3
¶201 Theory of Differential Reinforcement	3
¶202 Theory of Differential Association	3
¶203 The Social Learning Theory	4
¶204 The Fraud Triangle	6
¶205 The Elements of Fraud	7
¶206 Predication of Fraud	8
¶300 Occupational Frauds	9
¶301 Skimming	10
¶302 Lapping	11
¶303 Counterfeit Currency	11
¶304 Asset Misappropriations	12
¶305 Accounts Payable Frauds	13
¶306 Accounts Receivable Frauds	14
¶307 Revenue Frauds	15
¶308 Expense Reimbursement Frauds	16
¶309 Inventory Frauds	18
¶310 Financial Statement Fraud	20
¶311 Double Cashed Checks	22
¶312 Payroll Frauds	22
¶400 Cyber Frauds	24
¶401 Data Breaches	24
¶402 Credential Stuffing	26
¶403 Ransomware	28
¶404 Phishing	30
¶405 Vishing	34
¶406 Brand Hacking	34
¶407 Spoofing	35
¶408 Denial of Service (DoS) Attacks	35
¶409 Pharming	36
¶410 Hacking	36
¶500 Financial Frauds	39
¶501 Credit and Debit Card Fraud	39

¶502	EMV Card Present Fraud	40
¶503	Obtaining Credit Card Information.....	41
¶504	Investment Frauds.....	41
¶505	Ponzi Schemes	42
¶506	Pyramid Schemes.....	42
¶507	Advance-Fee Scams.....	42
¶508	Bankruptcy Fraud.....	43
¶600	Identity Theft	45
¶601	Criminal Identity Theft	46
¶602	Sockpuppets	48
¶603	Medical Identity Theft.....	49
¶604	Insurance Identity Theft.....	50
¶605	Child Identity Theft	51
¶606	Professional Identity Theft	51
¶607	Business Identity Theft.....	52
¶700	Tax Frauds	53
¶701	Tax Refund Identity Fraud	54
¶800	Other Frauds	55
¶801	Unemployment Fraud	55
¶802	Worker's Compensation Fraud.....	55
¶803	Charity Frauds.....	56
¶804	Lottery or Contest Frauds.....	56
¶805	Corporate Prize Scam	56
¶806	Fake Dating Profiles	57
¶807	Government Documents Fraud	57
¶808	Employment Fraud.....	57
¶809	Resume Fraud.....	58
¶810	Fraudulent Recruiter Scam.....	58
¶811	Fraudulent Employment Scam	58
¶812	Internet Auction and Fake Retail Schemes.....	59
¶813	Long-Lost Relative.....	59
¶900	Government-Specific Frauds	62
¶901	Medicare Fraud.....	62
¶902	Social Security Fraud.....	62
¶1000	Not-for-Profit Specific Frauds	63
¶1001	Netting.....	63
¶1002	Overstating the Value of Non-Cash Gifts.....	63

¶1100 Money Laundering 66

¶1200 Corruption 69

¶1300 Fraud Wrap-Up..... 71

Glossary of Terms 73

Answers to Knowledge Check Questions 81

Index 85

Final Exam Instructions 87

Final Exam..... 90

Answer Sheet 96

2019 Fraud Review course: Evaluation Form 97

About the Author..... 98

¶100 Introduction to Fraud

Fraud is a white-collar crime; therefore, the theories as to why people commit crime will apply to why they commit various types of frauds. Organizations can limit the opportunity criminals have to commit fraud by establishing effective anti-fraud internal controls. This course will concentrate on various types of fraud including occupational frauds affecting public companies, private companies, not-for-profits, and governmental entities. To study fraud, we have to start with a definition:

An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury. Anything calculated to deceive, whether by a single act or combination, or by suppression of the truth, or suggestion of what is false, whether it be by direct falsehood or innuendo, by speech or silence, word of mouth, or look or gesture. A generic term, embracing all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated.¹

White-collar crimes, like fraud, are illegal and or unethical actions taken by employees or other agents of an organization.² The term *white-collar crime* is attributed to Dr. Edwin Sutherland, who first used the term in 1939. He pointed out the difference between crimes of trust, such as fraud, and blue-collar crimes such as murder and robbery. Dr. Sutherland was one of the early criminologists in the United States and his works are widely accepted.³ White-collar crimes

1 Black, Henry, Black's Law Dictionary, Sixth Edition, West Publishing Co., St. Paul, MN, 1990.

2 Vadera, A., and Aguilera, R. (2015). The evolution of vocabularies and its relation to investigation of white-collar crimes: An institutional work perspective. *Journal of Business Ethics*, 128, 21–23.

3 Alalehto, T., and Persson, O. (2013). The Sutherland tradition in criminology: A bibliometric story. *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, 26, 1–18.

are often viewed as being less severe than violent crimes despite the financial damage done by white-collar criminals.⁴ Dr. Sutherland went on to note that the penalties for white-collar criminals tend to be less severe than the penalties imposed on violent criminals.⁵ Court ordered restitution and voluntary restitution agreements are common punishments for white-collar criminals.⁶ However, a study by the Association of Certified Fraud Examiners (ACFE) indicated 53 percent of victims recover nothing after a fraud and 32 percent make a partial recovery, while only 15 percent make a full recovery of losses.⁷

4 Leshem, E., and Ne'eman-Haviv, V. (2013). Perception of white-collar crime among immigrants from the former Soviet Union in Israel. *Crime, Law & Social Change*, 59, 555–576.

5 Dorminey, J., Fleming, A. S., Kranacher, M., and Riley, Jr., R. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27, 555–579.

6 Faichney, D. (2014). Aurocorrect? A proposal to encourage voluntary restitution through the white-collar sentencing calculus. *Journal of Criminal Law and Criminology*, 104, 389–420.

7 Association of Certified Fraud Examiners 2018 Report to the Nation on Occupational Fraud and Abuse.

¶200 Fraud Theories

¶201 Theory of Differential Reinforcement

Gabriel Tarde was a 19th-century French criminologist who developed the theory of differential reinforcement in the 1880s and 1890s. The major components of this theory are that people are most likely to imitate the actions of both those with whom they are in close contact and their superiors. The concept of individuals imitating the actions of their superiors is a grounding principle in the Committee of Sponsoring Organizations' (COSO) control environment or as it is often referred to as the "Tone at the Top." Ethics flows from the top of an organization down through the ranks. The theory of differential reinforcement supports an organization's need for an ethics policy and a code of conduct. Gabriel Tarde was also the first to recognize a criminal's tendency to return to the scene of the crime and to be a repeat offender.

¶202 Theory of Differential Association

The field of criminology has accepted Dr. Edwin Sutherland's (1947) theory of differential association and Akers's (1985) social learning theory.¹ There is empirical evidence to support the social learning theory's concepts that white-collar criminals anticipate the rewards they will obtain have greater value than the consequences they will suffer if caught, and that criminals learn their behavior from other criminals.² Dr. Sutherland coined the term *white-collar criminal* for crimes involving a breach of trust rather than violence.

Fraud researchers categorize fraudsters into one of three criminal categories: situational offenders, routine offenders, and professional offenders. Situational offenders are individuals who happen upon the opportunity and commit the crime. Routine offenders look for and take advantage of opportunities as a type of continuous criminal enterprise. Unlike most street criminals, professional fraudsters learn their trade from research and participation in the legitimate and illegitimate economy and from association with other criminal offenders.³

1 Durrant, R., and Ward, T. (2012). The role of evolutionary explanations in criminology. *Journal of Theoretical and Philosophical Criminology*, 4(1), 1–37.

2 Moore, M. (2011). Psychological theories of crime and delinquency. *Journal of Human Behavior in the Social Environment*, 21, 226–239.

3 Vieraitis, L., Copes, H., Powell, Z., and Pike, A. (2015). A little information goes a long way: Expertise and identity theft. *Aggression and Violent Behavior*, 20, 10–18.

¶203 The Social Learning Theory

Akers's (1998) social learning theory postulates that individuals learn criminal activity and rationalize the acceptability of criminal activities based on their social networks.⁴ One quantitative study using regression models to compare the variables supported the social learning theory as it relates to online criminal activity by linking peer offending to online criminal activities in juveniles.⁵ Allen and Jacques (2013) conducted a qualitative study of 16 campus police officers of a large university and in their findings indicated a link between criminal activity to opportunity, social learning, peer pressure, supervision, and culture.⁶ Another study indicated that virtual peers are just as influential to online criminals as traditional peers are to offline offenders.⁷ Another mixed-methods cross-sectional study of 1,674 participants indicated that the social learning theory was valid despite the debate about the effects of self-control on criminal behavior.⁸

The social learning theory is a combination of the differential reinforcement theory and the theory of differential association (Akers, 1998). The theory of differential reinforcement postulates that criminal behavior occurs when individuals experience positive reinforcement, such as obtaining something they desire, either actual or anticipated, and the adverse consequences of their action are minor and do not control or prevent further criminal behavior.⁹ By contrast, the theory of differential association postulates that individuals learn criminal behavior by associating with other criminals, the same way law-abiding citizens learn to behave by associating with other individuals who obey the law.¹⁰ Dr. Donald Cressey conducted a review of the critics' issues with Dr. Sutherland's differential association theory and stated that many of the critics' issues derived from misinterpretation by the critics.¹¹

4 Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston, MA: Northeastern University Press.

5 Holt, T., Bossler, A., and May, D. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, 17, 378–395.

6 Allen, A., and Jacques, S. (2013). Police officer's theories of crime. *American Journal of Criminal Justice*, 39, 206–227. doi:10.107/s12103-013-9219-1

7 Miller, B., and Morris, R. (2014). Virtual peer effects in social learning theory. *Crime and Delinquency*, 1–27.

8 Yarbrough, A., Jones, S., Sullivan, C., Sellers, C., and Cochran, J. (2012). Social learning and self-control: Assessing the moderating potential of criminal propensity. *International Journal of Offender Therapy and Comparative Criminology*, 56, 191–202.

9 Megens, K., and Weerman, F. (2012). The social transmission of delinquency: Effects of peer attitudes and behavior revisited. *Journal of Research in Crime and Delinquency*, 49, 420–443.

10 Moore, M. (2011). Psychological theories of crime and delinquency. *Journal of Human Behavior in the Social Environment*, 21, 226–239.

11 Cressey, D. (1952). Application and verification of the differential association theory. *Journal of Criminal Law, Criminology and Police Science*, 43(1), 43–52.

The social learning theory also contains variables from other criminology theories including deterrence, social bonding, and neutralization theories.¹²

Dr. Akers indicated that the probability persons will engage in criminal and deviant behavior increases (and the probability of conforming to the norm decreases) when they:

- Differentially associate with others who commit criminal behavior and espouse definitions favorable to it,
- Are relatively more exposed in-person or symbolically to salient criminal/deviant models,
- Define it as desirable or justified in a situation discriminative for the behavior, and
- Have received in the past and anticipate in current or future situations a relatively greater reward than punishment for the behavior.

Akers's social learning theory has received significant empirical support in explaining criminal behavior and is regarded as one of the leading theories in criminology.¹³

According to the social learning theory, it is possible that when fraudsters perceive that the potential benefits outweigh the risk of punishment associated with the criminal act of fraud, they will commit the crime.¹⁴ The benefits received by the fraudsters include employment, health care, social status, purchasing power, and access to credit facilities. Because individuals with similar demographics and perhaps geographic locations can be grouped together, it is possible that individuals observing others in the same demographic or geographic group receiving benefits from fraud would want to learn the skill from those who were successfully committing the crime.

Knowledge Check Question

1. Which of the following individuals developed the Social Learning Theory?
 - a. Gabriel Tarde
 - b. Ronald Akers
 - c. Edwin Sutherland
 - d. Donald Cressey

12 Capece, M., and Lanza-Kaduce, L. (2013). Binge drinking among college students: A partial test of Akers' social-structure-social learning theory. *American Journal of Criminal Justice*, 38, 503–519.

13 Tittle, C. R., Antonaccio, O., and Botchkovar, E. (2012). Social learning, reinforcement and crime: Evidence from three European cities. *Social Forces*, 90, 863–890.

14 Maskaly, J., and Donner, C. (2015). A theoretical integration of social learning theory with terror management theory: Towards an explanation of police shootings of unarmed suspects. *American Journal of Criminal Justice*, 40, 205–224.

¶204 The Fraud Triangle

The theoretical framework supporting fraud investigations and internal controls is the fraud triangle theory. The seminal work about why people commit fraud, including occupational fraud, is the fraud triangle developed by Dr. Donald Cressey in 1952. The fraud triangle has three main points:

- Pressure or needs
- Rationalization
- Opportunity

Pressure comes from the need for something, such as cash to pay bills. Rationalization is how individuals find ways to believe actions they know are wrong are acceptable under the circumstances, such as convincing themselves they are only borrowing the money rather than stealing the money. Finally, opportunity occurs when the victim allows the fraudster access to the victim's assets. Kassem and Higson proposed a new fraud triangle theory adding a new dimension: (a) motivation, (b) capability, (c) opportunity, and (d) personal integrity.¹⁵ There is currently insufficient research to support this expansion of the fraud triangle theory.

While Dr. Donald Cressey originally developed what researchers came to call the fraud triangle, the first use of the term *fraud triangle* to describe the idea came from the ACFE instead of Cressey.¹⁶ The American Institute of Certified Public Accountants (AICPA) integrated the fraud triangle into the Statement on Auditing Standards Number 99.

Studies such as Dellaportas's 2013 study on why accountants commit fraud have continued to show the validity of Dr. Cressey's fraud triangle theory.¹⁷ The cognitive dissonance theory indicates fraudsters commit the crime then rationalize their behavior to improve their own self-worth.¹⁸ I believe the cognitive dissonance theory supports the rationalization component of the fraud triangle theory. Other researchers have claimed the professional development of the fraud triangle as a criminology theory concentrates on limiting opportunity and an individual's lack of ethics to the exclusion of other factors such as the role of society and political agendas in combatting crimes such as fraud.¹⁹

15 Kassem, R., and Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, 3(3), 191–195.

16 Morales, J., Gendron, Y., and Guenin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39, 170–194.

17 Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum*, 37(1), 29–39.

18 Trompeter, G., Carpenter, T., Jones, K., and Riley, R. (2014). Insights for research and practice: What we learned about fraud from other disciplines. *Accounting Horizons*, 28, 769–804.

19 Morales, J., Gendron, Y., and Guenin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39, 170–194.

Sykes and Matza studied how perpetrators of crimes rationalized their behavior by using neutralizing language.²⁰ There are five basic ways to use neutralizing language to rationalize criminal behavior:

- Denial of responsibility
- Denial of victim
- Denial of injury
- Condemnation of the condemners
- Appeal to higher loyalties²¹

By rationalizing their behavior, most white-collar criminals do not consider themselves to be criminals and deny they had intent when committing their crimes.²² Except for their ability to rationalize their behavior and resistance to considering their activities as crimes, white-collar criminals have been assumed to be basically normal people.²³ Historically, white-collar crime, including identity theft, was considered to be a civil dispute under common law rather than a criminal act.²⁴

¶205 The Elements of Fraud

There is another theory that explains how individuals commit white-collar crimes, such as fraud, which is known as the elements of fraud.²⁵ In this theory, Dorminey et al. stated there are three elements of fraud:

- The act,
- Concealment
- Conversion

The act consists of the actual theft or misappropriation of assets. Concealment represents the perpetrator's attempts to hide the act from others. Finally, conversion is the process of turning the ill-gotten gains into something the perpetrator can use. Criminals use other people's identities in order to conceal

20 Sykes, G., and Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22, 664–670.

21 Klenowski, P. (2012). "Learning the good with the bad": Are occupational white-collar offenders taught how to neutralize their crimes? *Criminal Justice Review*, 37, 461–477.

22 Stadler, W., and Benson, M. (2012). Revisiting the guilty mind: The neutralization of white-collar crime. *Criminal Justice Review*, 37, 494–511.

23 Benson, M. (2013). Editor's introduction – White-collar crime: bringing the offender back in. *Journal of Contemporary Criminal Justice*, 29, 324–330.

24 Bennett, R., LoCicero, H., and Hanner, B. (2013). From regulation to prosecution to cooperation: Trends in corporate white collar crime enforcement and evolving role of the white collar criminal defense attorney. *Business Lawyer*, 68(2), 411.

25 Dorminey, J., Fleming, A. S., Kranacher, M., and Riley, Jr., R. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27, 555–579.

their illegal activities. It's important to note that internal controls help to limit the opportunity fraudsters have to commit the act or crime.

The elements of fraud are used by managers to help identify the risk of fraud in a business.²⁶ Internal controls can be used to help prevent or detect the act, which is the first element in the elements of fraud theory. Managers and those with responsibility for governance must implement controls to restrict a perpetrators access to assets and deny them the opportunity to commit the act of fraud. Based on the elements of fraud theory, managers and those charged with governance concentrate on developing internal controls for the theft or misappropriations of assets.²⁷ The elements of fraud theory focus on starting with the criminal act without considering the demographics or motivations of the fraud perpetrators that led up to the act.²⁸

¶206 Predication of Fraud

It is necessary to determine if there is a predication of fraud before starting a fraud investigation. Sometimes red flags for fraud, upon examination, are nothing more than human error, with no intent to deceive or commit fraud. Predication of fraud is the total of the direct and circumstantial evidence that would lead a reasonable person, trained in law enforcement or fraud investigations, to believe that a fraud has occurred, is occurring, or will occur in the future. Suspicion, alone without any objective direct or circumstantial evidence, is an insufficient basis for conducting a fraud investigation. Because fraud investigations can be costly it is necessary to determine that a predication of fraud exists prior to commencing a fraud investigation.

This should not be taken to indicate that suspicions of fraud should not be reported. Employees who suspect fraud should report their concerns to their supervisors, managers, human resources, or the company's audit committee. The ACFE's 2018 Report to the Nations on Occupational Fraud and Abuse indicated that a majority of frauds are discovered by receiving tips and over half the tips reporting fraud come from employees.

26 Power, M. (2013). The apparatus of fraud. *Accounting, Organizations and Society*, 38, 525–543.

27 Power, M. (2013). The apparatus of fraud. *Accounting, Organizations and Society*, 38, 525–543.

28 Dorminey, J., Fleming, A. S., Kranacher, M., and Riley, Jr., R. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27, 555–579.

¶300 Occupational Frauds

Frauds that affect the workplace are considered to be occupational frauds. There are three basic types of occupational frauds:

- Asset misappropriation
- Corruption
- Financial statement fraud

Asset misappropriation is the theft of either tangible or intangible assets. For example, this could be fixed assets, inventory, or sensitive data. Corruption is the misuse of an individual's position for personal gain whereas financial statement fraud is commonly referred to as "cooking the books." According to the ACFE's 2018 Report referenced previously,¹ asset misappropriation is the most common type of occupational fraud, followed by corruption, and financial statement fraud. Many times, these types of fraud occur together because criminals commit financial statement fraud to cover up corruption and theft of assets. The ACFE study also indicated organizations lose over \$7 billion a year to fraud, have an average loss of \$130,000 per fraud scheme, and the fraud schemes run for an average of 16 months before they are detected.

The ACFE report also noted that internal control weaknesses were responsible for nearly half of all frauds. Organizations that implemented anti-fraud controls had lower losses than organizations that didn't have anti-fraud controls. Organizations suffered the greatest losses when there was collusion with a median loss of \$339,000. Only four percent of the fraud perpetrators had a prior fraud conviction and over the last ten years referrals for prosecution have declined by 16 percent. The main reason for not making a referral for prosecution is the fear of bad publicity. One interesting note was that employees who had been with their organizations over five years stole an average of \$200,000 which was nearly twice as much as employees who were with their companies for less than five years.

Asset misappropriations start with the basic theft of an organization's assets. Thefts of inventory, fixed assets, financial assets, data, and other intangible assets are common in today's world. Securing both tangible and intangible assets is important for all organizations. Cash and financial assets are frequently stolen

¹ Available at www.acfe.com.

by fraudsters. According to the ACFE report, 89 percent of detected fraud cases are asset misappropriation cases with a median loss of \$114,000. Asset misappropriation frauds average lower losses than financial statement frauds which have a median loss of \$800,000. In the next sections of this course, we will examine some of the common fraud schemes (in no particular order).

301 Skimming

The ACFE report noted that the average loss for a skimming scheme was \$50,000. Skimming is a fraud where employees or volunteers steal cash or checks before transactions are entered into the accounting system. They provide the customer with products or services and instead of entering the transaction into the cash register they pocket the payment and don't record a sale. This is a common fraud when employees are working alone, in drive-through retail outlets, and at fundraising events for not-for-profit organizations. Governments are also susceptible because many taxpayers prefer to pay taxes and fines in cash or by check. Skimming can be difficult to detect because nothing has been entered into the accounting system so there is no audit trail or transaction to review. Common internal controls that are effective in preventing and detecting skimming include using cameras to record cash registers and cash collection points. Many businesses post signs at the cash registers asking customers to report to management anytime they don't receive a receipt for their transaction. Often customers are offered a reward such as a free coffee or gift card for taking the time to make the report. This brings the customer into the internal control process and makes it difficult for employees to process transactions without receipts.

Employees can also use coupons and discounts to conduct skimming schemes. An example of this would be ringing up a customer who doesn't have a coupon at the cash register and then voiding the transaction after the customer leaves and reinputting the transaction with the coupon. The employee can then pocket the cash. The explanation for the transaction is that the customer remembered the coupon or discount after the original transaction was processed and asked to have the coupon or discount applied.

Skimming is also done by business owners in order to reduce their tax burden. By removing receipts from the business, they can reduce both their sales tax and income tax liabilities. A common red flag for owner skimming is owners offering discounts for cash payments. The owners pocket the cash payments and don't include them in the company financials or on their tax returns. This type of fraud can be difficult to detect and is usually discovered during a tax audit when the auditors do a lifestyle audit to show the business owner is living well beyond their means based on the reported tax income.

Receipts skimming is also done to reduce alimony and child support payments, which are based on income. Another common reason for owner skimming is to qualify for government benefits or to qualify for needs-based scholarships and government backed student loans for their children's college education.

Knowledge Check Question

2. Taking cash before it is recorded in the accounting system is referred to as:
 - a. Cash larceny
 - b. Kiting
 - c. Skimming
 - d. Cash drawer loans

¶302 Lapping

Lapping is a fraud scheme where employees “rob Peter to pay Paul.” Lapping most commonly occurs in organizations that have many customers who have similar payments. A typical lapping plan works in the following pattern. An employee steals a payment from Customer A and pockets the money. Before Customer A gets a late notice or late fee, the employee steals a payment from Customer B and posts it to Customer A's account. Then the employee steals funds from Customer C to cover the theft from Customer B. At this point Customer A and Customer B are current on their payments and the employee only needs to worry about covering the payment for Customer C. It can be difficult for employees to track all the payments they have stolen and to cover them before they become past due, making lapping one of the easier frauds to detect.

¶303 Counterfeit Currency

Counterfeit currency is another fraud that organizations have to consider in their risk assessment. Counterfeit currency schemes can be perpetrated by customers or employees. Customers can use counterfeit currency to pay for transactions, and employees can swap counterfeit currency for real bills in their cash drawer, which leaves the employer holding the counterfeit currency. Individuals can make counterfeit currency using a color copier, or they can purchase it on the Internet. (Just Google “Buy Fake Dollars” and you will get over 22K hits).

Common internal controls to detect counterfeit currency include using black lights, counterfeit detection pens, and counterfeit detection machines. Black lights allow employees to view the color of the security threads in

modern U.S. currency. Under a black light the security thread in a \$100 bill is pink, a \$50 bill is yellow, a \$20 bill is green, a \$10 bill is orange, and a \$5 bill is blue. If the color of the security thread under a black light doesn't match the denomination of the bill, then it is a counterfeit. Counterfeit detection pens are iodine-based pens that are used to detect standard wood-based paper used in copiers and printers. U.S. currency is printed on a cloth-based paper. The iodine in the counterfeit detection pen leaves a permanent black mark on wood-based paper while leaving a temporary brown mark on cloth-based paper. Remember, it is illegal to use or possess counterfeit U.S. currency. The simple possession of the currency is punishable with a prison term of up to 20 years. You should not attempt to deposit or pass off counterfeit currency to another company. Federal statute 18 USC Section 471 criminalizes making copies of U.S. currency, unless they are much larger or much smaller than real U.S. currency (a minimum of 50 percent larger or 25 percent smaller) or unless they are "rendered in black and white," with up to 15 years in prison. Should you receive a counterfeit bill, you are required to forward it to the U.S. Secret Service (<http://www.secretservice.gov/forms/ssf1604.pdf>).

Knowledge Check Question

3. The security thread in a \$20 bill glows _____ under a black light.
 - a. Blue
 - b. Green
 - c. Yellow
 - d. Pink

¶304 Asset Misappropriations

Asset misappropriation is usually tied to items of value that can be easily monetized. Cash is one of the most frequently stolen assets because once the criminal has the cash in their possession, it is difficult to prove they stole the cash and it wasn't theirs to start with. This is another reason to have cameras as part of your internal controls. Cash can be stolen from cash registers, from safes and vaults, from the mail room, and from deposits. I am still amazed that in today's world people still send cash through the mail. Asset misappropriation can also include the theft of inventory and fixed assets. Criminals are usually trying to steal small, expensive items that are easily converted into cash. An organization missing inventory or fixed assets should search online sales sites, such as EBay and Craig's List, as the thieves often try to sell the items they have stolen. Intangible assets such as trade secrets, research and development,

customer information, employee information, and other data are also misappropriated by criminals. Organizations have to make sure they have good internal controls in place to protect both tangible and intangible assets.

¶305 Accounts Payable Frauds

There are numerous ways to commit accounts payable fraud. The most basic accounts payable fraud scheme is to submit multiple invoices for the same transactions. The extra invoice will be sent with a different invoice number or a slightly altered invoice, such as a “-A” at the end, to attempt to circumvent the automated controls in the victims accounting software. Sometimes statements are generated by the criminal after a payment is received but before it is posted to the system in order to obtain a duplicate payment. If the victim questions the statement, they are told it “crossed in the mail.”

Criminals will also generate fake invoices, or documents that look like invoices in order to obtain payments. The classic example of this was invoices for the “Yellow Book,” which were made to look like invoices for yellow pages ads. Today we see fake invoices for website optimization and SEO optimization, services that were never ordered or provided, but the fraudsters hope the victim will process the invoice. There was an interesting fake invoice scheme in Arizona a few years ago. The fraudsters sent out fake invoices for \$300 to limited liability companies in Arizona claiming that had not filed their annual corporate reports. It should be noted that limited liability companies in Arizona are not required to file corporate reports. The invoices contained the logo for the Arizona Corporation Commission and were written to look like official correspondence from the Corporation Commission. The Attorney General for the State of Arizona put out a warning because thousands of businesses fell victim to this fake invoice scheme.

Another type of accounts payable fraud is payment splitting. Payment splitting occurs when an employee gets an invoice, either real or fake, that is over their approval limit. In order to avoid review by a supervisor, the employee splits the invoice into two payments, both of which fall into the employee’s approval limit. Sometimes employees collude with vendors to have them reissue multiple invoices when the original payment is over their approval limit.

Shell companies are often created in order to create and submit fake invoices. A shell company is a company in name only. It is properly registered with the state, has an EIN, P.O. Box address, and usually has a bank account, but it provides no actual goods or services and has no operations other than generating invoices and receiving payments. W-9s are generated and the shell companies are set up as vendors in the victim’s accounting system. Fake invoices are sent out and the payments are processed through the shell company’s bank account.

It isn't always necessary to go to all the trouble of setting up a shell company in order to commit a disbursement fraud. Employees can find a stale vendor (a vendor that hasn't been used in a while) and process a change of address for that vendor. Since the vendor is already in the system and approved, there is no need for a new W-9 or approval. The employee then creates and approves invoices for the vendor and misappropriates and cashes the checks.

Altering a check is also a common type of disbursement fraud. Accounting personnel can print a check and then alter the payee in the accounting system. It is also possible to steal a check from the check run and then to negotiate the check, making it look like a legitimate cashed check on the bank reconciliation. The ACFE report indicated the average loss to a company that is a victim of check and payment tampering is \$150,000.

Escheated funds are another area that are ripe for disbursement fraud. Sometimes recipients fail to cash the checks they are sent. These checks have been issued but they are variances on the bank reconciliation. At a certain point, depending on the state, the funds should be turned over to the government. Employees can reissue the checks, usually having them sent to a new address controlled by the employee, and then cash the checks. From the company's perspective, it appears that the check was reissued and cashed by the intended recipient.

¶306 Accounts Receivable Frauds

Accounts receivable frauds start with the basics of skimming and lapping, which we have already reviewed. More advanced accounts receivable frauds include account identity theft. With account identity theft, the criminal sets up a bank account in a name similar to that of the victim. The criminal then steals checks intended for the victim and deposits them in the criminal's bank account. The funds are then withdrawn or wired out of the account as soon as the check clears. The payor sees that a check they wrote cleared and they are unlikely to take any action until they are contacted by the victim, usually several months later, to inquire about a past due payment.

Reaging receivables is a fraud perpetrated by management when the receivables are being used for collateral for a loan. It is also done when fake sales have been entered into the accounting system in order to disguise the fact that a payment hasn't been made. The reaging of receivables involves creating a new, fresh receivable and using the funds to pay off an aged receivable. This can be done multiple times to make the accounts receivable aging report show only current, and few past due, invoices.

Receivables dumping occurs when an employee, who normally has a connection with a collection company, writes off a collectable receivable and

sends it out for collection. The collection company usually gets a third of the collection and the employee either has an undisclosed interest in the collection company or is receiving a kickback from the collection company.

Sometimes companies receive payments on accounts that have been written off as uncollectable. The payments can come from a customer, lawyer, or the bankruptcy courts. Since the company is not expecting to receive payments on accounts it has charged off, it is easy to divert these funds.

Payment diversions occur when an employee accepts a payment from the customer and posts it to their own account or to the account of a friend, relative, or other accomplice. This type of fraud can be difficult to prove as the employee will assert that they “just made a mistake.”

Factoring fraud occurs when management inflates the value of accounts receivable in order to qualify for a loan using the receivables as collateral. Fictitious sales are recorded on the books to increase the accounts receivable balance. Factoring fraud is usually done in conjunction with receivables reaging.

Knowledge Check Question

4. Creating new receivables to pay off older receivables is an example of:
 - a. Duplicate invoices
 - b. Receivables dumping
 - c. Reaging
 - d. Skimming

¶307 Revenue Frauds

The Public Company Accounting Oversight Board (PCAOB) reported the most common reason for having to restate financial statements was for improper revenue recognition. Companies recognize revenue before it is earned in order to increase profitability in the current period and drive up stock prices. Companies can also record revenue from fake sales. They create a sale using accounts receivable to increase revenue in the current period and then either carry the receivable indefinitely or write it off in a future period. The ACFE report notes that the average loss for a billing fraud scheme is \$100,000.

Recording revenue on conditional sales is done to manipulate a business's revenue. Conditional sales occur when the buyer has the right to return some or all of the merchandise being purchased. Under U.S. GAAP, the revenue should not be recorded until the return period has lapsed and the sale is complete. At a minimum, it is necessary to set up an allowance for any potential returns.

Bill and hold frauds are another way to manipulate revenue in a company. With a bill and hold scheme, the company sends an invoice to a customer for goods that were never ordered by the customer, nor sent by the company. If the customer pays the invoice, the company sends the goods; otherwise, the invoice is reversed or written off. Sometimes the receivable is offset with a credit memo to avoid a direct write-off.

Improper sales cut-offs are a way to manipulate revenue in a company. There is a high risk of cutoff issues for any company that has commissioned sales people or that pays bonuses based on sales. Salespeople are known to manage their commissions by sandbagging sales into future periods or by backdating sales in order to receive commissions sooner.

Channel stuffing is another fraud scheme that can be used to manipulate revenue. Channel stuffing occurs when a business ships more merchandise to a distributor than they can reasonably be expected to sell. The distributor accepts the merchandise knowing they can return any unsold items for credit. The company prematurely records the revenue for this transaction as if the sale was final.

Knowledge Check Question

5. Which type of revenue fraud involves billing for goods without receiving an order or shipping anything?
 - a. Bill and hold
 - b. Improper sales cut-off
 - c. Fake sales
 - d. Channel stuffing

¶308 Expense Reimbursement Frauds

The Association of Certified Fraud Examiners 2018 report to the nation on occupational fraud and abuse indicated the average loss for expense reimbursement fraud schemes was \$31,000 per scheme. It takes an average of two years for a company to identify and detect an expense reimbursement fraud scheme. Expense reimbursement frauds are more likely to happen in smaller companies than they are in larger companies. Larger companies tend to have automated expense tracking and better internal controls, which help to reduce expense reimbursement fraud.

Marking up expenses is one way employees commit expense reimbursement fraud. For example, a vice president of sales would entertain current and potential customers. He paid for the tab on his personal credit card. At the

restaurant he would receive two copies of the credit card receipt. On the copy he left at the restaurant, he would place a zero-dollar tip, and on the copy he submitted for reimbursement, he always had a 20 percent tip. The 20 percent was pocketed by the employee.

Another way employees commit expense reimbursement fraud is known as the buyer and return fraud. Employees purchase items for the business but do not actually deliver them to the business. Instead, they return them to the merchant for refund. Sometimes employees will leave the items in their vehicle, and if the items aren't counted at the business location, it's easy for them to return them; if the items are counted, they merely claim, "let me check my car," and after checking their car will tell you the item must've fallen out of the bag they found in their trunk. The purpose, of course, is to make this appear as if it was an honest error or accident.

Purchasing personal items and including those items in their expense reports is another way that employees commit expense reimbursement fraud. This can be easily done at a hotel by having personal charges billed to the room and then only submitting the credit card receipt rather than the detailed hotel invoice for reimbursement. Employees have also been caught using company credit cards or purchase cards (PCards) to make personal purchases.

Salespeople have a scheme known as "if you can't sell, drive." With this scheme, they make sales appointments all over town driving from north to south and east to west to generate a lot of mileage for reimbursement. Sometimes they don't even attend the meetings they record on their mileage logs.

Employees can submit fraudulent receipts for reimbursement. Sometimes receipts are submitted more than once, allowing for the payment of duplicate expenses. Employees can also take advantage of companies that don't require receipts for de minimis expenses. One example was an employee who submitted receipts for meals at \$24.99 when the company's controls indicated no receipts were required for expenses under \$25.

In some cases multiple employees are at the same meal or event and sometimes they all will submit for reimbursement, even though only one employee paid. Another issue to watch for is unauthorized expenses, such as employees who make purchases without getting advanced authorization for those purchases. When employees have the opportunity to make purchases for the company or on behalf of the company, it is necessary to make sure that they don't have a conflict of interest with the vendor. Sometimes the employee has an ownership interest in the vendor or might be receiving kickbacks from the vendor in order to process payments to that vendor.

Other types of expense reimbursement fraud include making purchases through a shell company, purchasing gift cards in addition to the legitimate purchases they are making, and altering receipts prior to submitting them for

reimbursement. There have also been issues with employees who purchase extended warranties on items and submit for reimbursement the purchase including the extended warranty, while going back to the vendor and canceling the extended warranty and receiving a refund. That issue also has occurred with deposits, where a rental deposit, or other type of deposit, is paid for up front and expensed to the business. When the rental item is returned and the deposit is refunded on the employee's credit card, the employee does not return the funds to the business.

Knowledge Check Question

6. Employees generally commit expense reimbursement fraud by all of the following, **except**:
- a. Expensing items and then selling them on the Internet
 - b. Purchasing and canceling extended warranties
 - c. Entertaining customers
 - d. Shell companies

¶309 Inventory Frauds

Businesses that maintain inventory are susceptible to various types of inventory frauds. The most common issue with inventory is the theft of inventory, either by employees or by shoplifters, using the old “five-fingered discount.” Inventory is stolen and the criminals either use the items themselves or sell them for cash or virtual currencies. The stolen inventory can also be bartered for drugs, prostitutes, or other illegal items. It is important to have good internal controls in place to keep the inventory secure. This can include using barcodes, Radio Frequency Identification (RFID) chips, cameras, locked display cases, and alarm systems.

One type of inventory theft scheme involves having an employee who works at a cash register collude with an outside party. The accomplice brings several items to the checkout point, including one high-priced item. The employee rings up the items but places his hand over the barcode of the high-priced item while passing it over the scanner, thus preventing it from being recorded. The accomplice then pays for the lower priced items and walks out with all of the items, including the items not recorded by the cash register. If a supervisor is watching, or even if cameras are present, this can look like a legitimate sale and no red flags are raised—until the inventory is counted, and shortages are detected.

Another inventory fraud scheme starts with an employee removing inventory from the store or warehouse and passing it off to an accomplice. The

accomplice brings the item back to the store and requests a refund. There is usually an excuse for not having an original receipt, such as “it was a gift.” The employee then processes a refund by paying the accomplice and returning the stolen item into the store’s inventory.

Criminals also commit inventory fraud in manufacturing companies. In addition to stealing finished goods, they also steal scrap. A classic example occurs at home builders. Subcontractors order more materials, such as drywall, counter tops, wiring, etc., and they cut the items down to size or keep the extra. We have caught subcontractors using stolen goods to fix up the properties they purchased to flip. You have a good profit margin when all or the majority of your materials are free.

Failing to remove inventory from the books once it is sold is another classic inventory fraud scheme. This was easier to do when companies used periodic inventory tracking rather than perpetual inventory tracking. Since the inventory isn’t removed from the books, the cost of goods sold is lower and the profits are higher. The Phar-Mor fraud is a classic case study for this type of fraud. Phar-Mor even moved inventory from store to store, so every day when the auditors arrived to count the inventory, the stores were full of inventory. The auditors didn’t know they were counting the same inventory over and over again.

Shell companies without any actual operations are also used in inventory frauds. In this fraud the purchasing manager orders inventory from a shell that he or she set up or had a relative or friend set up. The shell company then orders the merchandise from legitimate vendors and repackages it and sends it to the victim company. The shell company will then invoice the victim, typically for 10 percent to 20 percent over what they purchased the merchandise for from the legitimate vendor, and the difference is all profit. A good internal control to prevent this type of inventory fraud is to do periodic Internet price checks on all the goods and services purchased to make sure the prices being paid are in line with the market.

It is not uncommon for owners, managers, and employees to temporarily use items from inventory for personal purposes. The items are removed from the packaging and used by the fraudsters. The items are then repackaged and sold as new. The unsuspecting customer believes they are purchasing a new product when in fact they are purchasing a used product.

Merchandise inventory fraud also occurs through short shipping. This fraud can be conducted by either management or employees. When a customer places an order for 100 items, the company short ships 98 items, hoping the victim doesn’t count the items upon receipt. Should the customer count the items, the company claims it is an error and immediately offers to ship the missing items or to issue a credit memo. Employees commit this type of fraud

by stealing items prior to shipping, and if a shortage is reported, they will claim it was simply an error.

Manufacturers can commit inventory fraud by incorrectly recording overhead and other indirect costs as direct inventory costs that are then capitalized with the inventory rather than being expensed in the period in which the expense was made. For large construction projects like buildings or airplanes, these companies can manipulate the percentage of completion in order to manipulate the costs of construction.

It is always necessary to commit financial statement fraud to explain the inventory shortages when a physical inventory count is done. Commonly, transactions are entered to record the stolen inventory as breakage, shrinkage, spoilage, or obsolescence. Other ways to conceal inventory frauds include altering inventory counts, altering inventory values, recording phantom inventory, recording intercompany sales as final sales, failing to record inventory at the lower of cost or market, and using improper cut-offs for recording inventory purchases and sales.

Knowledge Check Question

7. Which of the following is a type of inventory fraud?
- a. Bill and hold
 - b. Lapping
 - c. Cooking the books
 - d. Short shipping

¶310 Financial Statement Fraud

Financial statement fraud is usually done in conjunction with other frauds in order to conceal the fraud and hide illegal activities. Financial statement fraud can also occur on its own and is the costliest of the occupational frauds. You are probably already aware of some of the famous financial statement frauds, such as Enron, WorldCom, Waste Management, etc. These financial statement frauds occurred when management wanted to give the appearance of increased profitability in order to drive up stock prices. Managers can add fictitious revenues or hide or capitalize expenses in order to make a company look more profitable. The executives at Enron used off-balance-sheet financing to move liabilities off the company's balance sheet into special purpose and variable interest entities.

It should be noted, however, that the vast majority of financial statement frauds are not designed to make a company look more profitable. Indeed, the business owners skim revenue out of the business and pay personal expenses from business funds for the sole purpose of making the company look less profitable. This is done to reduce the sales and income taxes the business owner would otherwise have to pay. There are far more small businesses in the country than there are large businesses, which is why this is a more common fraud. Don't be dismayed, however, because when it comes time to sell the business, these criminals are more than willing to cook the books to make the company appear more profitable for the buyer.

The easiest way to commit financial statement fraud is to record fictitious transactions on the books. This includes recording fake sales in order to increase revenue or recording fake expenses in order to reduce taxable income. Many times, fraudulent entries are input into the accounting system using top-sided or other journal entries. Businesses using the accrual method can also prematurely recognize revenue in order to manipulate the financial statements.

It is also possible to manipulate the financial statements by overstating the value of assets such as inventory, although intangible asset values are easy to manipulate. Failing to record or miss recording depreciation and amortization is another way to manipulate asset values. Companies have also been known to record consignment goods as part of the company's inventory. Understating liabilities or failing to disclose liabilities in the financial statements is another example of financial statement fraud.

Manipulating reserve accounts, such as the allowance for doubtful accounts, warranty, and repair allowances, environmental cleanup funds and returns and allowances is another way to commit fraud. It is often common to see unrecorded liabilities, especially in small businesses where the owners are funding the business with personal loans or by using their personal credit cards. Failure to disclose contingent liabilities can also be an issue. Improperly recording transactions in the wrong period, either holding transactions for a future period before recording them, or backdating transactions into past periods, it is also an example of financial statement fraud.

Financial statement frauds can be undertaken to alter the balance sheet, income statement, or the statement of cash flows. Failure to provide proper financial statement disclosures or filing misleading financial statement disclosures is also a type of financial statement fraud.

¶311 Double Cashed Checks

There is a growing trend in check fraud schemes. This particular scheme takes advantage of some of the newest technology in online banking. When a payee receives a check, the payee uses their cell phone to deposit the check into their bank account. The check clears, and the victim reconciles their bank account without any issues. Up to this point everything is legal and above board. The fraudster then sits on the check for about five months and then takes the original check to a checking cashing outlet and cashes the check. If the victim is properly reconciling their bank accounts, they will notice this check cleared a second time. If the victim is lucky, and using positive pay, then their bank may refuse to pay the check a second time. Herein comes the legal issue. Since the check cashing store has an original check with a valid signature, unless the victim can prove the check cashing store knew the check had been previously deposited, the check cashing store will be able to obtain a judgment for the amount of the check.

Once the victim has paid the check cashing store, their only recourse is to sue the payee who cashed the check twice. It would be especially difficult to convince a prosecutor to file criminal charges against the payee unless the victim could show a history of double cashing checks, because the payee is going to claim it was a mistake and they forgot they previously cashed the check. The payee will often offer a payment plan of a minimal amount per month with no interest to repay the money. Because of the claim that this was an error and an offer for restitution, it would be all but impossible for the prosecutor to establish mens rea or intent for the crime.

¶312 Payroll Frauds

The ACFE report notes that the average cost to an organization that is the victim of a payroll scheme is \$63,000. There are numerous types of payroll fraud schemes. Payroll fraud schemes can be conducted by employees, the accounting department, or by owners and managers. The most basic payroll fraud scheme conducted by employees is to improperly record hours on a time sheet, thereby getting paid for hours that are not worked. Workers have been known to ask their fellow employees to “clock me out” because they need to leave early, or to ask someone to “punch me in” if they know they are going to be late. The unwritten agreement is a quid pro quo that if you help me out now, I will do the same for you in the future. This is an example of combining asset misappropriation and corruption into one fraud scheme. Another common employee fraud scheme is slow work for overtime. This works because the employee deliberately works slowly, knowing the

work needs to be done by a certain deadline, and then the employee works overtime to get the job done.

Employees have another scheme that applies to fire departments, police departments, and other essential service personnel. Employees usually have sick days or personal time off that they can use, and they take those days when friends who need some extra cash are on call. They get the day off and the friend gets overtime for the shift. There is an understanding that the favor will be returned when the employee who took the day off needs some overtime. Paperwork requirements can also be used to create overtime. One example is leaving all of the paperwork until the end of the shift and then working overtime to get caught up. Audits of government entities show many first responders receive half of their W-2 income from overtime. This is a difficult area to control because the work needs to be done and many times there are legitimate reasons for the overtime.

Many payroll frauds can be conducted by employees in the accounting department. Accounting personnel can enter ghost employees or ghost independent contractors into the accounting system. Accounting personnel can also give unapproved raises to related employees or sometimes give an employee an unapproved raise and then split the raise with the employee by getting a kickback every payday. One case I investigated involved a property management company where the husband was the maintenance manager and the wife was the bookkeeper. She slowly raised her husband's monthly salary from \$2000 per month to \$4500 per month without the knowledge or permission of the business owner. Red flags for ghost employees include no deductions for insurance or retirement accounts, no use of sick time or vacation time, and multiple direct deposits being made to one account.

Managers and owners can also commit payroll fraud. Owners can misclassify employees as independent contractors in order to avoid paying payroll taxes on the employee's wages. Non-exempt employees can also be misclassified as exempt employees in order to avoid paying overtime. Some business owners and managers hire undocumented immigrants to work in their businesses because they can pay them off the record, usually in cash, and pay them less than the legally mandated federal minimum wage.

¶400 Cyber Frauds

Cybercrime is evolving and is becoming more sophisticated. Cybercriminals now have their own social networks and even have escrow services to protect their identities and interests when conducting online transactions with other criminals. Malware can be licensed by criminals, and, if they experience issues, there are even tech support teams to assist them with their criminal activities. Criminals can rent botnets by the day or by the hour to use in their illicit schemes. There are also pay-for-play malware programs available for purchase on the darknet in addition to an active market for zero-day exploits.¹

¶401 Data Breaches

The theft of information, also known as a data breach, is a crime that was virtually unknown two decades ago but is flourishing in the 21st century. A data breach is defined as the theft of personal information including names, Social Security numbers, birth dates, medical information, driver's license numbers, user names and passwords, and financial account information such as credit or debit card numbers. With an ever-increasing reliance on computers and information technology, organizations are increasingly susceptible to this type of fraud. Information thieves are misappropriating data and selling the stolen information on the darknet. A data breach occurs when someone gains access to information that contains confidential information. Confidential information includes personally identifying information (PII) and personal health information (PHI). This can occur because of a lack of security, the bypassing of security, or the elimination of security. Data breaches occur when information is stolen from computers and other electronic devices. Data breaches can also occur when devices containing information are lost or misplaced. Because an organization is considered to be negligent in its duties to safeguard the information provided to it by employees, customers, and others, there is a significant cost to being a victim of a data breach. Criminals breach the IT security of companies, not-for-profit organizations, and even governmental units and steal information from their computers. Often, the Human Resources department of an entity is targeted for payroll information, which includes Social Security numbers. Retail outlets are also targeted because they store customer information, including

¹ See www.knowbe4.com.

credit card numbers, on their computers. Not all data breaches are aimed at large organizations. Small businesses are also targeted, including tax providers, attorneys, medical offices, and insurance agents, because these professionals often have their clients' personal information stored on their computers.

One of the main reasons for stealing data is to profit from the data breach. Criminals can sell stolen user IDs and passwords for \$5 to \$20 each on the dark net. Criminals are aware that many people use the same passwords for multiple websites and computer systems. The purchased IDs and passwords are input into software that searches the Internet for websites where the stolen IDs and passwords work and then notifies a human operator that access has been gained so they can determine if there is any value in the website that was illegally accessed. This is known as credential stuffing. Another large market for information on the dark net is the sale of stolen credit card numbers. There are thousands of dark net sites selling stolen credit and debit card numbers. Prices range from \$2 to \$100 per credit or debit card number, depending on the validity of the numbers. Some card brokers even offer guarantees that if you purchase a minimum number of credit or debit card numbers, should any of these numbers prove to be invalid, they will replace them for free; sort of a money-back guarantee for criminals.

In addition to credit card, debit card, and Social Security numbers, criminals also purchase names, addresses, dates of birth, phone numbers, driver's license numbers, health insurance ID numbers, union numbers, and other personal identifying information (PII) on the dark net. These purchases are usually done with virtual currencies, such as BitCoin. There are even resources on the Internet for up-and-coming criminals, including books and videos on how to profit from stolen credit cards and how to do credential cramming. Stolen personal information is often used to commit identity theft.

Over the years, the theft of data has become a very profitable crime. In today's modern economy, businesses offer goods and services on credit to strangers based on the data in the buyer's credit history or through electronic means of payment such as credit and debit cards. With telecommunications and Internet technology, buyers and sellers do not need to meet in person to consummate their transaction. The Internet has made access to information almost instantaneous. Additionally, people's willingness to share personal information about themselves on social media has increased the risk of that information being misappropriated. Increased access to data on the Internet has provided criminals easier access to personal information from both inside and outside the United States. Identity thieves can use the Internet to gather an individual's identifying information without ever coming into personal contact with the victim.

Retail outlets are also targets of data breaches because they store customer information, including credit and debit card numbers on their computers. The cyberthieves targeted the point-of-sale (POS) cash registers in the Home Depot data breach, allowing them to obtain the credit and debit card information of

every customer making a purchase at the stores. Data breaches allow criminals to obtain a substantial amount of information with a minimum risk of being caught. Many data breaches are initiated through a phishing or other social networking attack wherein the criminals email or otherwise contact an individual in the target company and include a virus or other form of malware in the communication.

One of the most well-known data breaches occurred in November and December of 2013, and the victim was Target. It was estimated that 70,000,000 debit and credit card numbers were stolen from Target's computers. In addition to the debit and credit card numbers, the criminals also misappropriated the customer's PINs, CVV codes, Zip codes and other personal information. The initial estimates of the costs to Target for this data breach were \$3.6 billion. The Target data breach is important because of the litigation that followed. The banks that had to replace the 70 million stolen credit cards filed litigation against Target to recover their costs. The Federal District Court ruled in favor of the banks, and Target appealed the ruling. The Federal Appellate Court reaffirmed the lower court's ruling, and Target appealed to the Supreme Court. The Supreme Court declined to review the case, leaving the Appellate Court's ruling in place.

The courts have determined that companies have strict liability for lost information. In other words, the victims do not need to prove the stolen information was used in an identity theft. The fact that they need to pay to monitor their credit or take other actions to protect their identity creates sufficient grounds for damage awards. Businesses must use reasonable procedures to secure data in their possession. The procedures must be documented in writing and be tested or audited on a periodic basis. There is no way to guarantee that an organization will not become a victim of a data breach, but good internal controls can reduce the risk of becoming a victim of this type of fraud.

Knowledge Check Question

8. A data breach occurs when:
 - a. Information is electronically copied from a credit card by a waiter at a restaurant.
 - b. A fraudster takes a picture of a credit card while standing in line at a store.
 - c. Information is stolen from a company computer.
 - d. A shell company is used to process transactions on stolen credit cards.

¶402 Credential Stuffing

When I am speaking or conducting seminars on internal controls, I always stress the importance of having complex passwords and updating them on a regular basis. In fact, it is much better to use a complex pass phrase consisting of a minimum

of twenty-four characters, including uppercase letters, lowercase letters, numbers, and special symbols. It is much harder for a criminal to hack a passphrase than to hack a short six-character password. The fact that many individuals use the same user ID and password for multiple sites is well known to criminals.

Credential stuffing is one of the ways criminals gain access to various systems. When the criminals obtain user IDs and passwords through data breaches, phishing, or other means, the criminal uses software to test the acquired user IDs and passwords on various websites and computer systems. The criminal will attempt to access financial, social media, email, and other sites using the stolen information. Company and government websites are vulnerable because employees are not diligent in changing and protecting their passwords and often use the same password on multiple systems.

One common software for conducting credential stuffing is known as Sentry MBA. Less than 1 percent of these attempts are successful, but the successful attempts are very profitable for the criminals as they gain access to the victim's information and accounts. Remember that credential hacking is done at computer speeds, so a criminal can test the credentials millions of times an hour. If criminals are able to obtain 1 million credentials by purchasing them in bulk on the darknet, they would be able to access approximately 10,000 accounts. Also, since a user ID and password is only attempted once per website, the user ID is not locked when it does not work, so the victim is unaware their information has been tested. The criminals also use botnets (hijacked computers) so that the requests all come from different IP addresses to prevent the tested website from recognizing the access attempt is coming from a single source.

Organizations need to monitor login failure rates as a detective control to determine if they are targets of a credential stuffing attack. Adding two-factor authentication to a website is a good preventive control to limit credential hacking. Another good internal control is requiring complex passwords that contain an uppercase letter, a lowercase letter, a number, and a symbol, and requiring users to update passwords every 90 days and prohibiting the reuse of passwords.

One way to determine if your organization is being attacked by a criminal using Sentry MBA is to Google "sentry mba your company name". You can also search your web logs for some of the common user agent strings associated with Sentry MBA:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)

- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en) AppleWebKit/522.11.3 (KHTML, like Gecko) Version/3.0 Safari/522.11.3
- Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.0 Version/10.00

Knowledge Check Question

9. Which type of cyber fraud involves using stolen user IDs and passwords to try to access multiple IT systems?
- a. Data breaches
 - b. Credential stuffing
 - c. Ransomware
 - d. Phishing

¶403 Ransomware

Another type of cyber fraud that has been growing in the last year is ransomware. Ransomware is a type of malware that is placed on a computer and then encrypts all of the files on the computer. The criminals then require that the victim pay a ransom in order to obtain the decryption key and have access to their files. The most well-known example of ransomware is CryptoLocker. Cryptowall 2.0 is a newer version of ransomware being used by cybercriminals.



The FBI estimates that ransomware is a \$1 billion a year fraud. A new type of ransomware, called Reveton, installs itself onto the computer without the

user's knowledge. Then, the computer freezes. A bogus message from the FBI pops up on the screen, saying the user violated federal law. To unlock their computer, the user must make a payment to the criminals.



For a single computer, the cybercriminals will initially request a ransom ranging from \$300 to \$500. Larger ransoms are demanded when more computers are infected with the ransomware. Once the deadline for the payment has passed, the criminals up the ransom demand to around \$1000 per infected computer.² Unfortunately, criminals are not always honest. When a victim makes a payment, sometimes the criminal gives them the decryption code, sometimes the criminal asks for more money, and sometimes the decryption code doesn't work and they refer the victim to a 900 number help desk where the victim pays by the minute for help decrypting his information. Governments have also been victims of ransomware. In the spring of 2018, the City of Atlanta was infected with ransomware that shut down city services for weeks.³

Typical ransomware software uses RSA 2048 encryption to encrypt files. Just to give you an idea of how strong this is, an average desktop computer is estimated to take around 6.4 quadrillion years to crack an RSA 2048 key.⁴ One issue with ransomware is that it is a franchise-type criminal activity. Criminals

² <https://www.knowbe4.com/>

³ <https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html>

⁴ <https://www.knowbe4.com/>

with no programing experience can contact ransomware developers on the darknet. The criminals pay an initial fee to get access to the ransomware, and the developer provides them with a link to send out to all of their contacts. If victims click on the link, infect their systems with ransomware, and pay the ransom, the criminal gets 80 percent of the ransom and the developer gets 20 percent.

Knowledge Check Question

10. Which of the following cyber frauds encrypts the data on your computer?
- a. Phishing

b. Ransomware



c. Spoofing

d. Spyware


¶404 Phishing

Phishing is a cybercrime in which the criminals contact the victim through email messages that appear to come from legitimate business or government sources. Social networking through phishing schemes is a common way to get around an organization’s IT security. Often, the email headers are spoofed to make them look legitimate. One purpose of the phishing email is to obtain information such as names, addresses, Social Security numbers, phone numbers, dates of birth, credit card numbers, EIN numbers, and other personal information from the victims. When the victims supply the information, the criminals are able to use the information to steal the victim’s identity and assets. Criminals also send phishing emails containing links with the hope that the victim will click on the link and download the criminal’s malware onto the victim’s computer.

Phishing Email Example 1

 Kevin miller <spavogt@aol.com> 

2016 tax information

 Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox. We converted this message into plain text format.

Hi,

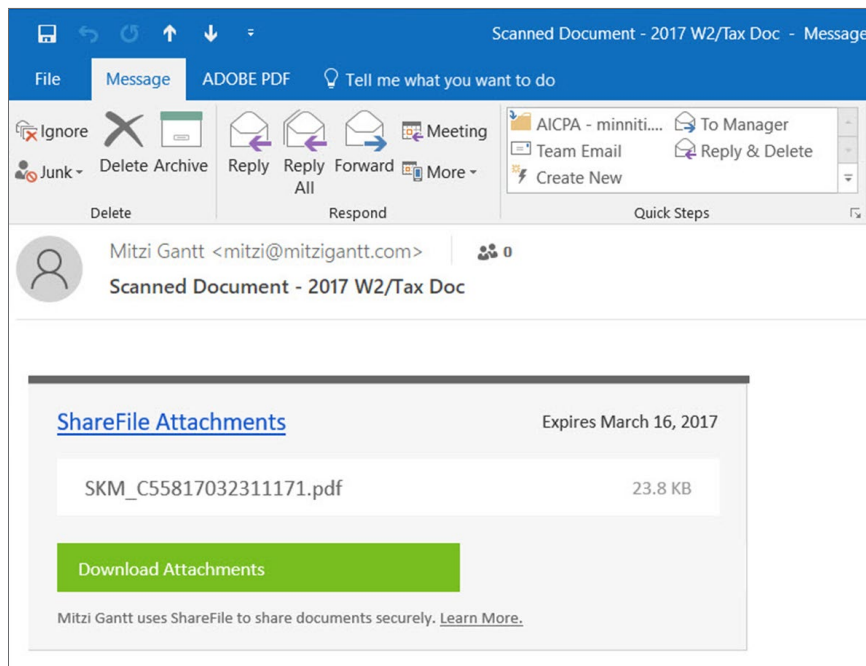
I'm ready for you to do my taxes, so attached is a Adobe document with all my statement forms. The Adobe is encrypted for security and privacy. To open the file here <<http://tinyurl.com/zrpkb05>>

Can you please, let me know you've received this e-mail, and able to open the document.

Forms include:
*W2 Work Statement
*Mortgage loan Statement
*Installment Loan
*HSA Statement (1099-SA)

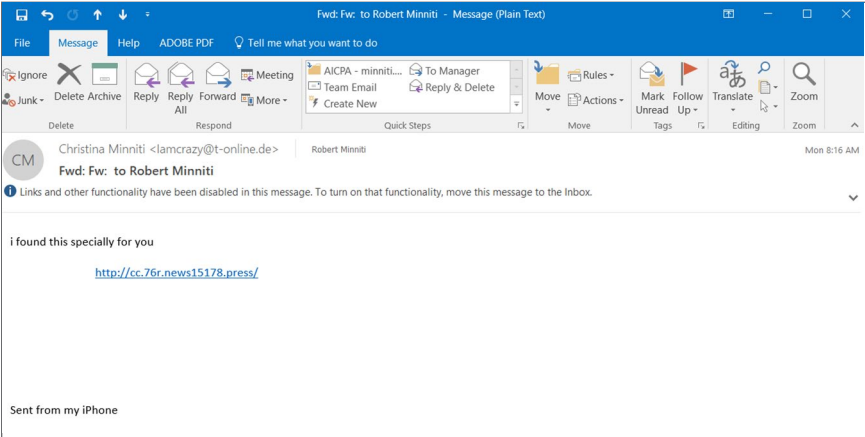
This email was sent out during tax season to tax preparers and at first glance appears to be a request for assistance with personal taxes. If the recipient clicks on the link to download the tax data, their computer will be infected with malware. Be alert for phishing emails that include poor grammar in the text of the message and that provide no contact information, such as a phone number or address. Also note that most phishing emails come from outside the United States or use free services like Gmail and AOL.

Phishing Email Example 2



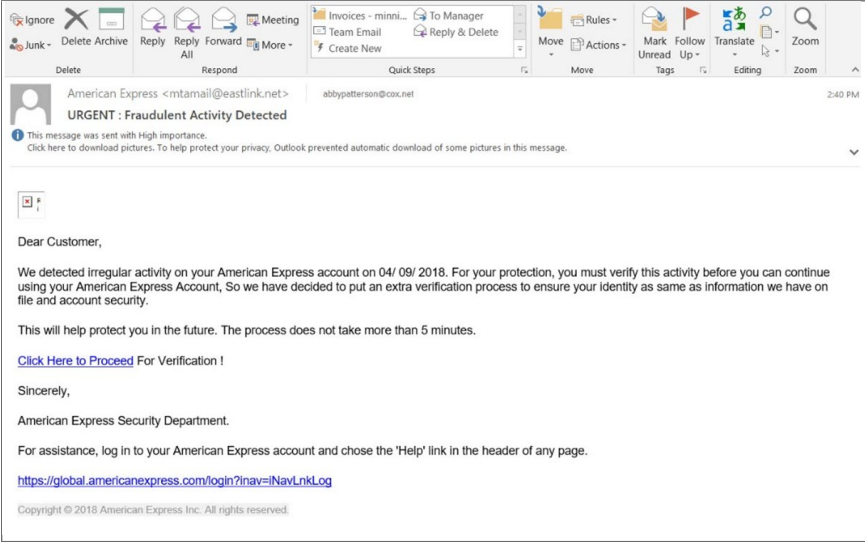
In this phishing example, the fraudster is trying to get the victim to click on a link for a ShareFile attachment, and if the victim clicks on the link, their computer is infected with malware. DropBox and other file service providers have also been used for this fraud.

Phishing Email Example 3



With this example, you can see the fraudsters spoofed my daughter’s email in order to make it look like the email was coming from her. The criminals get the names of your friends, relatives, and associates from your social media accounts and then send you phishing emails containing links that will download malware onto your computer that look like they are coming from someone you trust.

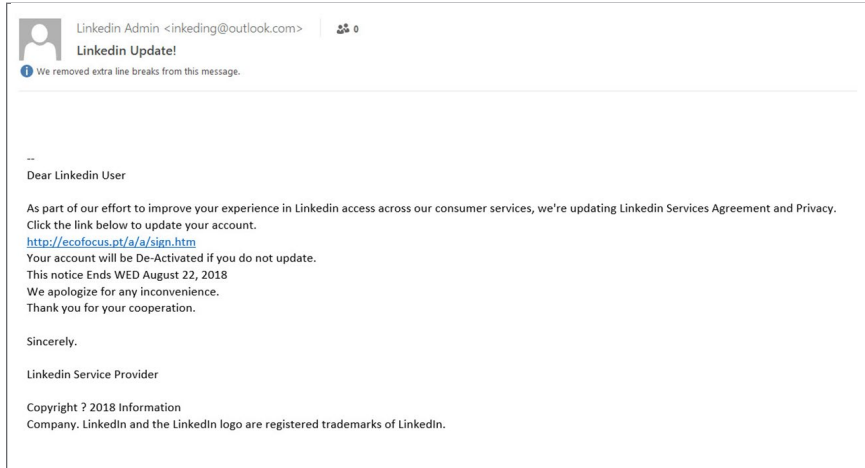
Phishing Email Example 4



Criminals will often try to make you think a phishing email is coming from your bank, credit card company, or other financial institution. They may indicate there is a problem with your account or that your password is expiring.

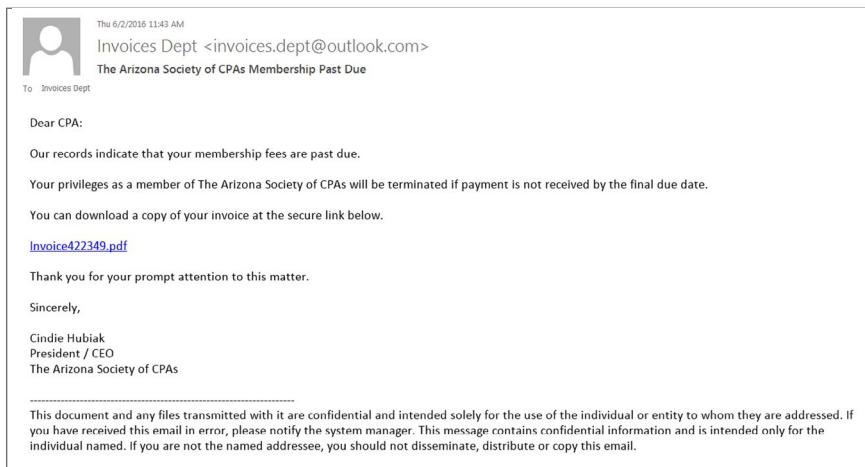
Either way, they ask you to click on the link in the email and enter your user ID and password. Once they have that information, they can use your user ID and password to access your real accounts and misappropriate all of your funds.

Phishing Email Example 5



Criminals also use phishing emails to try to convince you there is an issue with your social media accounts, or that your accounts need to be updated. They will stress the fact that you will lose all your posts on Facebook, Twitter, LinkedIn, etc., if you don't immediately log in through the link in the email and update your account.

Phishing Email Example 6



Some criminals actually do their research before sending out a phishing email. This is known as spear phishing. They gather information on the prospective victim and tailor a phishing email directly at them. These emails can include the victim's name, and the names of people the victim knows. This phishing email purports that I failed to pay my ASCPA dues in a timely manner. It even includes information for Cindie Hubiak, who really is the president of the Arizona Society of CPAs. The criminals went to some effort to make this look like a legitimate email. Once again, note the lack of contact information in the body of the email. Also, the email came from a outlook.com email address rather than the society's normal ascpa.com address.

¶405 Vishing

Vishing is similar to phishing except the criminals use phones instead of emails. The criminals will call a new employee or newly promoted employee (they get the information from social media) pretending to be from the IT department, and tell the employee they need to finish setting up their computer for the access they will need. The criminals tell the employee they need to remote into their computer, and then once inside the system set up a backdoor so they have continued access to the company's computer systems.

Vishing calls are also made to alert individuals or businesses that fraud has been detected on their credit cards. The criminals use spoofed phone numbers to make it appear that the call is coming from a bank or financial institution. The criminals then ask the victim to verify information on the credit card, such as the account number, billing zip code, security code, or expiration date, in order to gain access to information that will allow them to use the credit card.

Other common vishing calls include calls that claim to be from the Internal Revenue Service (IRS) trying to collect past due taxes, calls from collection agencies trying to collect past due bills, and calls from law enforcement or regulatory agencies trying to collect fines. A red flag for vishing calls is a request that payment be made with gift cards, with virtual currencies, or by sending money through a money transfer service. They will also stress the urgency to pay immediately in order to avoid jail time or other penalties.

¶406 Brand Hacking

Brand hacking occurs when criminals post false or misleading information on websites about a company's products or services or about the company itself. This is usually done via social media websites, rating websites such as Trip Advisor, or individual blogs. The criminal's purpose when brand hacking is to tarnish or damage the reputation of the brand being hacked. Negative ratings

on the Internet can steer customers away from a product or business. A twist on the concept of brand hacking occurred when a hotel chain paid its employees to rate their “roach motel” as a four-star resort on various travel sites, enticing customers with fictitious reviews to get them to stay there. For businesses in the service industry, the hackers can also go after the personal brand or the reputation of the organization’s employees, often implying sloppy or unethical work. Brand hacking is often linked to unsatisfied customers, disgruntled current or former employees, and a business’s competition.

¶407 Spoofing

Spoofing is a term used to describe activity that makes a fraudulent website or email look legitimate. Criminals can also spoof phone numbers and social media accounts. The purpose of spoofing is to make the victim believe they are communicating with someone they know, when, in fact, they are providing information to the criminals.

The CEO invoice spoof is a common type of email spoofing fraud directed at companies. The typical CEO email spoof occurs when criminals send an email to an accounting clerk, bookkeeper, or payables manager that appears to have originated from the CEO, CFO, or other senior executive of the company. There is usually an invoice attached with instructions to wire or ACH the funds to the vendor as soon as possible. There is usually a tone of urgency applied such as, “Don’t leave work until this is done” or “We will have to pay a large penalty if the payment isn’t received today” to spur the employee into processing the transaction quickly. The bank account receiving the funds is usually overseas, or, if it is in the United States, the funds are immediately transferred overseas when they are deposited. Another version of this cybercrime requires the request for copies of payroll records or W-2 and other tax records, giving the criminals access to personal information of the company’s employees. In 2018, for the 2017 tax season, there were a large number of spoofing emails that appeared to come from a company’s auditors requesting payroll information and claiming the information was needed to complete the audit.

¶408 Denial of Service (DoS) Attacks

Denial of service (DoS) attacks occur when criminals use their own computer networks, or botnets, which are networks of infected computers, to bring down a website or computer system by overloading its capabilities, thereby crashing the system. In many instances, the criminals follow up on the DoS attack with an attempt to hack into the system and upload malware onto the victim’s computer while the victim is busy trying to fix the damage being done by the denial of service attack.

The most common and obvious type of DoS attack occurs when an attacker “floods” a network or website with large amounts of information or requests for access. When you type a URL for a particular website into your browser, you are sending a request to that site’s computer server to view the webpage. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can’t process your request. This is a “denial of service” because you can’t access that site. In a distributed denial of service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is “distributed” because the attacker is using multiple computers, including yours, to launch the DoS attack.⁵

¶409 Pharming

Pharming occurs when a virus or other malicious software is placed on the victim’s computer. The malware hijacks the victim’s web browser and causes it to divert the user to the criminal’s websites. When the victim types in the website for a legitimate company, usually a bank or financial institution, the malware directs the victim’s browser to a fictitious copy of the website set up by the criminal. The fraudsters often copy the legitimate website, so it can be difficult to recognize that you have been diverted. The criminal is hoping to capture the victim’s user ID and password or other useful information. Pharming can also be done by exploiting vulnerabilities on an organization’s website to allow the criminals to redirect legitimate customers to a spoofed fraudulent website. It is important to always verify the website address before entering any confidential information, such as a user ID or password, onto the site. Often the change will be minor, such as “BanksofAmerica” instead of “BankofAmerica”.

¶410 Hacking

Virtually everyone has heard of hacking. Hacking is commonly done by placing malware on a computer system in order to allow the criminals to gain control of the victim’s computer or to gain access to information stored on the computer or other electronic device. Hacking is usually done over the Internet, and any device connected to the Internet with either a wired or wireless connection is at risk of being hacked. Computers, cell phones, tablets, webcams, IoT devices, and other electronic equipment connected to

⁵ Department of Homeland Security, www.us-cert.gov/ncas/tips/ST04-015.

the Internet are the main targets of cybercriminals. As the world is becoming more automated, cybercriminals are increasingly attacking robots and automated production systems in addition to computer information systems. Gaining control of a robot such as a self-driving truck transporting goods would allow the criminals to hijack the shipment. Locking up the robots in a factory and halting production allows the criminals to extort a payment from the company to release their automated systems.

A common tool used by cybercriminals in a computer hack is a computer virus. A computer virus is a segment of computer code that attaches itself to a program, such as Microsoft Office, that is already loaded on the victim's computer. A computer virus can cause the infected program to delete, email, or copy files on the computer or to perform other actions such as altering files or destroying data. A computer virus creates copies of itself that it inserts in data files thus when employees share files they also share the computer virus allowing the virus to spread throughout the company's system and to customers, vendors, and others with whom files have been shared.

Another common type of malware is known as a Trojan or Trojan Horse. A Trojan is a stand-alone malware program that is disguised as something else, usually a program or application that the user wanted such as a computer game. Trojans, unlike viruses, are stand-alone programs and do not need to infect a program already installed on the computer but instead act on their own. Typical types of trojans include spyware, keystroke loggers, and other software designed to compromise a system or to gather data from a system. Malware can also be used to make an individual device or system part of a botnet. A common use is to infect computers to create a network of slave computers that is then used to mine crypto currencies like BitCoin. Trojans are often disguised by piggy-backing on them on a free program or application downloaded by the unsuspecting user of the device.

A computer worm is a type of malware that transmits itself over networks and the Internet and infects any computer connecting with an infected source such as an infected website. Computer worms can be transferred by linking to or visiting infected websites. A computer worm is a stand-alone program that does not need to attach itself to an existing program on the computer. A computer worm can carry a payload such as a ransomware program. The most common payload is a program that installs a backdoor on the infected computer. You are probably aware of how websites install "Cookies" on your computer when you visit the website. You could consider a worm to be a bad cookie.

A rootkit is specifically designed to modify the operating system of an infected computer. Legitimate uses for rootkits include installing updates and patches to a computers operating system. However, criminals use rootkit programs to hide other malware from the user of the computer. Because a rootkit

program has administrator access, it is not only able to modify the operating system but can also modify any other software installed on the computer. Rootkits can be used to hide malware that the criminals placed on a victim's computers, so the victim can't find or remove the malware. Often the only fix when this is done is to wipe the computer and reload everything from a backup.

A very dangerous type of malware is known as a backdoor. A backdoor allows the cybercriminal unimpeded access to the infected computer, allowing the criminal to bypass the normal authentication processes. A backdoor usually provides the hacker with administrative access to the infected computer. A backdoor is the equivalent of the criminal having their own user ID and password to gain access to the system whenever they want.

It's a common misconception that hackers are geniuses that dropped out of MIT and are working on supercomputers in their basements. Although there are a number of hackers who can bypass an organization's firewalls and other cybersecurity defenses to gain access to a system, a majority of hacking attacks are done using social engineering. An organization's employees are the weakest link in the organization's cybersecurity defenses. The hackers know this and attack the employees with phishing and vishing attacks, or by friending them on social media websites and then sending them infected links.

A common method for infecting mobile devices with malware is through a charging station. Cybercriminals load malware onto charging stations located in public places like airports, malls, sports arenas, and subways. Unsuspecting users whose batteries are running low, use their USB ports to connect to the charging stations to recharge batteries in their devices. While they are connected, the data on their devices is copied, and malware is installed. Employees should be required to use USB condoms whenever recharging a company mobile device at a non-company location. The USB condom blocks the data ports and prevents any transfer of data while allowing the battery to be recharged. An alternative is to only charge devices through a standard electrical outlet.

¶500 Financial Frauds

¶501 Credit and Debit Card Fraud

Stolen personal information is often used to commit credit card fraud. According to Statistic Brain, 40 percent of all financial fraud is related to credit cards. This amounts to a total of \$5.5 billion in credit card fraud worldwide annually. The same report breaks this down into five types of credit card fraud: 37 percent is counterfeit credit cards, 23 percent is lost or stolen cards, 10 percent is “no-card” fraud, such as giving information to a non-legit telemarketer, 7 percent is cards stolen during mailing, and 4 percent is identity theft.¹

Most credit and debit card fraud occurs in the United States. In fact, a 2015 research note from Barclays stated that the United States is responsible for 47 percent of the world’s credit and debit card fraud despite accounting for only 24 percent of total worldwide payment card volume. U.S. credit card fraud is on the rise. About 31.8 million U.S. consumers had their credit cards breached in 2014, more than three times the number affected in 2013. Credit card fraud isn’t cheap for the banks and financial institutions either. Nearly 90 percent of credit and debit card fraud victims in 2014 received replacement credit cards, costing issuers as much as \$12.75 per card.² Despite the risk of fraud, credit and debit card transactions have been increasing over the last decade. There are over 407 million credit cards in use in the United States alone and over 1.5 billion credit cards in use worldwide according to CreditCards.com. Additionally, there are approximately 1.9 billion debit cards being used worldwide.

Credit card application fraud is done by submitting false information to the financial institution to obtain credit cards. This is often done online or through the mail. Fraudsters also take over existing credit and debit card accounts. This can be done by using stolen credit card information to make online purchases or by creating a duplicate credit or debit card to use for live purchases. Criminals can purchase a credit and debit card duplicator online for around \$150. They can also purchase blank cards, including EMV cards on the Internet. A common method used by criminals is to purchase a five-dollar gift card, then to use the gift card and then copy the stolen information onto the gift card using the duplicator. This allows them to present the gift card

1 <https://www.cdkpay.com/fraud-risk-management/credit-card-fraud-detection/>

2 <http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388>

with the appropriate logo on the card, instead of using a blank white card to make a purchase. Some larger credit card fraud rings actually order credit and debit card blanks that are printed with the appropriate logos and contain all the security features of the cards issued by the banks.

Knowledge Check Question

11. There are approximately _____ credit cards issued worldwide.
- a. 407 million
 - b. 1 billion
 - c. 1.5 billion
 - d. 1.9 billion

¶502 EMV Card Present Fraud

While many people believe the security of their credit and debit cards has increased because the banks and card issuers added EMV (Europay MasterCard and VISA) chips to the cards, this may not in fact be true. Although the EMV chips make it more difficult for criminals to skim the information on the card and create a duplicate card, the criminals have developed a new fraud scheme to take advantage of the vulnerabilities of the EMV chips. These chips are RFID, and you can pay for a transaction by waving the EMV chip card over a point-of-sale transaction device designed to capture the RFID information. What most consumers don't know is that the chips in a smart card can be read at distances up to three feet away.

The criminals are aware of the new chip card's vulnerability and they use portable, battery operated, point-of-sale devices to capture the information broadcast by the smart cards and process card present transactions. The criminals go to crowded areas such as malls, sports venues, subways, buses, and other public places carrying these portable devices and have them automatically process a card present transaction for under \$50, which is the federal legal limit for the amount of a fraudulent transaction that is the responsibility of the consumer. For fraudulent transactions over \$50, the card issuer is responsible for the transaction. When consumers attempt to dispute these transactions, some card issuers will argue that since the card was present, and you still have possession of the card, it must be a legitimate transaction. They may even imply you just forgot about it.

Businesses and consumers need to protect themselves from this type of fraud. If you have a smart card with an EMV chip, you need to carry the debit or credit card in an RFID sleeve or an RFID safe wallet. RFID sleeves and RFID safe wallets have a lead lining that prevents portable point-of-sale devices from reading the RFID chips while you are carrying your card in your pocket, wallet or purse.

¶503 Obtaining Credit Card Information

Criminals use multiple methods for obtaining credit card information. One way is through data breaches like the Equifax data breach that occurred in 2017, where the criminals were able to steal the personal information of 147 million individuals. Another common way to obtain credit card information is through the use of credit card skimmers. These can be either handheld or attachable devices. Handheld skimmers are used by individuals who have access to a credit card, such as a waiter or waitress who takes a customer's card to the back to process the payment and then skims the information from the card. Attachable skimmers are attached to ATMs, point of sale devices, and gas pumps, just to name a few. When customers use credit or debit cards on these payment systems, the information is copied for the criminals. The criminals often put cameras up around ATMs and other places cards are run to record Personal identification numbers (PINs) and billing zip codes to make it easier to use the cards they create with the skimmed information. Another common method for gathering credit and debit card information is to stand behind someone in line at a retail store and use a cell phone to record the information on a card when the person in front of them in line presents it to the clerk.

Once the criminal has obtained the information on the credit or debit card, they can then use a credit card duplicating device to create a copy of the card. I was able to purchase a copy of a credit card duplicator on the Internet for \$150 and was able to purchase blank cards for a few cents each. The chip cards cost a little more, around 20 cents when purchased in bulk. I did a test run and copied one of my own credit cards. I then went to a local retail store and made a purchase using a plain white card by swiping the card through the magnetic reader at the retailer. The cashier never asked to see the card nor did she ask for identification. I was able to make a purchase exceeding \$250 with a plain white card and a copied magnetic strip. Based on the ease of this transaction, I am sure you can see why criminals find this to be a very profitable endeavor.

¶504 Investment Frauds

When discussing investment scams, the first one to come to mind is churning. Investment advisors buy and sell securities in a customer's account not to benefit the customer but to generate commissions for the investment advisors. Selling inappropriate investments to generate commissions is another type of investment fraud. In one case the investment advisor was visiting elder care centers. He convinced a 94-year-old victim to cash out her certificates of deposit and purchase a 40-year annuity with an 18 percent front load and a 12 percent early termination fee. The victim would have had to live to be 134 to break even on this investment.

Pump and dumps are another type of investment fraud. The criminals purchase a non-performing stock, usually a penny stock, and then hype the stock on the Internet or at investor luncheons. As the victims buy in, the criminals' cash out and take their profits. One version of the pump and dump is done by leaving messages on voice mail that sound like the caller got the wrong number. For example, "Bill, don't tell anyone, but the law firm I'm working with is working on a deal for Google to purchase XYZ Corp, buy the stock now if you want to make a bundle."

¶505 Ponzi Schemes

A Ponzi scheme is an investment fraud in which the fraudster promises high financial returns or dividends that are not available through traditional investments. Instead of investing the victims' funds, the fraudster pays returns to the initial investors using the principal amounts provided by subsequent investors. The scheme generally falls apart when the fraudster flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of investment returns.

¶506 Pyramid Schemes

Pyramid schemes, which are also called franchise fraud, are marketing and investment frauds in which a victim is offered a distributorship or franchise to market a particular product or service. The real profit is earned not by the sale of the product or service, but by the sale of new distributorships or signing up new members. The emphasis in a pyramid scheme is on selling franchises and recruiting new members, rather than on selling the product. Eventually this leads to a point where the supply of potential investors is exhausted and the pyramid collapses. At the heart of each pyramid scheme is the claim that new participants can recoup their original investments by inducing two or more new prospects to make the same investment. Promoters fail to tell prospective participants that this is mathematically impossible for everyone to do, as eventually you run out of new victims to con.

¶507 Advance-Fee Scams

An advance-fee scam is a confidence trick in which the victim is persuaded to advance sums of money in the hope of realizing a future benefit. Current versions of this scam used against consumers include getting advance payments from victims for credit repair, employment opportunities, mortgage modification, debt consolidation, and for obtaining a loan. For businesses, the fraudsters promise business loans and credit lines, contacts with foreign

buyers, introductions to decision makers, inside information on projects and bids, etc. Fraudsters often use official-sounding corporate names to help gain the confidence of the victim. Once the fees are paid, the fraudster absconds with the money and no services are performed.

¶508 Bankruptcy Fraud

One classic example of bankruptcy fraud is the “bust out.” This scheme starts with the criminals creating a corporation and a great sales pitch. The criminals bring in investors and secure loans for the new business. The criminals use all the funds to pay themselves, and to pay for lavish business trips for the founders. When they have pulled all of the money out of the company, they file for bankruptcy, leaving the creditors and equity investors with the losses.

It is also common for individuals and business that are going through a legitimate bankruptcy to commit bankruptcy fraud. This can be done by hiding assets from creditors and the bankruptcy court. I’ve always found it interesting that a bankruptcy debtor can remember every debt they have, even that they borrowed two dollars from a college friend to buy a beer, but they can’t remember what happened to their assets. In one case an individual claimed to have misplaced \$500,000 in gold coins that were collateral for a loan and couldn’t find them. The amazing thing was she never reported the loss to her insurance company or filed a claim for the missing coins.

In addition to transferring assets, another scam used to protect assets is to file fraudulent liens on the property. Related entities and shell companies can also be used to file fraudulent liens. This is commonly done with real property and registered personal property. The fraudulent liens are filed in the name of friends or relatives, but no loan took place. The liens are put in place to eliminate any equity in the property. Obtain proof of a transfer of funds for any liens from friends, related entities, and relatives.

The bankruptcy courts can be used by criminals to forestall a foreclosure on real property. This was fairly common after the real estate bust. When a house is in foreclosure, it is put up for sale at an auction on the courthouse steps. The fraudster goes to the bankruptcy court to find an individual who is in bankruptcy. This is easy to do since all bankruptcy court records are a matter of public record. Once they get the name and case number of the victim, a day or two before the foreclosure sale the fraudster files a quit claim deed with the county recorder to make the bankruptcy debtor a one percent owner of the real property. This triggers the automatic stay, and the property can’t be sold without the permission of the bankruptcy court. The lender has to schedule a debtor’s hearing with the court. The debtor testifies they know nothing about the property, do not have and never had an interest in the property, and also

note they never signed the quit claim deed. The creditor then gets to start the foreclosure over again, and a day or two before the foreclosure sale another quit claim deed is filed, giving a one percent interest in the property to a different bankruptcy debtor.

¶600 Identity Theft

Identity theft is a crime that 20 years ago was hardly a concern for businesses or individuals; however, today it is one of the most recognized crimes in the United States. This does not imply that identity theft did not occur 20 years ago. Instead, the effects on the victims were less noticeable. People in the 18th century coming to America from Europe could use the identity of a person still in Europe with little or no effect on that person. Even during the 19th century, it was common for someone in the United States to move west and assume a new identity to escape criminal charges or creditors. Indeed, until the passage of the Social Security Act in 1935 and the issuing of Social Security numbers, a person's identifying information consisted mostly of his or her name and face. Even as late as the 1960s and 1970s, if you wanted to check a person's credit, you had to call all of his or her creditors individually, and you had to trust that person had provided you with a complete list.

Over the years, identity theft has become a more profitable crime. This is because in the modern economy, businesses offer goods and services on credit to strangers based on the data in the buyer's credit history. With telecommunications and Internet technology, buyers and sellers do not need to meet in person to consummate their transaction. The Internet has made access to information almost instantaneous. Increased access to data on the Internet has provided identity thieves easier access to an individual's personal information from both inside and outside the United States. Identity thieves can use the Internet as a means to gather an individual's identification without ever coming into personal contact with the individual.

Identity theft is broadly defined as the use of one person's identity or personally identifying information by another person without his or her permission. Identity theft is a type of fraud and can be committed against an individual or an organization. Fraud is defined as making a false statement, omission, or action that someone else relies upon and based on that reliance gives up something of value. By using false information to obtain items of value, identity thieves are committing fraud.

The federal criminal definition of identity theft is when someone "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in

connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”¹

Until 1996, identity theft was not recognized as a crime at the state level. Arizona was the first state in the United States to pass laws against identity theft. Arizona made taking the identity of another person or entity or knowingly accepting the identity of another person a class 4 felony.² Aggravated identity theft of another person or entity is classified as a class 3 felony.³ Aggravated identity theft includes taking the identity of three or more persons by purchasing, manufacturing, or possessing any identifying information or where the economic loss from the identity theft exceeds \$3000. Arizona also identifies trafficking in the identity of another person or entity as a class 2 felony.⁴ Trafficking in the identity of another person or entity includes any sale, transfer, or transmission of any personal identifying information to obtain or continue employment or for any unlawful purpose whether or not an actual loss is suffered by the victim. Other states have followed Arizona’s lead by adopting laws criminalizing identity theft. Because identity theft is changing by adapting to new technology and thieves are finding new ways to obtain identifying information and new ways to benefit from its fraudulent use, state laws have not kept up with the changes in the methods used to commit identity theft.

Identity theft has become a major problem on both national and international levels. On May 10, 2006, President Bush issued Executive Order 13402, which established the Identity Theft Task Force. Seventeen federal agencies and departments were appointed to create a national strategy to combat identity theft.

To cushion businesses from the effects of identity theft, the Federal Trade Commission has taken several steps. For example, in 2008, the Federal Trade Commission adopted the “Red Flags Rule,” which requires organizations identified in the rule to develop and implement written identity theft protection programs. The Red Flags Rule applies to all businesses that allow a consumer to pay for a product or service after the product has been received or the service is performed.

¶601 Criminal Identity Theft

Many of us are aware of the issues with financial identity theft; which occurs when someone misappropriates your personal information to open new accounts or uses your existing accounts to make purchases. A new type of identity

1 18 USC § 1028(a)(7).

2 Arizona Revised Statutes § 13-2008.

3 Arizona Revised Statutes § 13-2009.

4 Arizona Revised Statutes § 13-1010.

theft is spreading across the country, and it can be even more damaging than having a criminal destroy your credit rating. This new type of identity theft is known as criminal identity theft.

The typical pattern for criminal identity theft is for the criminal to first misappropriate your Social Security number and personal information. There are various ways to do this, including data breaches, mail fraud, phishing, vishing, etc. Once they have your personal information they use your name and Social Security number to set up a shell company, which is usually an LLC because it is the easiest to set up. The paperwork for the shell company will be filed with the state, but there are no operations nor is there any real business being conducted. After they have the shell company approved, they open a bank account, with you as the principal, again using your Social Security number, as the sole owner of the LLC. The address for the shell company will usually be a box at a mailbox store that was rented in the victim's name, usually paid with cash in advance.

In setting up the shell company and bank accounts, it is sometimes necessary to have documents notarized. To accomplish this, the criminal orders fake notary seals because they know the notary's credentials will rarely be challenged. Just to prove how easy it is to get a fake notary seal, I ordered one for "I'm A Crook," which cost me \$25 and expires in 2020. So if I were a criminal, I could use that to notarize documents. As long as the criminals are willing to pay the fees, they can get as many notary stamps as they want.

Once the shell company and bank accounts are set up, the fraudsters get to work cashing stolen checks and processing transactions from stolen credit cards in the shell company's bank accounts. In one case in Houston, Texas, the fraudster was able to cash over \$5 million in stolen checks in this type of a fraud scheme. Once the funds are available in the accounts, the criminals immediately wire the money out of the accounts, usually on the very same day the funds were released. The funds are usually sent to overseas bank accounts to make it more difficult to trace. The money is then laundered and put back into the economy.

This situation works well for the thieves because when law enforcement is advised of the fraudulent and stolen checks, and the multiple transactions being processed on stolen credit cards, they launch an investigation into the accounts where these funds were deposited, and this leads them to the shell company. Since the identity theft victim's name and Social Security number are listed on the shell company and bank account, that person becomes the prime suspect for law enforcement investigating the stolen funds. Usually, the victims of criminal identity theft don't know they have a problem until law enforcement officers show up at their home or place of business with an arrest warrant and a search warrant. This puts you in a difficult position because you get to do a perp walk and spend time being interrogated by law enforcement,

who usually don't believe it when you tell them you are innocent. You have to give them proof you didn't do it.

As you can see, criminal identity theft can cause a person serious embarrassment and cost a significant amount in legal fees to clear their name. Unfortunately, using a credit monitoring service usually won't alert you that you are a victim of criminal identity theft. In addition to reviewing your credit report on a regular basis, it is also necessary to run a background check on yourself to find out if you are listed as an owner or statutory agent on any businesses you don't recognize, and to find out if there are any warrants out for you or if any litigation has been started listing you as a plaintiff. Running a regular Google or other search on your name can also be helpful in detecting criminal identity theft. Unfortunately, just like with financial identity theft, there is no way to guarantee you won't be a victim, so you need to take proactive steps to protect your personal information and carry identity theft insurance to cover the expenses of clearing your name.

Knowledge Check Question

12. Which of the following types of fraud involves opening bank accounts using false information?
- a. Cash drawer loans
 - b. Skimming
 - c. Criminal identity theft
 - d. Refund fraud

¶602 Sockpuppets

Is your personal information safe on your social media sites? Unfortunately, many people will accept any friend requests they receive, putting them at greater risk for identity theft. In the increasingly active world of identity theft, criminals have to find ways to gather information on their victims. One common way of gathering information is to set up fake social media accounts, known as sockpuppets, and use the fake accounts to “friend” people. Obviously, the criminals don't want to use their real names or social media accounts because these would be easy to trace in an identity theft investigation.

The criminals start by getting fake personal information on websites like fakenamegenerator.com. This website produces a fake name, address, birthdate, phone number, mother's maiden name, etc. It also gives you the opportunity to validate the fake Social Security number you help generate. To further backstop the fake identity, the criminal is provided with an email address, employment information, height, weight, blood type, and a credit card number with an

expiration date and CVV number.

Once the criminals have the fictitious identity information, they open accounts on social media websites, dating websites, etc., in order to gather information. They send out multitudes of friend requests to everyone they can find on the sites. Similar to a phishing email, they are hoping you will accept their friend request. Once you accept, they have access to your information and the information of your other friends.

To protect yourself, take a little extra time to look at the profile of the person sending you a friend request, unless of course you know them already. To spot a sockpuppet, look for few, if any, postings; few pictures; only one or two employers; no group membership; one or two schools; one or two addresses; etc. Another giveaway is few, if any, recommendations. Usually, the criminals don't take the time to fully develop the sockpuppet profile. There could be major gaps in their employment history or their profile shows they have worked for 20+ years in the same entry-level job.

¶603 Medical Identity Theft

Medical identity theft occurs when the fraudster uses the medical insurance of the victim. Most victims fail to notice this type of identity theft because the bills are sent to the insurance company and the provider of the medical services has been given a false address for sending bills to the fraudster. This type of identity theft can cause far greater harm than just the increased insurance premiums. In today's computerized world, your medical records are becoming digitized and available to various providers of medical services. A doctor or hospital could provide the incorrect treatment or refuse treatment based on false information in your medical records. Some of the signs of medical identity theft include: items on your explanation of benefits (EOB) that you do not recognize, including procedures and doctors; a bill for medical services you did not receive; and calls from collection companies for unrecognized medical bills.

Medical identity theft can occur in a number of ways. The most basic is an identity thief using your medical ID number to receive medical services while avoiding paying for the services, usually because they can't afford to purchase their own insurance. Another form of medical identity theft occurs when criminals set up fake doctor's offices or pharmacies and then bill the insurance companies for products and services that were never provided. The other common type of medical identity theft is drug addicts using your medical ID number to obtain prescription drugs. Some drug dealers have even been caught doing this and then selling the drugs on the street.

One issue with medical identity theft is that under current law, many victims do not have the right to review their medical files or correct errors in

the files. HIPAA rules make it difficult for individuals to discuss their medical information and find errors. Also, victims of medical identity theft do not have the legal right to prevent health-care providers, insurance companies, and medical clearinghouses from re-reporting any information that was originally reported due to the identity theft. With medical identity theft, the criminal doesn't need your Social Security number. Your medical ID number, date of birth, and address are usually enough information to commit the crime.

The Ponemon Institute, in its Fifth Annual Survey on Medical Identity Theft,⁵ reported that the average cost to clear up an issue of medical identity theft is \$13,500. NBC News reported instances of medical identity theft in 2014 exceeded 2.3 million victims.⁶ Since the passage of the Affordable Care Act, there has been an increase in medical identity theft. The most common way for criminals to obtain your health insurance information is by hacking government computers, insurance company computers, hospital computers, pharmacy computers, and computers in doctors' and other provider's offices.

In addition to the financial costs, the costs of medical identity theft could be life-threatening. Cases of individuals being administered drugs that they were allergic to and even being given the wrong blood type in emergency situations have resulted in death because the wrong information was entered into the computer when the identity thief used their medical ID and the hospital relied on the medical records in the computer. In another case, a woman used a stolen medical ID to cover the costs of the birth of her child. The identity thief's drug test came back as positive for illegal drugs, so child protective services removed the victim's children from her care because she was a drug addict. The victim then had to go to court to get her children back.

¶604 Insurance Identity Theft

Medical insurance is not the only type of insurance stolen by fraudsters. Individuals who are uninsurable or who would otherwise pay extremely high insurance premiums use insurance identity theft as a means of obtaining insurance. A good example of this is auto insurance. An individual with multiple DUIs who cannot obtain insurance purchases car insurance in the name of the victim. The fraudster usually purchases the minimum required by state law to avoid being arrested if he or she is pulled over for another traffic offense, as all states require drivers to carry insurance. This type of insurance fraud not only hurts the victim whose identity was stolen, and who usually finds out

5 http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

6 <http://www.nbcnews.com/tech/security/stolen-identity-2-3-million-americans-suffer-medical-id-theft-n311006>

about the crime when they are sued for an accident in which they were not involved, but also harms the victims in the accident who find out there is no insurance to cover their losses.

Another type of insurance identity theft is committed against life insurance companies. The fraudster assumes the identity of the beneficiary of a life insurance policy owned by the victim. The fraudster files a fraudulent death certificate with the insurance company along with obituaries from the Internet to document the victim's death. The insurance company pays the beneficiary the proceeds of the policy. Victims don't find out until they see their own death reported on a credit report, or until they are arrested for using the credit cards of a "deceased" individual. This type of fraud scheme usually involves an employee of the insurance company.

¶605 Child Identity Theft

Child identity theft occurs when the fraudster steals the identity of a person under legal age. The most common type of identity theft affecting children is the use of a child's identity to obtain loans and credit cards. Surprisingly, family members who mismanaged their own credit are usually the perpetrators in the theft of a child's identity. Often, a child doesn't find out about his or her identity being stolen until he or she applies for student loans or attempts to get a job.

In one case the fraud was exposed when the child was ready to go to college. She filled out her Free Application for Federal Student Aid (FAFSA) information and was denied her scholarship and student loans because of charged-off accounts on her credit report. While investigating the fraud, it became apparent that the person who stole her identity was her aunt. She was able to obtain the child's Social Security number from her mother by telling her she wanted to buy a U.S. Savings Bond for the child, who was 12 at the time, and that the bank required the child's Social Security number to record it on the bond.

The general public has several misconceptions about the difficulty of committing child identity theft. People often assume that creditors verify the date of birth and/or age of credit applicants. Usually, this information is taken at face value based on what was entered on the credit application. Another misconception is that the credit reporting agency will know that the Social Security number belongs to a minor. Unfortunately, the birth date in the credit bureau's file becomes official when the first request for a credit report is sent to the credit bureau.

¶606 Professional Identity Theft

Professional identity theft occurs when the fraudster steals the professional identity of another person. Because professional licenses and license numbers

are a matter of public record, it is relatively easy to commit this type of identity theft. An example is a fraudster who cannot obtain a PTIN to file tax returns assuming the identity of a CPA and preparing fraudulent tax returns using the PTIN obtained with the CPA's license number. Another common type of professional identity fraud is known as "notario fraud." This type of professional identity fraud occurs when an individual uses the identity of a real attorney, to pose as an attorney and collect fees from victims under the guise of assisting them with immigration issues. Physicians are a prime target for professional identity theft because the criminals want to use physicians' prescribing power to obtain prescription drugs for illegal use or to sell on the street. We have seen individuals steal professional licensing information to pose as nurses, law enforcement officers, teachers, day care workers, etc. In some of the worst cases, pedophiles steal the identities of teachers so they can get hired to work in schools with young children.

¶607 Business Identity Theft

With business identity theft, the fraudsters use the business name to obtain loans or credit. Often, they send out invoices in the name of the business or skim checks and deposit them into an account they control in the business name. Fraudsters who commit business identity theft are usually insiders, current or former employees with access to the business' financial information. Another type of business identity theft is to spoof a website for a real business in order to get customers to enter their credit card information for purchases. The victims never receive the products but find out that their credit cards were charged to the limit within hours of their supplying their information on the website.

Knowledge Check Question

13. A situation in which a fraudster uses the professional license of another person is considered:
- a. Business identity theft
 - b. Financial identity theft
 - c. Professional identity theft
 - d. Employment identity theft

¶700 Tax Frauds

There are numerous types of tax frauds available to criminals willing to break the law. Some of the more common types include income tax fraud, sales and use tax fraud, excise tax fraud, payroll tax fraud, property tax fraud, and estate and gift tax fraud.

Income tax fraud is unfortunately fairly common. It is usually done in conjunction with financial statement fraud. When most people first think of financial statement fraud, they think of large companies like Enron and WorldCom, and individuals like Bernie Madoff, who cooked the books to increase revenue and/or decrease expenses to make the company look more profitable and drive up the stock price. It should be noted that the vast number of financial statement frauds in the United States work in the opposite direction. Small and midsized businesses reduce revenue and inflate expenses in order to make the company look less profitable, thereby reducing the tax burden on the business owners. This is particularly common for sole proprietorships and pass-through entities. The ultimate goal is to reduce the income and sales taxes paid by the owners to allow them to keep more money in their pockets. Business owners do this by skimming revenue out of the business. They might even offer customers discounts for paying in cash so they don't have to record the transaction on the books or deposit the funds in a bank, which leaves a paper trail. Business owners can also record personal expenses as business expenses to reduce the taxable income of the business. The new big-screen TV for the house is recorded as a computer monitor for the business, or the family vacation is recorded as a business trip.

Not recording sales in the accounting system also allows the business owner to avoid paying sales and use taxes on those transactions. Business owners can also misuse their sales tax exemption certificates, which allow the business to avoid paying sales taxes on items the business purchases for resale in the business, to make personal purchases. The most common place I have seen this done is in restaurants, where the owners purchase the family groceries at a restaurant supply store and use the business's sales tax exemption certificate to avoid paying sales taxes on those purchases. Many businesses make purchases on the Internet or from out of state and fail to report and pay the use taxes on those transactions. The recent *Wayfair* decision by the Supreme Court that overturned the previous *Quill* decision will probably make it harder to avoid paying sales and use taxes on Internet and out-of-state purchases.

Business owners have been known to borrow money from payroll withholdings, including an employee's payroll tax withholdings, 401(4) withholdings, or other items withheld from the employee's paycheck. These monies are often used to fund operations or to pay the owners. Businesses sometimes misclassify employees as independent contractors in order to avoid paying the business's half of the employees' payroll taxes.

Additionally, failure to report tips, or to under-report tips, is another type of tax fraud. Employees believe it is harmless and that they have a low chance of getting caught. Historically that may have been correct, but with data analytics software, it is possible to compare tips by employee, that were paid by credit card or check, to transactions paid in cash. If there is a material discrepancy, the taxing authority can access taxes on those tips as under-reported income. The IRS can also assess the business for failure to collect and remit payroll taxes on the tips.

¶701 Tax Refund Identity Fraud

Tax refund identity fraud, which is also known as stolen identity refund fraud, occurs when a criminal uses an individual's personal information to submit fraudulent information to the Internal Revenue Service (IRS). There are multiple ways this can be done. The most common type of tax return refund fraud involves obtaining the victim's name, address, and Social Security number and filing fraudulent tax returns in order to receive refunds from the IRS. The income and other information submitted with the return is usually made up by the criminals in order to maximize the refunds they receive, including the earned income tax credit (EITC) and other refundable credits. Usually, the victims find out about this type of identity theft when they go to file their tax returns and the IRS kicks them back saying they already filed a return that year.

Another type of identity fraud involving taxes is when the criminal uses the victim's information to obtain employment. Usually, the fraudster is in the country illegally and cannot obtain employment using their own information. The employers submit W-2s and 1099s to the IRS for the money paid to employees and independent contractors and, of course, the victims do not report this on their returns. Usually, the victims find out they are a victim of this type of tax fraud when they receive an audit letter from the IRS indicating they failed to include income on their tax returns.

Knowledge Check Question

14. Which of the following types of identity theft usually involves tax refunds?
- a. Stolen identity refund fraud
 - b. Medical identity theft
 - c. Government benefits fraud
 - d. Identity cloning

¶800 Other Frauds

¶801 Unemployment Fraud

Many businesses don't consider unemployment fraud to be a major issue. This is because the government makes the unemployment payments to the terminated employees. There is, however, a cost to the business in increased FUTA and SUTA payments. Unemployment fraud occurs when employees receive payments they are not entitled to. A common scheme is for an employee who is collecting unemployment to continue to file for and collect unemployment benefits after they have started a new job. This is especially common for individuals who decide to take a shot at self-employment. Other unemployment frauds include falsifying the reason for termination. An employee who was fired for cause or who quit claims they were laid off or terminated through no fault of their own in order to collect unemployment checks. Misstating benefit year earnings can also be done in order to increase the amount received in unemployment benefits. This can just as easily work the other way with an employer laying off an employee and then claiming they quit in order to avoid the unemployment claims. Employers have also under-reported base year earnings for terminated employees in order to reduce their premium costs.

¶802 Worker's Compensation Fraud

Worker's compensation fraud is a major issue for businesses in the United States. The National Insurance Crime Bureau estimates the costs of worker's compensation fraud in the United States to be approximately \$7.2 billion per year.¹ Many workers have been caught exaggerating or faking injuries in order to collect worker's compensation benefits. Workers who were in too much pain to spend eight hours at work have been videoed playing sports, running marathons, and riding jet skis. One worker who was in so much pain he couldn't get out of bed was recorded carrying 100-pound rolls of tar paper up a ladder to the roof of his house that he was repairing while receiving worker's compensation benefits. Even companies that have good safety records can be victims of worker's compensation fraud. The cost to

¹ <http://quickbooks.intuit.com/r/trends-stats/fraud-statistics-every-business-should-know/>

companies is indirect as a result of higher insurance premiums, but one company in southern California was able to reduce its worker's compensation insurance premiums by \$1.3 million a year by investigating and putting a stop to this type of insurance fraud.

¶803 Charity Frauds

Fraudsters set up fake websites for nonexistent charities and then spam for victims. Stories of victims of the California wildfires, Hurricane Katrina, and other natural disasters are posted on the website to get people to donate to help the victims. Once the money is received, the fraudsters take the money and none of it ever gets to the victims of the national disaster.

¶804 Lottery or Contest Frauds

Lottery frauds are perpetrated by sending the victim an e-mail, which is usually spam or spoofed, informing the victim that he or she has won a large sum of money in a lottery. The victim is told that the lottery commission needs personal information to verify the funds are being sent to the correct winner. Usually, the fraudsters will also indicate that tax payments are due on the winnings and the personal information is needed to complete the appropriate tax forms. Once the victim provides personal information, his or her identity is stolen and used by the fraudsters. Should the victim provide bank account information, so that the winnings could be sent to the victim, the victim will find that the fraudsters have cleaned out the his or her bank account.

¶805 Corporate Prize Scam

The corporate prize scam works similarly to the lottery scam, with the prize coming from a corporation or source other than a lottery. Often, fraudsters will claim that the victim's e-mail address was selected to receive a prize and will ask for the victim's personal information to verify the identity of the winner, or to complete tax forms on the prize won. A common corporate prize scam involves telling the victim Bill Gates set up a prize pool and Microsoft is giving money away. Another one in 2017 indicated Steve Jobs wanted to give away his fortune from Apple. Sometimes it's amazing what people will believe. One victim was told she was the winner of the worldwide e-mail lottery and that her e-mail had been picked out of all of the e-mails in the world to win the grand prize.

¶806 Fake Dating Profiles

In one version of this type of fraud, the criminals prey on lonely individuals posing as “supermodel” potential boyfriends or girlfriends from outside the United States. They then ask for money to help them clear passport issues in their home country, so they can come to America and marry the “love of their life.” Often, the photos posted on the Internet dating website bear no resemblance to the person with whom the victim is communicating. In another version of this scheme, the fraudster indicates that he or she is starting a business and asks the victim to buy items and have them shipped to the victim’s home with subsequent forwarding to the fraudster. The fraudster explains that the items cannot be shipped to his or her company commercially. Once the victim agrees, the fraudster then uses stolen credit cards (from other victims) to purchase items that are shipped to the victim’s home. The victim usually finds out they have been victimized when the police show up at their home with a warrant to search for items purchased with stolen credit cards.

Online dating profiles are also used to gather information about individuals in order to commit identity theft. The criminals will claim they want to get to know you, so they want to exchange personal information, such as your mother’s maiden name, your high school mascot, your father’s middle name, where you attended grade school, etc. This information can then be used to answer typical security questions at financial institutions (and other websites) to verify your identity if you have forgotten your password. The fraudsters freely provide answers on themselves for the same questions, but of course, their answers are all pure fiction.

¶807 Government Documents Fraud

In this type of identity theft, the fraudster obtains government documents such as a driver’s license, Medicare card, Social Security card, or other document. The documents will have the name of the victim, but usually have the fraudster’s photo. These documents are then used to obtain employment or government benefits.

¶808 Employment Fraud

In this type of fraud, the fraudster uses the name and Social Security number of the victim to obtain employment. This is often done because the perpetrator of the fraud is in the country illegally and needs legitimate documentation to obtain employment. In 1986, Congress enacted the Immigration Reform and Control Act of 1986. The act prohibits employers from hiring individuals who are in the country illegally and requires that employers verify individuals’

identity and eligibility to work in the United States prior to presenting an employment offer.²

¶809 Resume Fraud

Fraudsters are able to get away with resume fraud because many organizations do not do a thorough background check on new hires. Fraudsters who are committing resume fraud list unearned college degrees and professional certifications on their resume to make them look better to the prospective employer. They might also list exaggerated titles or positions they never held. I asked one individual I caught doing this why he did it, and he replied, “Nobody would be willing to pay me what I want to make if I told the truth.”

¶810 Fraudulent Recruiter Scam

Fraudsters retrieve the victim’s contact information from his or her online resume and send e-mails posing as recruiters. The victim receives an e-mail of usually one to three paragraphs explaining how the recruiter found the victim’s resume on the Internet and that he or she would be a perfect fit for several high-paying jobs the recruiter has available with large national or international companies. The message is usually signed by an individual with an impressive title, such as Vice-President of Global Recruiting or Senior Vice-President of National Recruiting. The e-mail contains a link to the recruiter’s website, and this is the only method in the e-mail for contacting the recruiter. When the victim clicks on the link and goes to the site, the website attempts to download malicious software (spyware, Trojans, and/or bots) onto the victim’s computer. Once on the site, the victim is presented with an application to complete that requests personal information such as date of birth, Social Security number, driver’s license number, and mother’s maiden name. This information is used to steal the victim’s identity.

¶811 Fraudulent Employment Scam

The fraudsters get the victim’s name and contact information from the posted resume and e-mails what appears to be a legitimate offer of employment. The e-mail is usually sent from “the HR Department” and usually does not contain a company name. The e-mail usually discusses a good salary and benefits package without specifying a position. The e-mail will indicate that a formal offer can only be made once the paperwork is filled out and the right to work

2 Harper, J. (2012). Internal enforcement, e-verify, and the road to a national ID. *CATO Journal*, 32(1), 125–137.

in the United States has been verified. The fraudster attaches a link to a W-4 and I-9 form, and sometimes a benefit form requesting names and Social Security numbers of the victim's spouse and dependents, to the e-mail asking the victim to complete the forms online. The government forms provide a sense of legitimacy, so the victim completes and returns the forms. The forms provide the fraudster with the information necessary to steal the victim's identity.

¶812 Internet Auction and Fake Retail Schemes

Fraudsters place items up for auction that do not exist, and once the victim pays for the item, he or she never receives the purchase. Also, when victims will not pay in advance, the fraudsters use stolen credit cards to purchase the items from a legitimate store and ship the stolen items to the victim who now pays.

A variant of this fraud scheme is used to scam people attempting to sell a used car by themselves by placing an ad for the car on the Internet or in a local paper. The criminals show up, usually on the weekend, with a fake cashier's check for the full asking price for the car. They give the victim the fake check and transfer the title to the car. By the time the victim finds out the check bounced and is worthless, the criminals have transferred the title to the car multiple times and finally to a third-party buyer who was unaware of the fraud. Since the current owner is was unaware of the fraud, the victim can't repossess the car but must instead sue the person who gave them the bad check to recover their losses.

¶813 Long-Lost Relative

In this scam, the fraudsters pose as a barrister from England or another country and claim the victim is the sole surviving relative of their deceased client. They will tell the victim that he or she is inheriting a large sum of money as the only surviving heir of a rich relative. Usually the claim that follows is that the estate taxes need to be paid before the victim can receive his or her large inheritance. Once the victim sends money or bank account information, the victim's funds are promptly stolen from the account.

¶900 Government-Specific Frauds

¶901 Medicare Fraud

The National Health Care Anti-Fraud Association estimates healthcare fraud costs the U.S. government between \$68 billion and \$230 billion per year. In 2015, the Department of Justice filed claims under the Federal False Claims Act and recovered \$1.9 billion that was fraudulently billed to Medicare and Medicaid.¹ Billing fraud occurs when doctors and other medical providers bill for services that were not performed. In June 2015, the Medicare Fraud Strike Force teams arrested 240 doctors, nurses, and other medical professionals, charging them with billing \$712 million for unnecessary services and for services never performed.²

One large Medicare fraud involved the scooters that the elderly and disabled use for mobility. Hoveround billed Medicare over \$27 million for these mobility devices. Many of them were never used. An audit of 200 recipients of Medicare-provided scooters determined that 154 individuals who received the chairs were not eligible for the chairs they received. Some scooter companies were enlisting seniors and paying them a kickback to use their Medicare cards.

¶902 Social Security Fraud

In March 2015, the Inspector General reported there were 6.5 million people in the United States getting Social Security who are over 112 years old.³ The inspector general's report said that between 2006 and 2011, individuals using nearly 67,000 Social Security numbers generated \$3.1 billion in tips, wages, and self-employment income. Yet the employees' or self-employed individuals' names didn't match the Social Security number account-holders' names. In one case, an individual opened bank accounts using Social Security numbers for individuals born in 1869 and 1893. The Social Security's official database of active numbers indicated that both beneficiaries were alive—meaning they would be older than 145 and 121 years, respectively.

1 <http://www.bcbsm.com/health-care-fraud/fraud-statistics.html>

2 <https://oig.hhs.gov/fraud/strike-force/>

3 <http://www.thefiscaltimes.com/2015/10/27/Here-s-New-Plan-Crack-Down-Social-Security-Fraud>

¶1000 Not-for-Profit Specific Frauds

¶1001 Netting

As its name implies, netting involves reporting as contribution income the net amount left after conducting a special fundraising event. For example, if an organization incurs \$70,000 of costs in running a special event that brings in \$190,000, the organization limits its financial reporting to the \$120,000 net proceeds—in essence showing \$120,000 of contribution income with no offsetting costs. U.S. accounting rules were clarified in the 1990s to drastically limit the instances in which this practice is acceptable (SFAS Nos. 116 and 117). However, some organizations continue to do it rather than reporting the total amount received as income and the costs of the event as fundraising and management and general costs, as would normally be required. Netting results in lower than actual fundraising and management and general costs, which artificially inflates the program expense ratio.¹

¶1002 Overstating the Value of Non-Cash Gifts

Many charities receive non-cash contributions in the form of food, clothing, equipment, supplies, vehicles, and other assets. Additional non-cash contributions may include rent-free use of land or buildings and volunteer time. U.S. GAAP requires that most of these contributions be recorded at fair market value (although certain types of contributed services are not to be recorded at all). In most cases, this means recording income and expense in equal amounts, based on the fair value of the contributed goods or services. Most of the expenses are classified as program expenses since the donated items or services are used in carrying out program activities. As a result, inflating the fair market values of such contributions distorts the program expense ratio.²

1 Zack, G. 2004. Identifying and Investigating Financial Reporting Fraud of Non-Profit Entities. Presented at the ACFE's 15th Annual Fraud Conference, Las Vegas, NV; July 2004.

2 Zack, G. 2004. Identifying and Investigating Financial Reporting Fraud of Non-Profit Entities. Presented at the ACFE's 15th Annual Fraud Conference, Las Vegas, NV; July 2004.

¶1100 Money Laundering

Money laundering often coexists with fraud and other criminal activities because criminals need to launder their illegally obtained funds to make them look legitimate. “A definition of money laundering that covers both legal and illegal contexts is to take money that comes from one source, hide that source, and make the funds available in another setting so that the funds can be used without incurring legal restrictions or penalties.”¹ Usually, the public associates money laundering with drug lords and prostitutes, professions that have traditionally relied on laundered funds. Recently, money laundering has received a significant amount of press for the use of laundered funds to sponsor and fund terrorist activities. One of the main uses of money laundering is to avoid paying taxes on income; and since governments rely on tax income to support their operations, they have a vested interest in preventing money laundering. Recently, we have seen an increase in another use of money laundering, the conversion of funds provided by government grants, which are reserved for specific uses, to general purpose funds of the recipient organization or individual. Also, government officials who accept bribes (e.g., an Illinois governor who wanted to personally gain from appointing a person to fill a vacant Senate seat), need to launder the funds before they can be spent.

The U.S. Treasury Department estimates that there are \$300 billion in illicit funds being laundered on an annual basis.² A majority of the illegal funds being generated are from drug trafficking and fraud. The three basic steps for laundering money are:

1. Placement
2. Layering
3. Integration

Placement is the initial deposit of the funds into an account at a financial institution. Layering is moving the funds through various businesses entities, such as trusts, LLCs, not-for-profits, and corporations, and often through

1 Crumbley, D. Larry; Heitger, Lester, Smith, G. Stevenson, *Forensic and Investigative Accounting*, 2nd ed., 2005, Chicago, CCH Incorporated.

2 <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>

multiple countries to hide the origins of the funds. Integration is moving the funds into a legitimate account controlled by the money launderer to make the funds appear legitimate.

To help combat money laundering, the Department of the Treasury requires banks and financial institutions to file a Currency Transaction Report (CTR) when they receive or disburse cash in excess of \$10,000 in one or more related transactions in a year. Money service businesses are also required to file a Suspicious Activity Report (SAR), and according to the Internal Revenue Service, "There are two different dollar thresholds that require a SAR. They depend on the stage of discovery and the type of transaction involved. A \$2,000 threshold applies if a customer is conducting or attempting to conduct a transaction(s) that aggregates to \$2,000 or more. A threshold of \$5,000 applies for transactions identified by issuers of money orders or traveler's checks from a review of clearance records. These thresholds are known as the \$2,000 front door/\$5,000 back door rule. The \$2,000 front door transactions are face-to-face with the customer. The \$5,000 rule applies after the records have been processed at the issuer level, thus the back door."³ Additionally, the IRS requires taxpayers to file Form 8300 for all cash transactions in excess of \$10,000.

One tool of the trade for money launderers is correspondent banks. International banking is comprised of a network of correspondent and respondent banks that allow for the 24-hour transfer of cash to and from anywhere in the world. Each correspondent bank can have relationships with thousands of other banks around the globe, and large international banks can process over a trillion dollars in wire transfers a day. Correspondent banking takes place when one bank provides services to another bank to transfer funds, exchange currencies, and access investment services such as money market accounts, overnight investment accounts, trading accounts, certificates of deposit, and their computer software for making wire transfers and instant updates on customer account balances. Another service provided by foreign respondent banks to their clients through these correspondent-banking relationships is a payable-through account. Such an account enables the respondent bank's clients within the country where the bank is registered to write checks that are drawn directly on the respondent bank's correspondent account in the United States, thus disguising the source of the funds.

Shell banks are usually high-risk banks that exist without any physical presence in any legal jurisdiction. Often shell banks only exist on the Internet. Shell banks will have a legal banking license in a specific country, but they are unlikely to have staff and may be operated as part of another business or operated out of an individual's personal residence. Shell banks are not subjected to

3 <http://www.irs.gov/businesses/small/article/0,,id=154555,00.html>

any scrutiny by local banking regulators in the country they are licensed in. Shell banks should not be considered to be a branch bank without a physical presence in the country.

Offshore banks are different than shell banks, although the characterization is not mutually exclusive. An offshore banking license prevents the bank from transacting banking activities with any citizens of the licensing country or transacting business using the local currency. Offshore banking operations solely exist to conduct international financial transactions.

Knowledge Check Question

15. Which of the following is one of the three steps of money laundering?
- a. Layering
 - b. Opportunity
 - c. Conversion
 - d. Rationalization

¶1200 Corruption

Corruption occurs when individuals use their position in their company, with a not-for-profit, or with a governmental entity for their own personal gain. Anyone in a position of power can be tempted to cross the line. As the saying goes, “Power corrupts, and absolute power corrupts absolutely.” Corruption involves unethical behavior by those in positions of power. It can be as simple as dishonesty or it can be an elaborate fraud scheme. The basic tenet of corruption is that the individual is doing it for personal gain. Corruption has been uncovered in politics, sports, academics, unions, governments, not-for-profits, and businesses. According to the ACFE 2018 Report, the average cost of a corruption scheme is around \$250,000. You are also more likely to find corruption in larger organizations, those with over 100 employees, than you are to find corruption in smaller organizations. However, you shouldn’t assume that small organizations are free from the risk of corruption. Instead, they just have a lower risk. Tips play a big role in discovering corruption, with tips resulting in the detection of 50 percent of all corruption schemes.

There are many forms of corruption. Petty corruption involves the exchange of small gifts or the use of personal property or connections in exchange for favors, or for speedy approvals from governments. Bribery is the paying or receiving of something of value (it doesn’t have to be money) in exchange for preferential treatment or special favors. Kickbacks and bid rigging are two examples of bribery. An illegal gratuity occurs when someone provides a gift, or something of value, after favorable actions have been completed. Unlike a bribe, an illegal gratuity isn’t usually arranged in advance of the action, and you don’t have to prove an intent to influence the person who received the gift.

Extortion and blackmail are other examples of corrupt behavior. This occurs when someone is threatened with actions, such as violence against themselves or their loved ones, or is threatened with the release or publication of information that could harm the person’s reputation. Basically, if you don’t want something bad to happen to you or someone you love, you better do as you are told.

Abuse of discretion occurs when an individual misuses their power or authority for personal gain; for example, a board member who favors a vendor owned by a friend and presses the company to select that vendor. Other

abuses of authority include favoritism, cronyism, and nepotism when people in positions of authority provide special treatment or favors to friends, associates, or family members.

One type of corruption that is often overlooked is an undisclosed conflict of interest. A conflict of interest impairs an individual's ability to make a fair and impartial decision. These conflicts usually result in the person acting to benefit themselves instead of meeting their fiduciary responsibilities to the organization or individuals they are representing.

Graft is the use of a political office, either an elected or appointed position, for personal gain. Taking a position on a political issue in exchange for campaign contributions is one example of graft. Accepting an all-expenses-paid vacation in exchange for voting a certain way is another example of graft.

Bid rigging is another type of corruption. Government entities and many large companies put projects and product requests out for bid. The contract is supposed to go to the company that provides the lowest price or bid while meeting the contract requirements. Bid rigging occurs when somebody at the purchasing organization provides information to one of the bidders to give them an inside track. This is done for personal gain, and kickbacks are usually involved. With the inside information, the criminals can adjust their bid to make sure they come in as the lowest bidder, usually just barely beating the next lowest bid.

For corruption to occur, someone has to have the power to make or influence a decision. They have to exercise that power to provide preferential treatment based on their relationship, or on receiving something of value, and there has to be a beneficiary of that preference.

Many people consider corruption to include a monetary payment, but money isn't the only thing that can be used to influence people. Debt forgiveness, loans, sexual favors, access to decision makers, keeping secrets, and the free or discounted use of assets are all examples of methods of payments used in corruption schemes.

¶1300 Fraud Wrap-Up

Once criminals commit fraud, they need to take steps to conceal the fraud in order to avoid being caught. The ACFE Report describes the top eight methods for concealing fraud as follows:

- 55 percent of the time fraudsters created fraudulent physical documents.
- 48 percent of the time fraudsters altered physical documents.
- 42 percent of the time fraudsters created fraudulent transactions in the accounting system.
- 34 percent of the time fraudsters altered transactions in the accounting system.
- 31 percent of the time fraudsters altered electronic documents or files.
- 30 percent of the time fraudsters destroyed physical documents.
- 29 percent of the time fraudsters created fraudulent documents or files.
- 27 percent of the time fraudsters created fraudulent journal entries.

Remember that multiple methods are used to conceal a fraud, because a criminal has to cover all of the bases to avoid being caught. Only 3 percent of the discovered fraud cases did not involve an attempt to conceal the crime.

The ACFE Report documented the primary ways fraud is detected in organizations. They include the following:

- 40 percent of the time fraud is detected with tips.
- 15 percent of the time fraud is detected by internal auditors.
- 13 percent of the time fraud is detected by management reviews.
- 7 percent of the time fraud is accidentally discovered.
- 6 percent of the time other detection methods discover fraud.
- 5 percent of the time fraud is detected by reconciling accounts.
- 4 percent of the time fraud is detected through documentation examinations.
- 4 percent of the time the external auditors detect fraud.
- 3 percent of the time fraud is detected through surveillance and monitoring.
- 2 percent of the time organizations are notified by law enforcement.
- 1 percent of the time IT controls detect fraud.
- 1 percent of the time the criminals confess.

Fraud is reported in the following ways:

- 53 percent of fraud reports come from employees
- 21 percent of fraud reports come from customers
- 14 percent of fraud reports are done anonymously
- 8 percent of the time fraud reports come from vendors
- 5 percent of the time fraud reports come from other sources
- 3 percent of the time fraud is reported by competitors
- 2 percent of the time fraud is discovered by shareholders or owners

Knowledge Check Question

- 16.** According to the 2018 ACFE Report, which of the following is the most common way to conceal a fraud?
- a. Creating fraudulent transactions in the accounting system
 - b. Creating fraudulent journal entries
 - c. Destroying physical documents
 - d. Creating fraudulent physical documents

Glossary of Terms

AAA: American Accounting Association.

ABV: Accredited in Business Valuation.

Accounting equation: Assets = liabilities + stockholder's equity.

Accounting: The process of documenting and recording company's business transactions.

Accounts payable: Amounts due to vendors for products and services received.

Accounts receivable: Amounts due from customers for products or services provided.

ACFE: Association of Certified Fraud Examiners.

ACFEI: American College of Forensic Examiners International.

Ad hoc: For a single or special purpose.

Advance fee fraud: Fraudulently obtaining a fee in advance for services that are never done.

AICPA: American Institute of Certified Public Accountants.

Amicus curiae: Also known as "Friend of the Court"; a third party who is not directly involved in the litigation or dispute is allowed to file a brief on behalf of one of the parties to the litigation.

Arbitration: In lieu of litigation the dispute is heard before a third party that renders a decision. Arbitrations can be binding or nonbinding.

Authentication: The process of making a written document admissible as evidence in a court of law.

Automated controls: Automated controls are controls that are built into the computer software. Automated controls can be either preventive or detective.

Backdoors: A backdoor is a route into a computer that circumvents the user authentication process and allows hackers open access to the system once it is installed.

Balance: Summarizes a company's assets, liabilities and shareholders' equity at a specific point in time.

Bank reconciliation: The process of matching the balances in an entity's accounting records for a cash account to the corresponding information on a bank statement.

Bankruptcy: A legal way to discharge or reorganize debt.

Best evidence rule: (also referred to as the *original writing rule*), to prove the contents of a writing, recording, or photograph, the original writing, recording, or photograph usually must be presented.

BitCoin: A type of virtual currency.

Bookkeeping: The process of recording all of the accounting information for a business.

Bribery: Illicit payments for information or actions paid to corrupt employees or officials.

Budget: A forecast of the financial results and financial position of a company for one or more future periods.

Business calculation: A business calculation is less extensive than a business valuation and uses an agreed upon methodology. Business calculations cannot be presented in court.

Bustout: A preplanned bankruptcy used to misappropriate assets from creditors.

CFE: Certified Fraud Examiner.

CFF: Certified in Financial Forensics.

CFIP: Certified Forensic Investigative Professional.

Chaffing: A method for sending hidden messages over the Internet.

Chain of custody: The process for verifying who had care, custody and control of evidence from the time it is collected until it is submitted to the court.

Chart of accounts: A list of all accounts used in a business.

Check tampering: Altering information on a check.

CIA: Certified Internal Auditor.

Circumstantial evidence: Indirect evidence from which the validity or truth of an issue can be derived.

Common costs: Costs that are not directly tied to making and selling a product or service.

Common law: Consists of the usages and customs of a society as interpreted by the courts, it is also referred to as case law.

Complaint: The plaintiff's formal written pleading filed with the court expressing a claim for relief and initiating court action.

Computer crime: An illegal act conducted using a computer or electronic device.

Computer forensics: Procedures applied to computers and electronic equipment to gather evidence that can be used in a court of law.

Computer virus: A computer virus is usually hidden in a computer program and performs functions such as copying or deleting data files. A computer virus creates copies of itself that it inserts in data files or other programs.

Computer worms: A type of malware that transmits itself over networks and the Internet to infect more computers with the malware.

Conflict of interest: Occurs when an employee, manager, or executive has an undisclosed economic or personal interest in a transaction that adversely affects that person's employer.

Control activities: Approvals, segregation of duties, reconciliations, reviews, procedures, etc. that ensure that processes are followed and that the opportunities for errors or fraud have been minimized.

Control environment: Often referred to as the "Tone at the Top," the ethical values of the organization and relies on the strength of corporate governance.

Control risk: The risk that a control does not prevent or detect a material misstatement in an account balance.

CPA: Certified Public Accountant.

Credit report: A report maintained by independent organizations containing information on an individual's credit history.

CrFA: Certified Forensic Accountant.

Cross-examination: Questioning of witnesses in court by the other party's attorney.

Current liabilities: Liabilities expected to be paid in cash- within 12 months or the accounting cycle of a business. The 12-month period is almost always used.

CVA: Certified Valuation Analyst.

Data breach: The release or taking of data from a secure source to an unsecured third-party location (computer).

Data mining: A process that uses mathematical algorithms to detect hidden patterns in data.

De facto: In fact; actually.

De jure: Lawful, in the law.

Debit entry: Accounting entries that are posted on the left side of a ledger.

Debt to equity ratio: Long-term debt/shareholders' equity. Indicates the amount of debt a company has, compared with equity.

Demonstrative evidence: Documents, photos, videos, charts, or other items that illustrate testimony but which possess no probative intrinsic value.

Deposition: Testimony given by a witness, under oath, but outside of the courtroom.

Detective controls: Policies and procedures that are put in place to help find errors or fraud that have already occurred. Detective controls are put in place so that corrections can be made.

Direct evidence: Evidence that directly proves a fact, without any need for presumption or conjecture.

Direct examination: The questioning of a witness by the attorney for which the witness is testifying.

Discovery: A pretrial process in which the parties to the litigation exchange information which will help them prepare for the trial.

Electronic data interchange (EDT): The exchange of electronic data between computers.

Electronic funds transfer (ETF): A transfer that is designed to move funds instantaneously between accounts.

Embezzlement: Theft of money or property by an employee or fiduciary from their employer.

Entity level controls: Internal controls designed to provide reasonable assurance that the entity's objectives are met. Entity level controls relate to the whole organization.

Expert report: A written report prepared by an expert witness on an issue before the court.

Expert witness: A person who, because of specialized training or experience, testifies in court to assist the judge or jurors understand complicated and technical subject matter.

Fact witness: A witness who testifies in court as to specific facts.

Financial statement fraud: Fraud designed to cook the books and present false information on the financial statements.

Firewall: Hardware or software designed to prevent malware from being installed on a computer and to prevent unauthorized access to a computer system.

Fixed assets: Assets that are used to generate revenue or operate the business. Fixed assets are generally held as long term assets and are not quickly converted into cash. Inventory is never considered a fixed asset.

Forensic: Pertaining to, connected with, or used in courts of law or public discussion and debate.

Fraud auditor: An accountant especially skilled in auditing who is generally engaged in auditing with a view toward fraud discovery, documentation, and prevention.

Fraud triangle: The theory developed by Dr. Donald Cressey explaining why individuals commit occupational fraud.

Fraud: A deception deliberately practiced in order to secure unfair or unlawful gain.

Ghost employee: A phantom employee that exists only on the books.

Habeas corpus: A writ asking the court to release a prisoner from unlawful imprisonment.

Hacker: Someone attempting to gain access to a computer for malicious or illegal purposes.

Hearsay: An out-of-court statement of an individual offered in court to prove the truth of the issue under litigation.

Horizontal analysis: A technique for analyzing the percentage change in individual financial statement items from one year to the next.

Identifying information: Information such as a name, phone number, address or Social Security number that can be used to identify an individual.

Identity theft: Broadly defined as the use of one person's identity or personally identifying information by another person without his or her permission. Identity theft is a type of fraud and can be committed against an individual or organization.

IIA: Institute of Internal Auditors.

IMA: Institute of Management Accountants.

Impairment: An other than temporary decline in value of an asset where the market value of the asset is lower than the book value of the asset.

Internal controls: A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Interrogation: The process of questioning an individual suspected to be involved in a crime.

Interrogatories: Questions that are submitted to an opposing party in a lawsuit.

Interview: The informal questioning of an individual.

Judicial precedent: Case law; using a prior court decision to settle a current case with the same or similar facts.

Jurisdiction: Authority of a court to hear a particular type of case.

Kickback: The giving or receiving anything of value to influence a business decision.

Larceny: Theft.

Litigation services: According to the AICPA, services that involve pending or potential formal legal or regulatory proceedings before a trier of fact in conjunction with the resolution of a dispute between two or more parties.

Litigation: Engaging in legal proceedings, a lawsuit.

MAFF: Master Analyst in Financial Forensics.

Mala prohibita: An act or omission that is by statute criminal regardless of intent (mens rea).

Malware: Software that is placed on computers or cell phones to hijack the computers, steal data, or encrypt the data for ransom.

Manual controls: Controls that are that are done by individuals. Manual controls can be either preventive or detective.

Means of identification: Any type of information that can identify a particular individual such as Social Security numbers, credit card numbers or the like.

Mediation: Process whereby an impartial third-person assists the parties in reaching a resolution of the dispute.

Mens rea: A person's state of mind; intent.

Misappropriation: Obtaining something of value, or avoiding an obligation by deception or false statements; a type of fraud.

Mitigate: To act to minimize damages.

Money laundering: Taking funds from an illegal source, hiding the source of funds, and making the funds available for use without legal restrictions or penalties.

Motion in limine: A motion requesting the court to exclude certain evidence from being presented at trial.

NACVA: National Association of Certified Valuation Analysts.

Net worth: The amount by which assets exceed liabilities.

Nolo contendere: A plea wherein the defendant agrees not to contest the charges, but does not admit to, or deny the charges.

Occupational fraud: Fraud occurring in the workplace or relating to employment.

Parol evidence: Oral evidence.

Pharming: A virus or malicious software is secretly loaded onto the victim's computer and hijacks the web browser.

Phishing: A technique used by fraudsters to obtain personal information for purposes of identity theft. This theft can include sending illegitimate emails asking for personal information.

Predication of fraud: Circumstances, when taken as a whole, will lead a reasonably prudent professional to believe a fraud is occurring, or has occurred, or will occur.

Preventive controls: Policies and procedures that are put in place to help prevent errors or fraud from occurring.

Pro se: Representing oneself in court.

Process level controls: Internal controls designed to provide reasonable assurance that the entity's processes are followed, applications are working, and transactions are properly completed and recorded. Process level controls relate to a single activity.

Pyramid scheme: A scheme in which a buyer or participant is promised a payment for each additional buyer or participant recruited by that person.

Qui tam suit: Litigation filed by a whistle-blower under the Federal False Claims Act against a contractor or company on behalf of the federal government.

Ratio analysis: A means of measuring the relationship between two different financial statement amounts.

Real evidence: Refers to physical objects which may be introduced as evidence at a legal proceeding.

Residuum rule: The rule is that no finding may be supported solely by hearsay evidence.

Risk assessment: An assessment conducted to determine where key controls need to be in the processes of the organization. Controls should be put in place in high risk areas, but it is necessary to consider the cost/benefit of each control because excessive controls can reduce an organizations efficiency.

Rootkits: Software that modifies the operating system to hide malware from the computer users. Some rootkits contain code that prevents the malware from being removed from the computer.

Rules of evidence: The rules governing the admissibility of evidence in court.

Shell companies: Legal business entities created for the purpose of committing fraud. There is no actual business, just the paperwork.

Skimming: Removal of cash from a victim entity prior to its entry in an accounting system.

Spoofing: Term used to describe fraudulent e-mail activity in which the sender's address or other parts of the e-mail header are altered to appear as though the e-mail originated from a different source.

Subpoena duces tecum: A court order to produce specified documents, or other items for the court.

Subpoena: A court order requiring a witness to appear at a specified time and place in order to testify.

Trojan horse: A malware program that is disguised as something else. Users assume it is a beneficial program when in fact it is not. Trojan horses are often used to insert spyware onto computers.

Venue: The place where the court has jurisdiction and will hear the case.

Vertical analysis: A technique for analyzing the relationships between the items on an income statement, balance sheet, or statement of cash flows by expressing components as percentages.

Virtual currency: A currency that only exists in cyber space. There is no physical or tangible item to represent the currency.

Whistleblower: An employee who reports illegal or unethical conduct of the employer.

Answers to Knowledge Check Questions

1. **a. *Incorrect.*** Gabriel Tarde developed the Theory of Differential Association.
b. *Correct.* Ronald Akers developed the Social Learning Theory. The social learning theory postulates that individuals learn criminal activity and rationalize the acceptability of criminal activities based on their social networks.
c. *Incorrect.* Edwin Sutherland developed the Theory of Differential Association.
d. *Incorrect.* Donald Cressey developed the Fraud Triangle Theory.

2. **a. *Incorrect.*** Cash larceny is stealing cash that has been recorded in the accounting system from a register, a deposit, or the safe.
b. *Incorrect.* Kiting is done with checks, not with cash. It involves taking advantage of the float to make use of non-existent funds in a checking or other bank account.
c. *Correct.* Skimming is taking the cash before it is recorded in the accounting system. This is a common fraud when employees are working alone, in drive-through retail outlets, and at fundraising events for not-for-profit organizations.
d. *Incorrect.* Cash drawer loans involve employees putting personal NSF checks in their cash drawer in exchange for cash.

3. **a. *Incorrect.*** The security thread in a \$5 bill glows blue under a black light.
b. *Correct.* The security thread in a \$20 bill is green when viewed with a black light.
c. *Incorrect.* A black light will show a yellow security thread in a \$50 bill.
d. *Incorrect.* Pink is the color of a security thread in a \$100 bill.

4. **a. *Incorrect.*** Duplicate invoice fraud involves sending multiple invoices hoping to get paid more than once.
b. *Incorrect.* Receivables dumping occurs when employees assign collectable accounts to a collection for a kickback or other compensation.
c. *Correct.* Reaging occurs when new accounts receivable are created to pay aged receivables to make the receivables look current. This can be done multiple times to make the accounts receivable aging report show only current, and few past due, invoices.
d. *Incorrect.* Skimming involves taking payments before they are recorded in the accounting system.

5. **a. Correct.** Bill and hold frauds involve billing for goods without receiving an order or shipping anything. If the customer pays the invoice, the company sends the goods; otherwise, the invoice is reversed or written off. Sometimes the receivable is offset with a credit memo to avoid a direct write-off.

b. Incorrect. An improper cut-off fraud involves posting transactions in the wrong period.

c. Incorrect. Fake sales are entered into the accounting system, but invoices are not sent.

d. Incorrect. Channel stuffing occurs when a business ships more merchandise to a distributor than it can sell, with a promise to buy back unsold items, while recording the entire sale as revenue.

6. **a. Incorrect.** Expensing items and then selling them on the Internet is a way that employees commit expense reimbursement fraud.

b. Incorrect. Purchasing and canceling extended warranties is a way that employees commit expense reimbursement fraud

c. Correct. Entertaining customers is not fraud. Instead, an example of a way an employee commits expense reimbursement fraud is to expense items and then sell them on the Internet.

d. Incorrect. Shell companies are a way that employees commit expense reimbursement fraud

7. **a. Incorrect.** A bill and hold scheme is a revenue scheme, not a type of inventory fraud.

b. Incorrect. Lapping is an accounts receivable fraud, not a type of inventory fraud.

c. Incorrect. Cooking the books is financial statement fraud, not a specific type of inventory fraud.

d. Correct. Short shipping is a type of inventory fraud. This fraud can be conducted by either management or employees.

8. **a. Incorrect.** This is an example of skimming, not a data breach.

b. Incorrect. This is an example of shoulder surfing, which is not a data breach.

c. Correct. Stealing information from a computer is an example of a data breach.

d. Incorrect. This is an example of criminal identity theft, not a data breach

9. **a. Incorrect.** A data breach involves obtaining confidential information from a computer system.

b. Correct. Credential stuffing involves using stolen user IDs and passwords to try to access multiple IT systems.

c. Incorrect. Ransomware encrypts data on a system.

d. Incorrect. Phishing is done with email. Social networking through phishing schemes is a common way to get around an organization's IT security.

10. **a. Incorrect.** Phishing uses email to obtain personal information or to get you to download malware by clicking on a link.

b. Correct. Ransomware encrypts the information on your computer. The criminals then require that the victim pay a ransom in order to obtain the decryption key and have access to their files.

c. Incorrect. Spoofing hides the true origin of an email or website to make it look legitimate.

d. Incorrect. Spyware tracks your information; it doesn't encrypt it.

11. **a. Incorrect.** There are 407 million credit cards issued in the United States, not worldwide.

b. Incorrect. There are more than a billion credit cards issued worldwide.

c. Correct. There are approximately 1.5 billion credit cards issued worldwide.

d. Incorrect. There are 1.9 billion debit cards issued worldwide, versus 1.5 billion credit cards.

12. **a. Incorrect.** Cash drawer loans involve postdated checks from an employee's bank account.

b. Incorrect. Skimming is taking funds before they are entered into the cash register or accounting system.

c. Correct. Criminal identity theft involves opening bank accounts using false information. The typical pattern for criminal identity theft is for the criminal to first misappropriate your Social Security number and personal information. There are various ways to do this, including data breaches, mail fraud, phishing, vishing, etc.

d. Incorrect. Refund frauds are committed by entering false returns into the cash register.

13. a. *Incorrect.* During a typical business identity theft scheme, the fraudsters use the business name to obtain loans or credit.

b. *Incorrect.* During a typical financial identity theft scheme, the fraudsters use the personal information to obtain financial benefits.

c. *Correct.* The fraudulent use of a professional license is considered professional identity theft. Physicians are a prime target for professional identity theft because the criminals want to use physicians' prescribing power obtain prescription drugs for illegal use or to sell on the street.

d. *Incorrect.* During a typical employment fraud scheme, the fraudster uses the name and Social Security number of the victim to obtain employment.

14. a. *Correct.* Stolen identity refund fraud involves filing false returns to receive tax refunds.

b. *Incorrect.* Medical identity theft involves assuming someone's identity to obtain health care.

c. *Incorrect.* Government benefits fraud involves using someone else's identity to receive government benefits.

d. *Incorrect.* Identity cloning involves concealing a fraudster's true identity by cloning a victim's identity and using it openly in plain sight.

15. a. *Correct.* Layering is one of the three steps of money laundering.

b. *Incorrect.* Opportunity is part of the fraud triangle, not one of the three steps of money laundering.

c. *Incorrect.* Conversion is an element of fraud, not one of the three steps of money laundering.

d. *Incorrect.* Rationalization is part of the fraud triangle, not one of the three steps of money laundering.

16. a. *Incorrect.* Creating fraudulent transactions in the accounting system occurs 42 percent of the time versus 55 percent of the time for creating fraudulent physical documents.

b. *Incorrect.* Creating fraudulent journal entries is the least likely way to conceal a fraud.

c. *Incorrect.* Destroying physical documents to conceal a fraud occurs 30 percent of the time versus 55 percent of the time for creating fraudulent physical documents.

d. *Correct.* Fifty-five percent of the time, fraudsters create fraudulent physical documents to conceal a fraud.

Index

(References are to paragraph numbers.)

- Accounts payable fraud ... 305
- Accounts receivable fraud ... 306
- Advance fee scams ... 507
- American Institute of Certified Public Accountants (AICPA) ... 204
- Asset misappropriations ... 304
- Association of Certified Fraud Examiners (ACFE) ... 100, 206, 300, 301, 305, 307, 308, 312, 1200, 1300
- Auction, Internet ... 812
- Backdoor ... 410
- Bankruptcy fraud ... 508
- Bid rigging ... 1200
- Blackmail ... 1200
- Brand hacking ... 406
- Business identity theft ... 607
- Charity fraud ... 803
- Checks
 - Accounts payable fraud ... 305
 - Accounts receivable fraud ... 306
 - Business identity theft ... 607
 - Criminal identity theft ... 601
 - Double-cashed ... 311
 - Skimming ... 301
- Child identity theft ... 605
- Committee of Sponsoring Organizations (COSO) ... 201
- Conflict of interest ... 308, 1200
- Corporate prize scam ... 805
- Corruption ... 1200
- Counterfeit currency ... 303
- Credential stuffing ... 402
- Credit card fraud ... 501
 - Obtaining credit card information ... 503
- Cressey, Donald ... 203, 204
- Criminal identity theft ... 601
- Currency Transaction Report (CTR) ... 1100
- Cybercrime ... 400
- Cyber fraud ... 400
 - Brand hacking ... 406
 - Credential stuffing ... 402
 - Data breaches ... 401
 - Denial of service (DoS) attacks ... 408
 - Hacking ... 410
 - Pharming ... 409
 - Phishing ... 404
 - Ransomware ... 403
 - Spoofing ... 407
 - Vishing ... 405
- Data breaches ... 401
- Dating profiles, fake ... 806
- Debit card fraud ... 501
- Denial of service (DoS) attacks ... 408
- Double-cashed checks ... 311
- Elements of fraud ... 205
- Employment fraud ... 808
 - Fraudulent employment scam ... 811
 - Fraudulent recruiter scam ... 810
- EMV card fraud ... 502
- Enron ... 310, 700
- Expense reimbursement fraud ... 308
- Extortion ... 1200
- Financial fraud ... 500
 - Advance fee scams ... 507
 - Bankruptcy fraud ... 508
 - Credit card fraud ... 501
 - Debit card fraud ... 501
 - EMV card present fraud ... 502
 - Investment fraud ... 504
 - Obtaining credit card information ... 503
 - Ponzi schemes ... 505
 - Pyramid schemes ... 506
- Financial statement fraud ... 310
- Fraud theories ... 200
 - Elements of fraud ... 205
 - Social learning theory ... 203
 - Theory of differential association ... 202
 - Theory of differential reinforcement ... 201
- Fraud triangle ... 204
- Fraudulent employment scam ... 811
- Fraudulent recruiter scam ... 810
- Government documents fraud ... 807
- Government-specific fraud ... 900
 - Medicare fraud ... 901
 - Social security fraud ... 902
- Graft ... 1200
- Hacking ... 410
- Identity theft ... 600
 - Business identity theft ... 607
 - Child identity theft ... 605
 - Criminal identity theft ... 601
- Definition of ... 600
 - Insurance identity theft ... 604
 - Medical identity theft ... 603
 - Professional identity theft ... 606
 - Sockpuppets ... 602
- Immigration Reform and Control Act of 1986 ... 808

- Insurance identity theft ... 604
- Internet auction schemes ... 812
- Inventory fraud ... 309
- Investment fraud ... 504
- Kickbacks ... 306, 308, 312, 1200
- Lapping ... 302
- Long-lost relative ... 813
- Lottery or contest fraud ... 804
- Madoff, Bernie ... 700
- Medical identity theft ... 603
- Medicaid fraud ... 901
- Medicare fraud ... 901
- Money laundering ... 1100
- National Health Care Anti-Fraud Association ... 901
- Netting ... 1001
- Non-cash gifts ... 1002
- Notario fraud ... 606
- Not-for-profit specific fraud ... 1000
 - Netting ... 1001
 - Non-cash gifts ... 1002
- Occupational fraud ... 300
 - Accounts payable fraud ... 305
 - Accounts receivable fraud ... 306
 - Asset misappropriations ... 304
 - Counterfeit currency ... 303
 - Double-cashed checks ... 311
 - Expense reimbursement fraud ... 308
 - Financial statement fraud ... 310
 - Inventory fraud ... 309
 - Lapping ... 302
 - Revenue fraud ... 307
 - Skimming ... 301
- Online dating profiles ... 806
- Payroll fraud ... 312
- Personal health information (PHI) ... 401
- Personally identifying information (PII) ... 401
- Pharming ... 409
- Phishing ... 404
- Ponzi schemes ... 505
- Predication of fraud ... 206
- Professional identity theft ... 606
- Public Company Accounting Oversight Board (PCAOB) ... 307
- Pyramid schemes ... 506
- Quill* decision ... 700
- Ransomware ... 403
 - CryptoLocker ... 403
 - Cryptowall 2.0 ... 403
- Recruiter scam ... 810
- Red Flags Rule ... 600
- Resume fraud ... 809
- Retail schemes ... 812
- Revenue fraud ... 307
- Sentry MBA ... 402
- Skimming ... 301
- Social learning theory ... 202, 203
- Social Security fraud ... 902
- Sockpuppets ... 602
- Spear phishing ... 404
- Spoofing ... 407
- Suspicious Activity Report (SAR) ... 1100
- Sutherland, Edwin ... 100, 202
- Tarde, Gabriel ... 201
- Tax fraud ... 700
 - Tax refund identity fraud ... 701
- Theory of differential association ... 202
- Theory of differential reinforcement ... 201
- Trojan ... 410
- Unemployment fraud ... 801
- U.S. GAAP ... 307, 1002
- Vishing ... 405
- Wayfair* decision ... 700
- White-collar crime ... 100
- Worker's compensation fraud ... 802
- WorldCom ... 310, 700

Final Exam Instructions

To complete your Final Exam go to **cchcpelink.com/printcpe**, click on the title of the exam you wish to complete and add it to your shopping cart (you will need to register with CCH CPELink if you have not already). Click **Proceed to Checkout** and enter your credit card information. Click **Place Order** to complete your purchase of the final exam. The final exam will be available in **My Dashboard** under **My Account**.

There is a grading fee for the Final Exam submission.

Online Processing Fee: **\$75.95**

Recommended CPE: **4 hours**

Instructions for purchasing your CPE Tests and accessing them after purchase are provided on the **cchcpelink.com/printcpe** website. **Please note, manual grading is no longer available. All answer sheets must be submitted online for grading and processing.**

Recommended CPE credit is based on a 50-minute hour. Because CPE requirements vary from state to state and among different licensing agencies, please contact your CPE governing body for information on your CPE requirements and the applicability of a particular course for your requirements.

Expiration Date: December 31, 2019

Evaluation: To help us provide you with the best possible products, please take a moment to fill out the course Evaluation located after your Final Exam.



Wolters Kluwer, CCH is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses of CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.learningmarket.org.

Additional copies of this course may be downloaded from **cchcpelink.com/printcpe**.

Final Exam

1. Which of the following types of cyber fraud is used to hide the origin of an email?
 - a. Phishing
 - b. Pharming
 - c. Whaling
 - d. Spoofing
2. Which of the following identifies the most common way to pay for stolen credit card numbers purchased over the Internet?
 - a. Cash
 - b. BitCoin
 - c. Credit card
 - d. Check
3. Bid rigging normally falls under which type of corruption?
 - a. Conflicts of interest
 - b. Bribery
 - c. Illegal gratuities
 - d. Economic extortion
4. Which of the following types of corruption primarily involves the misuse of political office?
 - a. Nepotism
 - b. Graft
 - c. Bribery
 - d. Illegal gratuities
5. Which of the following types of corruption payment is most likely to be associated with economic extortion?
 - a. Gifts
 - b. Hospitality
 - c. Access to decision makers
 - d. Keeping a secret

6. Counterfeit detection pens are used to detect:
 - a. Wood-based paper
 - b. Rag-based paper
 - c. Hemp-based paper
 - d. Inferior ink
7. Possession of counterfeit currency is punishable by up to ____ years in jail.
 - a. 5
 - b. 10
 - c. 15
 - d. 20
8. Which of the following components is **not** part of the fraud triangle?
 - a. Rationalization
 - b. Concealment
 - c. Opportunity
 - d. Pressure
9. Which of the following is the most common concealment method used by fraudsters?
 - a. Creating fraudulent physical documents
 - b. Altering physical documents
 - c. Altering electronic files
 - d. Creating fake journal entries
10. Which of the following individuals developed the fraud triangle theory?
 - a. Gabriel Tarde
 - b. Edwin Sutherland
 - c. Ronald Akers
 - d. Donald Cressey
11. Which of the following fraud schemes involves stealing payments from one customer and covering the theft with payments stolen from other customers?
 - a. Skimming
 - b. Lapping
 - c. Billing fraud
 - d. Graft

12. CryptoLocker is an example of:
- a. Phishing
 - b. Ransomware
 - c. Spoofing
 - d. Money Laundering
13. Which of the following is **not** a type of corruption?
- a. Conflict of interest
 - b. Bribery
 - c. Economic extortion
 - d. Asset misappropriation
14. Which of the following identifies the most common way that fraud is detected?
- a. External audits
 - b. Accidental discovery
 - c. Tips
 - d. Confession
15. Each of the following is an example of expense reimbursement fraud, **except:**
- a. Altering receipts
 - b. Split expenses
 - c. Laundered expenses
 - d. Deposit refunds
16. Which of the following types of cyber-attack is used to try to take down a government website?
- a. Denial of service
 - b. Phishing
 - c. Ransomware
 - d. Data breach

17. Banks are required to file a Suspicious Activity Report (SAR) for cash transactions over:
- a. \$1,000
 - b. \$5,000
 - c. \$7,500
 - d. \$10,000
18. Identity theft is a:
- a. Civil, not criminal, matter
 - b. Criminal misdemeanor
 - c. Criminal felony
 - d. Misdemeanor
19. The Identity Theft Task Force was established in what year?
- a. 1996
 - b. 2001
 - c. 2006
 - d. 2008
20. The Federal Trade Commission passed the Red Flags Rules in what year?
- a. 1996
 - b. 2001
 - c. 2006
 - d. 2008
21. Which type of asset misappropriation involves stealing cash before it is recorded in the accounting system?
- a. Theft of cash
 - b. Lapping
 - c. Skimming
 - d. Billing schemes
22. Which of the following is *not* a common way to steal data from a computer?
- a. Malware on charging stations
 - b. Social networking
 - c. Vishing
 - d. Hacking

- 23.** Which of the following statements is correct?
- a.** Fraudsters cannot duplicate gift cards.
 - b.** Fraudsters cannot duplicate the new chip cards.
 - c.** Fraudsters cannot purchase blank credit cards.
 - d.** Any card can be easily duplicated.
- 24.** Which of the following identifies the most common way that occupational fraud is discovered?
- a.** By accident
 - b.** Tips
 - c.** External auditors
 - d.** Internal auditors
- 25.** Shoplifting or employee theft would be considered to be a type of:
- a.** Corruption
 - b.** Skimming
 - c.** Asset misappropriation
 - d.** Lapping
- 26.** Sandbagging is related to:
- a.** Bill and hold frauds
 - b.** Channel stuffing
 - c.** Fake sales
 - d.** Improper sales cut-off
- 27.** Which type of payroll fraud uses fictitious employees?
- a.** Slow work for OT
 - b.** Vacation abuse
 - c.** Ghost employees
 - d.** Falsification of hours worked
- 28.** Which of the following accounts receivable frauds involves management misstating the accounts receivable balance to lenders?
- a.** Factoring fraud
 - b.** Payment diversions
 - c.** Skimming
 - d.** Check swaps

29. Which of the following would **not** normally be involved in a skimming scheme?
- a. Business owners
 - b. Employees
 - c. Managers
 - d. Customers
30. A person's _____ is not considered to be personally identifying.
- a. Name
 - b. Occupation
 - c. Address
 - d. Social Security number

Answer Sheet

2019 Fraud Review

(10070641-0001)

[Fill-In PDF](#)

Go to cchcpelink.com/printcpe to complete your Final Exam online for instant results.

A **\$75.95 processing fee** will be charged for each user submitting the exam to cchcpelink.com/printcpe for online grading.

Please answer the questions by indicating the appropriate letter next to the corresponding number.

- | | | | |
|----------|-----------|-----------|-----------|
| 1. _____ | 9. _____ | 17. _____ | 25. _____ |
| 2. _____ | 10. _____ | 18. _____ | 26. _____ |
| 3. _____ | 11. _____ | 19. _____ | 27. _____ |
| 4. _____ | 12. _____ | 20. _____ | 28. _____ |
| 5. _____ | 13. _____ | 21. _____ | 29. _____ |
| 6. _____ | 14. _____ | 22. _____ | 30. _____ |
| 7. _____ | 15. _____ | 23. _____ | |
| 8. _____ | 16. _____ | 24. _____ | |

Please complete the Evaluation Form (located after the Answer Sheet).
Thank you.

2019 Fraud Review course: Evaluation Form

(10070641-0001)

[Fill-In PDF](#)

Please take a few moments to fill out and submit this evaluation to Wolters Kluwer so that we can better provide you with the type of self-study programs you want and need. Thank you.

About This Program

1. Please circle the number that best reflects the extent of your agreement with the following statements:

		Strongly Agree			Strongly Disagree		
a.	The Course objectives were met.	5	4	3	2	1	
b.	This Course was comprehensive and organized.	5	4	3	2	1	
c.	The content was current and technically accurate.	5	4	3	2	1	
d.	This Course content was relevant and contributed to achievement of the learning objectives.	5	4	3	2	1	
e.	The prerequisite requirements were appropriate.	5	4	3	2	1	
f.	This Course was a valuable learning experience.	5	4	3	2	1	
g.	The Course completion time was appropriate.	5	4	3	2	1	

2. What do you consider to be the strong points of this Course?

3. What improvements can we make to this Course?

THANK YOU FOR TAKING THE TIME TO COMPLETE THIS SURVEY!

About the Author

Dr. Minniti is the President and Owner of Minniti CPA, LLC. Dr. Minniti is a Certified Public Accountant, Certified Forensic Accountant, Certified Fraud Examiner, Certified Valuation Analyst, Certified in Financial Forensics, Master Analyst in Financial Forensics, Chartered Global Management Accountant, and is a licensed private investigator in the state of Arizona. Dr. Minniti received his doctoral degree in business administration from Walden University, received his MBA degree and Graduate Certificate in Accounting from DeVry University's Keller Graduate School of Management, and received his Bachelor of Science in Business Administration degree from the University of Phoenix. Dr. Minniti teaches graduate and undergraduate courses in forensic accounting at Northwestern University, and the University of Phoenix. He designed graduate and undergraduate courses for Grand Canyon University, Northwestern University, and Anthem College. He is a writer and public speaker. He has experience in forensic accounting, fraud examinations, financial audits, internal audits, compliance audits, real estate valuations, business valuations, internal control development, business continuation planning, risk management, financial forecasting, and Sarbanes-Oxley compliance work. Dr. Minniti is an instructor teaching continuing professional education classes for the American Institute of Certified Public Accountants, Compliance Online, CPE Link/CCH . AccountingEd, Global Compliance Panel, Clear Law Institute, The Institute of Management Accountants, the National Association of Valuators and Analysts, and various state CPA Societies.

For Additional Information

LinkedIn Profile: www.linkedin.com/in/robertminniti

Company Website: www.minniticpallc.com