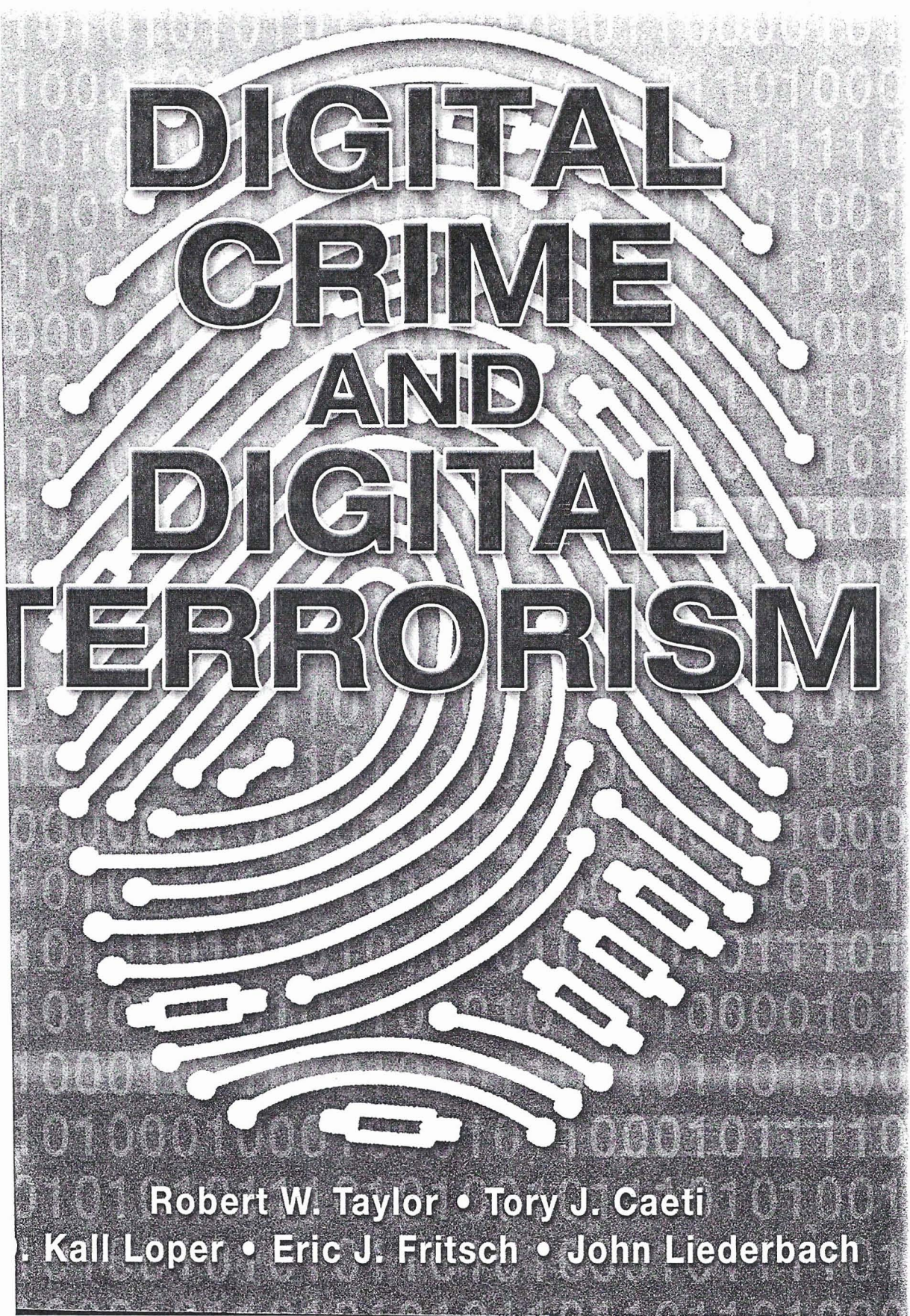
DIGITAL
CRIME
AND
DIGITAL
TERRORISM
Robert W. Taylor • Tory J. Caeti
. Kall Loper • Eric J. Fritsch • John Liederbach

fixation with the "gory details" such crimes produce has been a matter of some debate; what is clear is that the public's common perception of what constitutes "crimes" as well as who is the common "criminal" have been formed largely in relation to traditional street crimes.[1] As a result, crimes that do not fall under traditional definitions or those that are committed by persons who do not fit the public's common perception of the typical "criminal" have received much less attention.

Noted criminologist Edwin Sutherland was the first to highlight these disparities in the late 1940s, and he attempted to describe and define a class of behaviors very different from those of traditional street crimes, including acts committed by corporate executives, corrupt politicians, and unscrupulous professionals. He defined these acts as "white-collar crimes," and he suggested that they are largely ignored because the perpetrators of these offenses comprised society's elite—people with the economic wherewithal and status to shape the criminal law in their favor and avoid detection and punishment.[2]

This chapter will describe the ways in which the computer revolution has altered the techniques used to commit some of the most common white-collar offenses, specifically embezzlement, corporate espionage, money laundering, identity crimes, and fraud. The large-scale dissemination of computer and information technologies seems to have created greater opportunities for the white-collar offender, and law enforcement officials are now faced with the unenviable task of looking for loopholes in the ever-expanding technologies used to commit white-collar offenses.

EMBEZZLEMENT

Embezzlement has been defined as the unlawful misappropriation for personal use of money, property, or some other thing of value that has been entrusted to an offender's care, custody, or control. Embezzlement is essentially a theft in violation of a trust. As such, embezzlement has been recognized as a crime since English common-law traditions dating back to the 15th century.[3] The embezzler usually is engaged in some type of fiduciary relationship with the victim, either as an employee, guardian, or trustee. Traditionally, embezzlement has involved the physical theft of money or property by employees or others engaged in managing the assets of persons or organizations.

Embezzlement has been the subject of considerable research and debate in regards to both its definition as a traditional white-collar offense and the motivations behind embezzlement schemes. Although Sutherland specifically used embezzlement as an example in his early portrayal of white-collar offending, historically the embezzler has not been a person of high social status. Rather, he or she has typically been a person engaged in managing the financial affairs of societal elites. Historically, the typical embezzler is a low-level financial institution employee, usually a female bank teller engaged in stealing financial deposits directly from bank customers. In this regard, some have argued that the embezzler has more in common with the traditional street robber than the corporate executives or professionals originally highlighted by Sutherland in his depiction of white-collar offenders. So too, unlike most other white-collar offenses, embezzlement schemes are often carried out by individual offenders rather than by cor-

porations and other organized entities. These disparities aside, most researchers have historically categorized embezzlement as a white-collar offense, probably because the offense involves a violation of professional trust in which deception rather than physical force is used to carry out the act.

Donald Cressey, in his classic embezzlement study *Other People's Money,* identified a four-step process that described the motivations common to his sample of convicted embezzlers. Prior to the commission of the crime, the embezzler often finds themselves experiencing financial problems that cannot be solved through legitimate financial means. The offender then identifies embezzlement as an avenue through which to alleviate his or her financial problems. The embezzler must also possess the technical knowledge necessary to carry out the embezzlement scheme. Finally, the embezzler will use "neutralization techniques" in order to overcome any lingering shame or guilt associated with stealing money that has been entrusted to their care. These techniques may involve the intention of paying the money back before anyone notices its absence, or justifying the theft based on the belief that the "rich" individuals or organizations that have entrusted the money to the embezzler's care will not miss the funds. Freed from these considerations, the embezzler commits the theft in order to solve his or her financial problems.[4]

The advent of the computer age and the ubiquitous use of computers in the management, allocation, and tracking of both personal and business finances have transformed the methods used by embezzlers to misappropriate cash and/or property. Today, the computer provides the most available means to commit embezzlement, and knowledge relating to the manipulation of large-scale computerized financial databases has become the primary tool of the embezzler.

With regard to other computer crimes, embezzlement can be classified as a "computer-assisted" crime rather than a "computer-focused crime." Computer-assisted crimes are those where the computer is used in a supporting capacity. The specific crime, such as embezzlement, predates the introduction of computers. In contrast, computer-focused crimes have emerged more recently as a direct result of computer technology (e.g., hacking).[5] Anderson has classified the modern-day embezzler as an "internal perpetrator," or an authorized user of computer systems who uses legitimate access to computer files to commit theft. Because embezzlers have been authorized to use computer systems and resources, they are among the most difficult computer criminals to detect and apprehend.[6]

While the crime of embezzlement appeared centuries before the computer revolution, the use of computer technology does appear to have altered both the commission of the act and the profile of those who embezzle. First, the traditional embezzler was often limited by the physical nature of the theft act. That is, there was a limit to how much cash and or property the embezzler could actually steal because the act involved taking and transferring cash or other material goods. Modern embezzlement schemes using computerized records often may not involve the physical theft of anything. The embezzler's take is predicated only on his or her abilities as they relate to the misappropriation of data files, and millions of dollars can be stolen with simple keystrokes.

Second, the advent of technologically driven financial management techniques may have narrowed the pool of potential embezzlers to those individuals who possess the specialized skills required to use computer information systems. In this regard, modern-day "technical elites" who steal from their employers and organizations may more closely resemble the societal elites originally identified by Sutherland as typical white-collar offenders. Indeed, more recent studies of convicted embezzlers seem to suggest that rather than experiencing financial problems, many technically elite embezzlers are simply motivated by a desire for a more affluent lifestyle.[7] Nonetheless, the examples listed below of recent embezzlement cases involving the misuse of computer technologies can be used to illustrate the widely varied nature of both the perpetrators of modern day embezzlement and their victims, including private businesses, government agencies, and individuals:

- Thirty-six-year-old Daniel Gruidl of Minnesota pled guilty to computer fraud charges related to the embezzlement of funds from his employer, Vital Signs of Minnesota Inc. Grudl felt that he was underpaid, so he simply used false passwords in order to log onto the company's computerized payroll system. He proceeded to give himself raises and bonuses that totaled over $108,000. The scam went undetected for two years.[8]
- Don McCorry worked as a Senior Financial Manager in charge of government employee retirement accounts in Fairfax, VA. McCorry altered computer records of employee withdrawals from their retirement accounts by reassigning monies to his personal retirement account, labeling them "emergency" withdrawals in his own name. McCorry embezzled over $1.1 million over a four-year period. When he was arrested, investigators confiscated a Mercedes-Benz, a $50,000 art collection, a $100,000 wine collection, and fifty suits valued at $10,000 from his residence.[9]
- A computerized payroll glitch at a North Carolina hospital resulted in a hospital cook being paid $787 an hour over a three-month period. The cook failed to report the overpayment, stating that she believed the glitch to be a "gift from God."[10]
- Cleveland stockbroker Frank Gruttadauria defrauded 50 prominent business executives and investment clients over a 15-year period. He exaggerated the values of client investment portfolios by altering computerized financial statements. Clients believed they had $277 million in assets, but their accounts totaled barely $1 million in actual value. One individual investor appropriated about $120 million to Gruttadauria. $60 million was actually invested, and the actual cash value of his holdings upon detection of the scam was $8,000.[11]

CORPORATE ESPIONAGE

Corporate espionage involves any theft of proprietary business information through spying or deception, particularly the theft of "trade secrets." Trade secrets encompass any proprietary information that produces value to a commercial enterprise because it

provides competitive advantages over business rivals.[12] The informational targets to be stolen through corporate espionage schemes are wide and varied, including detailed customer lists, product specifications, research and development data, computerized source codes, memoranda detailing corporate strategies, pricing lists, and technology and computer systems data.[13]

Corporate concerns regarding espionage and the theft of business secrets have grown over the course of the last two decades. Several related factors have combined to increase the occurrence of corporate espionage and heighten awareness of the problem. First, the corporate community's increasing use of information and computer technologies to conduct business has provided corporate spies easier access to valuable proprietary information. In particular, the ubiquitous use of e-mail as a means of intra-office communication has made employee exchanges readily accessible to potential corporate spies who possess the technical expertise to crack such networks. In addition, global commerce has increasingly been conducted electronically over the Internet (i.e., "e-commerce"), which has created a wealth of accessible corporate data available to cyberspace hackers.[14] These factors have worked to make the theft of corporate information much easier. It is no longer necessary for corporate thieves to steal information physically, since most valuable corporate secrets usually exist solely in computerized form.

As a result of these factors, the incidence of and costs associated with corporate espionage have risen sharply. A recent survey by the American Society for Industrial Security (ASIS) estimates that Fortune 1,000 companies lost close to $45 billion dollars to corporate spies in 1999 alone.[15] Indeed, some analysts estimate that losses from business espionage have doubled since the early '90s. The average company detects 2.45 cases of corporate espionage per year, with each incident costing approximately $500,000. Technology companies appear to be particularly vulnerable. Fortune 1,000 tech firms report an average of 67 espionage attacks per year, costing these firms an average of $115 million annually.[16]

While the dawn of the information age has increased the use of spy tactics among domestic corporate rivals, global political and military trends have also played a role in elevating the costs related to corporate espionage. With the end of Cold War rivalries between the U.S. and Soviet militaries, nations have increasingly concentrated espionage efforts toward the theft of trade, rather than military, secrets. So too, the end of U.S.-Soviet hostilities helped to created a vast network of former military spies—individuals highly skilled in espionage tactics—available for corporate hire.[17] The result has been an increase in the use of corporate espionage by nations looking for competitive advantages for their domestic industries. The National Counter-Intelligence Agency estimates that U.S. businesses lost $44 billion to the theft of trade secrets by international spies between 1996 and 1997.[18]

Corporate spies can be divided into two distinct groups.[19] Most corporate espionage schemes are conducted by business "insiders," persons who have legitimate access to a company's computer networks, such as employees, information technology personnel, or corporate executives. Limited research suggests that up to 85 percent of all such schemes are carried out by these insiders, whose motivations extend from

blackmail and monetary concerns to a simple lack of loyalty or job dissatisfaction.[20] The remaining acts of corporate espionage are performed by corporate "outsiders," or persons who crack into a corporation's computer data networks without any form of legitimate access rights. Outsiders may penetrate computer systems via the Internet, or by gaining access to internal computer networks. Outsiders include domestic spies hired by corporate competitors, as well as foreign nationals hired by adversarial governments intent on gaining a competitive advantage over American firms. At the extreme, these types of spies may access proprietary information simply by entering the workplace facility and visually stealing computer passwords or gaining physical access to computer server rooms.[21]

Outside the realms of insiders and outsiders, the growing employment of independent contractors by large-scale corporations has created unique problems in regard to corporate espionage schemes. Independent contractors are individuals hired by a corporation to perform specific, limited jobs, such as database management, product introductions, or programming changes. These individuals (often referred to as "kites") more closely resemble temporary workers rather than full-time employees, and their resulting lack of loyalty and long-term commitment to the hiring corporation may make them vulnerable targets for information for competing firms. "Kites" may also be hired by competing firms because they have specific knowledge concerning competitor operations.[22]

Companies that have been victimized by corporate espionage schemes can pursue a civil action against the offending firm; however, civil suits often turn into lengthy affairs and the invariable costs incurred through civil courts are prohibitive. The case involving Silicon Valley software firms Cadence Design Systems and Avant! Corporation provides a prime example of the painstakingly slow and costly process involved in resolving domestic espionage suits (see Box 5.1 below for a timeline of events surrounding the case and its eventual outcome).[23] The case originated with an internal investigation conducted by Cadence Design Systems in 1995.[24] Over the course of the preceding four years, several top Cadence executives had left the company to form a rival firm, Avant! Corp. Both companies write software code that helps computer engineers design silicon chips used in advanced computer systems. Cadence executives claimed that Avant! executives had stolen Cadence source code in order to develop software that was producing over $100 million in sales by 1996. The civil and criminal trials took eight years to resolve.[25]

In response to these concerns, as well as the belief that the problem of corporate espionage had grown with the increasing use of computers in the workplace, Congress enacted the Economic Espionage Act of 1996. Under the act, corporations who suspect that they are victims of espionage schemes may request an FBI investigation. If such an investigation reveals criminal wrongdoing, the U.S. Attorney's office of the Department of Justice can prosecute the offending firm for theft of trade secrets.[26]

The Economic Espionage Act outlines two separate offenses related to corporate spying. First, the act attempts to enforce espionage crimes originating from foreign governments and businesses by creating criminal penalties for those who steal, destroy, or knowingly receive stolen trade secrets that would benefit foreign governments. Individual offenders may be fined up to $500,000 and/or face a prison sentence of up to fifteen

BOX 5.1 Cadence Design Systems vs. Avant! Corporation

June 1994	Avant! sales reach $39 million after former Cadence Vice President Gerald Hsu joins three other former Cadence executives to head up Cadence rival Avant!
August 1995	During a routine site visit to an Avant! customer, Cadence engineers notice similarities between Avant! code and Cadence code that they had developed years earlier. Four thousand lines of identical code are identified, including grammatical and program errors.
December 1995	Santa Clara Co. District Attorneys conduct a search and seizure at Avant! headquarters. Cadance files a formal civil complaint in U.S. District Court. The complaint contends that four Avant! executives conspired to steal trade secrets and copyrighted information over a three-year period.
April 1996	Avant! and six employees, including the Chairman and Chief Executive Officer, are indicted on criminal charges in Santa Clara County, CA.
March 1997	Cadence fails in its attempt to obtain a preliminary injunction against Avant! intended to stop the sale of software allegedly pirated from Cadence source code.
July 1997	Judge stays the civil suit against Avant! in consideration of the pending criminal charges.
September 1997	Preliminary injunction granted against Avant! barring the company from selling software developed from allegedly stolen source code.
February 1998	Avant!'s Chief Financial Officer resigns.
November 1998	Grand jury convenes to consider criminal indictment against Avant! employees.
December 1998	Federal judge extends preliminary injunction against Avant! barring it from selling newer version of software.
May 2001	Eleven Avant! employees and executives plead no contest to criminal charges related to trade secret theft. Individual fines range from $27,000 to $2.7 million.
July 2001	Avant! ordered to pay over $200 million in restitution and court costs to Cadence.
November 2002	Cadence agrees to settle all civil claims against Avant! and its employees in exchange for $265 million in damages. The companies agree to a reciprocal licensing agreement covering the software in question.

years. Under this portion of the act, corporations may be fined up to $10 million. Second, the act enforces domestic espionage between competing U.S. firms by making the theft of trade secrets related to or included in a product involved in interstate commerce a federal crime. Individual offenders may be fined up to $250,000 and/or face a prison sentence of up to ten years. Under this portion of the act, corporations may be fined up to $5 million.[27]

MONEY LAUNDERING

Money laundering is the act of concealing the source of assets that have been illegally obtained. The primary object in laundering is to hide the source and ownership of such funds through the creation of a seemingly legitimate history or paper trail. Like embezzlement, money laundering is an "old" crime whose opportunities have expanded greatly with the increasing use of technology in the marketplace. It is impossible to know the extent to which money laundering occurs; however, experts estimate that about $300 billion in cash is laundered each year. The amount of illegal money laundering associated with the drug trade alone is thought to be anywhere from $5 to 15 billion annually.[28]

Traditionally, money laundering was accomplished through three primary means: (1) Cash that was illegally obtained could be physically transported from its place of origin to a jurisdiction that had less stringent banking and reporting requirements. Although the money would eventually be "lost" in the eyes of law enforcement in this new jurisdiction, the act of physically moving cash from one place to another is time-consuming, dangerous, and cumbersome for the launderer. (2) The launderer could quickly transform hard currency into legitimate real property, such as real estate, commercial interests, or personal luxuries.[29]

The problems with transforming illegally gained assets in this manner are twofold. First, the large-scale purchasing of property is ostentatious, and authorities may notice changes tending toward a suddenly lavish lifestyle. Second, many criminals may have difficulty spending all of their ill-gotten cash, given the exorbitant profits in some illegal enterprises (e.g., large-scale drug trading). (3) Launderers often turned to a method commonly referred to as "smurfing." Smurfing involves the division of large amounts of cash into smaller denominations so as to conceal its common origin. The launderer would enlist several persons to deposit relatively small amounts of cash into several different accounts scattered over a geographic area. In this way, the launderer could successfully avoid federal reporting requirements regarding large-scale cash deposits.[30]

The increasing use of technology, especially telecommunications and the Internet, has provided a wealth of new opportunities for the money launderer. Obscuring the origin and owner of large amounts of cash is now a keystroke away. In order to understand the impact that technology has had on money-laundering crimes, it may be useful to view the advancement of technology in this area in two distinct phases. During the 1960s and '70s, governments, banks, and other financial institutions increasingly used telecommunications networks to move large amounts of cash.[31] These electronic cash transactions, or "electronic funds transfers" (EFTs), served to digitize the financial mar-

ketplace. Telephone lines and computer networks substituted for the physical transport of cash and other financial instruments.

Money is swiftly and easily moved both legitimately and illegitimately across these computerized networks. Currently, there are two primary cash transfer institutions. FedWire is the electronic payment network created by the Federal Reserve System. Over 250,000 transactions are performed on the system per day. CHIPS is a clearinghouse payment system created by private banking companies. This consortium moves over $866 billion per day.[32]

The electronic revolution that has occurred in the banking industry, especially the large-scale movement of cash in electronic forms, has made laundering easier. Because money transfers now involve electronic messages rather than physical cash, it is easier for the launderer to move money in a series of transactions over a short period of time. Smurfing can be accomplished by one individual at a keyboard rather than a large group of smurfs over a wide geographic area. So too, money that can be moved electronically is also easier to integrate into the mainstream banking system.

While the introduction of telecommunications and computer technologies in the 1960s and '70s served to increase the ease with which money could be laundered, the current explosion in e-commerce and the influence of the Internet may provide launderers even greater opportunities in years to come. The biggest concern for law enforcement officials is the recent introduction of anonymous electronic cash exchange systems, or "e-cash."[33] E-cash is digital money that may be exchanged over the Internet. It is an electronic replacement for cash. E-cash comprises an electronic series of numbers that have intrinsic value in some form of currency.[34] E-cash may be likened to the serial numbers located on hard currency, except in the case of e-cash there is no hard currency, only the related electronic numbers. Interest in the use of e-cash has grown in conjunction with the Internet, largely because it can be exchanged with increased speed and efficiency. On line businesses can also increase e-commerce profits through its use.

Authorities fear that the increasing use of such "cashless" systems may promote unique "cyberlaundering" schemes that are more difficult to detect and defend against. Researcher Mark Bortner describes a hypothetical scenario whereby the anonymous nature of e-cash and the ease with which it can be accessed through the Internet provides "cyberlaunderers" easy opportunities:[35]

> Doug drug dealer is the CEO of an ongoing narcotics operation. Doug has rooms filled with hard currency that is the profits from his illegal enterprise. This currency needs to enter into the legitimate mainstream economy so that Doug can either purchase needed supplies and employees, purchase real or personal property or even draw interest on his ill-gotten gains . . . Doug employs Linda launderer to wash the dirty money. Linda hires couriers ("smurfs") to deposit funds under different names in amounts between $7,500 and $8,500 at branches of every bank in certain cities . . . In the meantime, Linda launderer has been transferring these same funds from each branch and depositing the money with Internet banks that accept E-cash . . . Once the hard currency has been converted into digital E-cash, the illegally earned money has become virtually untraceable—anonymous. Doug drug dealer now has access to legitimate electronic cash.

Law enforcement authorities have several tools at their disposal to enforce money laundering crimes. The oldest among these is the Bank Secrecy Act of 1970 (BSA). The BSA requires banks and other financial institutions to file records concerning suspicious financial transactions over $10,000 (e.g., large cash deposits, foreign bank exchanges, cross-border currency transports). In addition, the 1986 Money Laundering Control Act works to close certain loopholes in the BSA that were exploited by launderers in the past. Specifically, the Money Laundering Control Act requires banks and other financial institutions to report any suspicious banking transactions (including possible "smurfing" schemes) regardless of the monetary amount of any single transaction.[36]

Finally, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) serves as a "central clearinghouse" for intelligence and information sharing on money laundering.[37] FinCEN's main objective is to provide law enforcement agencies the analytical tools necessary to identify and prosecute money laundering cases. FinCEN uses two primary avenues to accomplish this goal. First, FinCEN provides direct case support to over 150 local law enforcement agencies, and coordinates efforts with the International Association of Chiefs of Police (IACP), the National White Collar Crime Center (NWCCC), and the National Association of Attorneys General (NAAG). This support specifically involves developing linkages from the various aspects of money laundering cases so that prosecutions can occur. Second, FinCEN provides secondary support to local law enforcement agencies in the form of training, office space, and database research access. FinCEN officials have termed this support a "platform approach" to solving money-laundering cases, whereby federal resources are used to aid local law enforcement efforts directly.

Over the course of the last 13 years, FinCEN has provided law enforcement and regulatory agencies over 50,000 analytical case reports involving over 200,000 money laundering suspects. In recognition of the increasingly "borderless" nature of "cyber-laundering," FinCEN also spearheads efforts to promote international cooperation in the fight against laundering. FinCEN develops these international partnerships through Financial Intelligence Units (FIU), or centralized money-laundering analysis agencies located across the globe.[38] These FIUs appear to be of increasing importance, given the inherently global nature of international terrorists attacks and these organization's vital interest in maintaining adequate monetary resources in order to foster new terrorist networks and fund future terror attacks.

IDENTITY THEFT

The recent emergence of identity crimes as a primary public and law enforcement concern can be viewed as indicative of the more general patterns of growth we have witnessed in computer crimes during the course of the last several decades. The exponential growth in the incidence of identity theft can largely be attributed to the creation of opportunities that are directly linked to technological and commercial advances. These advances have produced an alarming rise in the fraudulent use of individual information such as Social Security numbers, dates of birth, and credit card numbers by thieves

who are intent on using this information for personal gain, and they have forced law enforcement agencies to redirect scarce resources in order to mitigate the threat.

Statistical trends reveal the feverish pace of growth in identity theft crimes. Experts estimate that personal losses related to identity theft reached $745 million in 1997 alone, a figure that represents a 68 percent increase in losses tied to identity theft over only a two-year span.[39] Credit thieves victimize approximately 1,000 individuals per day, and national estimates indicate that 350,000 to 500,000 persons annually experience monetary losses connected to identity crimes.[40] Trans-Union Corp., one of the three primary credit-reporting bureaus, indicates that about two-thirds of all consumer inquiries to the company's fraud division in 1997 involved possible identity theft crimes, or over 43,000 complaints per month.[41] In 1999, the Social Security Administration received over 62,000 allegations involving the misuse of Social Security numbers alone.[42] These explosive growth patterns are clearly beginning to strain law enforcement resources at the federal level—identity theft has been the primary charge in over 90 percent of all arrests made by the Secret Service's Financial Crimes Division since the mid-1990s. Losses related to closed identity theft cases by the Division topped $248 million in 2000, with potential losses tied to other reported cases nearing $1.5 billion.[43]

These trends can partly be attributed to the increasing use of Social Security numbers as personal identifiers. Social Security numbers, rarely referred to by those under retirement age decades ago, are now used as a means to conduct a wide range of business transactions, most notably the opening of new lines of personal credit. The use of Social Security numbers as personal identifiers, however, has not been limited to credit transactions. We are now asked to include the number on an ever-increasing array of forms, including medical records, motor vehicle driver's licenses, educational and employment records—some car dealers will even ask for it prior to allowing a customer to test drive a vehicle. Obviously, theft opportunities increase in relation to the number of times that consumers are required to use Social Security numbers as personal identifiers by commercial and governmental enterprises.

Moreover, growth trends in identity theft have strongly paralleled the advent of "e-commerce," or the use of on line technologies to conduct both consumer-based and business-to-business transactions. Today's consumer—ardently pounding out key strokes and "surfing" commercial Web sites—is far more likely to be asked to provide his or her Social Security number at their virtual "checkout" than was the more traditional pedestrian shopper of previous decades.

Identity thieves use a variety of methods to steal personal information. Heading up the list of low-tech means is "dumpster diving," or rummaging through private or commercial trash receptacles in search of discarded bills or pre-approved credit applications.[44] Other low-tech methods include the direct theft of mail, which may include a veritable treasure trove of personal information, contained on bank statements and unwanted telephone calling cards. Some thieves even complete change of address forms in the name of unwitting victims in order to divert and more easily access personal mail. "Shoulder surfing," or eavesdropping on conversations and cash transactions that involve the disclosure of personal identifiers, provides an avenue for low-tech thieves who are unwilling to steal documents outright.[45] While these theft techniques provide

BOX 5.2 Recent Identity Crime Prosecutions

- Federal agents arrested a former employee at a Long Island software company who allegedly originated a crime ring that eventually cost consumers $2.7 million. The suspect sold the credit reports of over 30,000 people, including names, Social Security numbers, and other credit information, to black market identity thieves who used the information to fraudulently obtain a wide variety of consumer goods. Each victim's credit history was sold for only $30.
- A defendant was recently convicted in federal court for fraudulently obtaining the names and Social Security numbers of high ranking military officers from internal government Web sites and using the information to apply on line for credit cards and other lines of credit. He was sentenced to 41 months in prison and ordered to pay over $186,000 in restitution.
- A former temporary employee of an insurance firm was convicted for using policyholders' bank account information to deposit over $764,000 in counterfeit bank checks.
- Seven defendants were recently convicted in an identity theft–drug smuggling scheme. The suspects used stolen Social Security numbers to garner employment and identification documents that were used to facilitate the smuggling of heroine and methamphetamine from Mexico. A number of the defendants also used their stolen identities to claim earned income tax credits on IRS tax forms.

opportunities for everyday thieves, more organized and technologically based methods have been used by sophisticated thieves intent on stealing mass quantities of personal information. These schemes may involve hacking information from corporate databases used for on line transactions or the bribing of employees who have internal access to customer identifiers.

Once personal identifying information is obtained, thieves can ransack a victim's financial status and destroy their credit history with frightening ease. For example, they may be able to open a new credit account using stolen Social Security numbers, names, and date of birth. The victim, of course, is left with the unpaid bills and delinquent accounts. Depending on the amount of personal information stolen, thieves may even be able to create entirely new bank accounts in your name, writing "hot" checks that are eventually traced back to the victim's credit history. Others have been victimized by thieves who have established wireless phone service, bought cars and other expensive consumer goods, and filed for bankruptcy under assumed identities in order to avoid paying past due accounts (see Box 5.2).[46]

Federal law enforcement agencies and the criminal justice system have begun to respond to the increasing threat posed by identity thieves through new legislation and consumer awareness programs. In 1998 Congress passed the Identity Theft and Assumption Deterrence Act. The law makes it a federal crime when someone:

> Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[47]

Violations of the law may be punishable by up to 15 years in prison. While the act clearly signifies a growing recognition of the costs associated with identity crimes, the impact of these and other laws aimed at curtailing identity theft may be largely symbolic for many of those victimized. The reality is that identity crimes remain extremely difficult to prosecute once detected. A large number of cases are detected too late for officials to investigate adequately. These cases are extremely labor intensive, and often require collaborative effort on the part of federal, state, and local law enforcement agencies for successful prosecution. So too, the actual monetary losses involved in many individual cases of identity theft may be considered too small for dedication of a large amount of prosecutorial resources.[48]

Given the difficulties inherent in detecting and prosecuting identity crimes, many experts believe that the establishment of consumer awareness and monitoring programs may be the most viable avenue toward thwarting the growth of identity theft. To this end, the Federal Trade Commission (FTC) has established the Identity Theft Clearinghouse. The clearinghouse collects identity theft complaints and provides victims referral information and other resources aimed at helping them restore their credit history and financial status. The clearinghouse has also established a hotline for consumers who believe they have been victimized in an identity crime.[49]

INTERNET FRAUD SCHEMES

The Internet has increasingly been used as a vehicle for interpersonal communications, research, consumer spending and business-to-business transactions over the course of the last decade. This growth has provided the public with previously unparalleled opportunities for personal and economic advancement, and has created entire new industries in the process. These advances, however, have also produced fresh opportunities for fraud and abuse on line. Interestingly, many fraud schemes committed over the Internet are simply new takes on old themes—chain letter hoaxes, confidence schemes, and bait-and-switch con games that are now performed over an electronic medium rather than in person or over the telephone. Whether in old or new form, it is clear that the increasing use of the Internet has given rise to an alarming growth in fraudulent schemes. According to the official reporting rates of the National White Collar Crime Center, consumer complaints concerning on line fraud have risen from 16,838 in 2000 to over 75,000 complaints in 2002, over a 400 percent increase in just two years.[50] These Internet fraud schemes encompass a wide range of offenses, including financial institution fraud, investment fraud, communications fraud, and confidence schemes. This section will briefly define and describe the first three above-mentioned types of Internet fraud, as well as discuss various types of confidence schemes in more detail.

Financial institution fraud involves attempts to conceal the truth from deposit and lending institutions so as to gain monetarily.[51] Examples of financial lending institution fraud include credit/debit card fraud and identity theft. Credit card fraud is one of the most widely reported Internet frauds, and identity theft has become a primary concern for law enforcement personnel and the public alike (see Chapter 10 for a discussion concerning enforcement efforts against identity theft). Investment frauds are "deceptive practices involving the use of capital to create more money," including traditional stock market investment schemes and pyramid business schemes designed to defraud individual consumers, all of which can be conducted on line.[52] Communication frauds involving new and different forms of technology have skyrocketed through thefts of wireless phone codes and other satellite communication devises.[53]

While all types of Internet fraud have experienced recent growth, frauds that involve a breach of personal trust, or what have been traditionally referred to as confidence schemes, may be among the most widely practiced and familiar to the general public. These schemes now typically use email communications or on line sites as a primary medium rather than the mail or telephone. The most widely perpetrated Internet confidence schemes include on line auction fraud, the Nigerian "419" fraud, chain letter hoaxes. and what are known as "urban legends" passed along through electronic mailings.

On line auction fraud is the most widely reported type of Internet fraud by a large margin. Sixty-four percent of all reported Internet fraud is auction fraud, and the Internet Fraud Complaint Center (IFCC) received over 30,000 auction fraud complaints in 2001. Losses related to on-line auction fraud surpass $4,000,000 annually; the average loss per complaint is $776.[54] Individuals and/or businesses participating in on line auctions can be defrauded in several ways. The most prevalent form of on line auction fraud is nondelivery of goods. In most cases, the victim of nondelivery has very little recourse if payment for the item has already been received by the would-be seller. Most on line auction buyers do not have a physical address or description of the perpetrator. Sellers may also purposely misrepresent the item to be auctioned in terms of its quality or characteristics. This can be accomplished through simple item descriptions or the altering of item pictures. "Shill bidding" is the use of intentional fake bidding on the part of the seller in order to artificially inflate an item's auctioned price. Finally, "fee stacking" occurs when the seller adds hidden charges to the cost of the item prior to delivery, most often through inflating the shipping cost. The costly nature of these schemes is detailed in Box 5.3, which provides excerpts from case summaries provided by the IFCC of two of the most extensive schemes recently investigated by federal law enforcement authorities.[55]

Another highly publicized on line fraud scheme has been dubbed the Nigerian 419 scheme by authorities. Since its origination in 1989, the on line e-mail letter scheme has cost individuals and businesses an estimated one billion dollars globally. The scheme is named "419" after the relevant Nigerian criminal codes that are involved. The scheme encompasses numerous different e-mails forwarded by Nigerian nationals in which the correspondence outlines nonexistent opportunities for recipients to receive Nigerian government funds in exchange for advance fees.[56] The following is an excerpted summary of the content of these fraudulent emails detailing the scheme from Interpol:[57]

BOX 5.3 Prominent On Line Auction Fraud Cases

CASE #1 The CATCH Task Force successfully prosecuted Raj Trivedi for victimizing more than 700 individuals throughout the world with his Internet fraud scheme of advertising high-tech products, accepting payment, and then failing to deliver the merchandise advertised. Losses from these frauds were over $992,000. Trivedi victimized consumers who went to his Web site to purchase electronic equipment (e.g., computers and camcorders) that Trivedi advertised on the auction Web sites eBay, uBid, and Yahoo. In March 2002, Trivedi was sentenced to three years in prison and ordered to pay restitution to his victims, who averaged $1,200 in individual losses.

CASE #2 The case against Teresa Smith of Massachusetts represents one of the largest on line auction fraud schemes on record. Smith was the subject of over 300 individual complaints stemming from frauds occurring from April 2001 through October 2002. Her scheme was simple: She would defraud her victims by selling a computer, requiring them to pay up front, and then not sending any of the auctioned merchandise. Smith then refused any type of refund request. During the investigation it was discovered that Smith had spent the victims' money on living expenses, a new vehicle, and advertising costs associated with the scheme. Smith would change her on line identity any time complaints were reported against her. The scheme was finally detected after investigators uncovered over $800,000 in fraudulent proceeds. Smith is currently awaiting sentencing.

> The letters explain that the money is from delayed approved contract payments by the Nigerian administration to certain companies or individuals who have abandoned their claims. The letter alleges that the present military government is now paying these claims. The signatories claim to be acting as middle men and request that the victim supply signed and stamped blank company letterheads and invoices together with detailed account information so that monies can be transferred in advance of payment in order to pay taxes and bribe relevant officials in charge of the supposed proceeds. Obviously, no money is ever received, resulting in a total loss of bank deposits from the victim.

The IFCC received over 16,000 complaints about the scheme in 2002 alone. Largely as a result of this scheme, Nigeria ranks second behind only the United States in losses associated with Internet fraud schemes.[58]

Chain letter hoaxes and "urban legends" comprise another highly publicized and common form of Internet fraud. Chain letter hoaxes over the Internet are simply on line versions of age-old schemes designed to perpetuate the forwarding of e-mails. Often, these letters ask the recipient to forward the e-mail message to as many people that they can in exchange for a specified sum for each forwarded e-mail.[59] Chain letter hoaxes are typically less costly than other forms of on line fraud because the recipient is simply duped into believing that they will receive compensation that is not forthcoming. These hoaxes have included claims that prominent businesses will compensate recipients for forwarded emails, including Microsoft, Outback Steak House, Victoria's Secret, Newell Company, Nokia, Old Navy, and McDonalds, among others.[60] These claims are

BOX 5.4 Common On Line "Urban Legends"

Needles on Gas Pumps

Some persons have been affixing hypodermic needles to the underside of gas pump handles in the Jacksonville, FL area. These needles appear to be infected with the HIV virus. In the Jacksonville area alone there have been 17 cases of people being stuck by these needles over the past five months. We have verified reports of at least 12 other cases around the country . . . Evidently, the consumers go to fill their car with gas, and when picking up the pump handle get stuck by infected needles . . . IT IS IMPERATIVE TO CAREFULLY CHECK THE HANDLE OF GAS PUMPS EVERY TIME YOU USE ONE!

Cyanide-Laced Deposit Envelopes

I hesitate to be an alarmist, but if anything like this happened to one of my family or friends I would not be able to forgive myself for not passing this along . . . A woman died recently from licking the deposit envelope at a Bank of America ATM. It was laced with cyanide. Investigators stated that they went back to the ATM in question and found six other envelopes in the slot . . . Please, I implore you to use extreme caution when using those envelopes. The radio station advised that you should first spit on the envelope, and then close it . . . I know this sounds gross, but better gross than DEAD.

Poison Perfume Samples

I was sent an email at work about someone walking up to you at a mall parking lot and asking you to sniff perfume they are selling at cut-rate prices. This isn't really perfume but ether, and you will pass out and they will take your wallet and all of your valuables. This is not a prank e-mail. This is true! I could have very well been a victim. PASS THIS ALONG.

Rat Feces

A stock clerk was sent to clean up a storeroom at his work place. When he got back there, he was complaining that the storeroom was really filthy, and that he had noticed dried mouse or rat droppings in some areas . . . A couple of days later, he started feeling like he came down with a stomach flu, achy joints, and headache. He went to bed and never woke up. Within two days he was ill and weak. His blood sugar count was down to 66. He was rushed to emergency where he suffered from complete organ failure. He died shortly before midnight . . . There is a virus that lives in dried rat droppings (much like Hanta virus). Once dried, these droppings are like dust and can be easily digested. ALWAYS carefully rinse off the tops of any canned foods or soda . . . A family friend recently died from drinking a can of soda!

never true, because currently there is no software in existence that is capable of tracking the number of times that an e-mail is forwarded and then subsequently compiling a report back to a central tabulator.[61] So-called urban legends are myths designed to create a generalized panic among e-mail recipients. These messages typically entail grandiose claims of impending danger arising from commonplace activities. Box 5.4 details some of the more common urban legends currently circulating on line. Rest assured, none of the claims are true.[62]

The Computer Fraud and Abuse Act (CFA) has become the primary vehicle for the prosecution of Internet fraud crimes. The CFA was initially enacted by Congress in 1984, primarily as a means to protect classified information contained on government computers. The scope of the CFA was expanded in 1986, and again in 1996. The 1996 amendments to the Act worked to incorporate *all* computers that are involved in interstate and/or foreign commerce under the Act.[63] Essentially, the CFA covers most fraudulent business practices that are conducted over the Internet.

SUMMARY

This chapter has defined and described how the growth in computer technologies has affected five major criminal offenses, including embezzlement, money laundering, corporate espionage, identity crimes, and fraud. The traditional crimes of embezzlement and money laundering have clearly become more prevalent, and modern technologies have increased opportunities to commit both crimes. In terms of embezzlement, the computer has allowed individuals increased access to funds manipulation and has eliminated problems related to the material bulk of moving large quantities of cash. Money laundering is now easier because of two primary reasons: (1) electronic funds are easier to conceal while maintaining anonymity, and (2) the advent of "cashless" banking systems such as e-cash has made detection of such crimes much more difficult.

In addition, computer technologies have created a wide array of new avenues to the pilfering of corporate secrets, including trade technologies, research and development strategies, and customer lists. Computerized corporate data is easier to access, and the prevalent utilization of electronic mail in business environments has given corporate thieves expanded opportunities. So too, the end of the Cold War has created a cadre of former spies who can provide foreign firms the skills and expertise necessary for stealing domestic trade secrets.

Finally, the traditional crime of fraud has taken on new forms as a result of the information revolution. In particular, the Internet has increasingly been utilized as a platform to perpetrate fraud, especially in on line auction schemes, financial institution frauds, and the transmission of "urban legends."

REVIEW QUESTIONS

1. Identify and describe the similarities and differences between corporate espionage offenders who are "insiders" and those who are "outsiders."
2. What is the Bank Secrecy Act of 1970? How has the advent of computer technologies created ways around this act?

3. What are "urban legends"? How have these "legends" changed over the course of the last two decades?

ENDNOTES

1. Reiman, J. (1995). *The Rich Get Richer and the Poor Get Prison.* Boston: Allyn & Bacon.
2. Sutherland, E. (1940). "White-Collar Criminality." In *White Collar Crime: Classic and Contemporary Views.* G. Geis, R.F. Meirer, and L.M. Salinger (eds.). New York: Free Press (pp. 29–38).
3. Green, G.S. (1997). *Occupational Crime,* 2nd ed. Chicago: Nelson Hall.
4. Cressey, D.R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement.* Glencoe, IL: Free Press.
5. Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* Boston: Addison-Wesley.
6. Anderson, J.P. (1980). "Computer Security Threat Monitoring and Surveillance." James P. Anderson Co.: Fort Washington, PA.
7. *Ibid.,* 3.
8. Fiedler, T. (1999). "Man Admits Helping Himself to Raises; Embezzlement Trial is the First Computer Fraud Case to be Heard in Minnesota." *Star Tribune* (Minneapolis, MN), June 24.
9. Glod, M. (2002). "Ex-Fairfax Official Gets 14 Years in Theft." *Washington Post,* November 23.
10. Kane, D. (2002). "Millions Vanish Through Theft, Embezzlement at North Carolina Agencies." *Knight Ridder/Tribune Business News,* November 24.
11. Murray, T.D. and Caniglia, J. (2003). "Broker's Victims Start Over; Gruttaduria's Investors Still Hurting, Rules Not Changed." *Cleveland Plain Dealer,* February 16.
12. Hudson, J.E. III. (2002). "Trade Secret Theft Threatens Everyone with Corporate Espionage Escapades." *Houston Business Journal,* October 4.
13. Robinson, S.W. *Corporate Espionage 101.* SANS Institute, 2003.
14. Konrad, R. (2000). "Leaks and Geeks: International Espionage Goes High-Tech." *C/Net News.Com,* September 21.
15. *Ibid.,* 14.
16. *Ibid.,* 14.
17. *Ibid.,* 14.
18. *Ibid.,* 12.
19. *Ibid.,* 13.
20. *Ibid.,* 13.
21. *Ibid.,* 13.
22. *Ibid.,* 13.
23. Bowman, L.M. (2001). "Avant Ordered to Pay $182 Million." *C/Net News.Com.,* July 19.
24. Swartz, J. (1997). "Felony Charges Halve Avant's Stock." *The San Francisco Chronicle,* April 16.
25. Burrows, P. (1997). "A Nest of Software Spies?" *Business Week,* June 15.
26. *Ibid.,* 14.
27. *Ibid.,* 12.
28. Lyman, M.D. and Potter, G.W. (2000). *Organized Crime.* Prentice Hall: Upper Saddle River, NJ.
29. *Ibid.,* 28.
30. *Ibid.,* 28.

31. GRABOSKY, P.N. and SMITH, R.G. (1998). *Crime in the Digital Age.* The Federated Press: New Brunswick, NJ.
32. *Ibid.,* 31.
33. BORTNER, R.M. (1996). "Cyberlaundering: Anonymous Digital Cash and Money Laundering." Presented as a final paper at the University of Miami School of Law.
34. *Ibid.,* 33.
35. *Ibid.,* 33.
36. *http://fincen.gov*
37. *Ibid.,* 36.
38. *Ibid.,* 36.
39. LEASE, M.L. and BURKE, T.D. (2000). "Identity Theft: A Fast-Growing Crime." *FBI Law Enforcement Bulletin,* 69 (8).
40. *Ibid.,* 39.
41. HOAR, S.B. (2001). "Identity Theft: The Crime of the New Millennium." *USA Bulletin* (March).
42. *Ibid.,* 41.
43. *Ibid.,* 41.
44. *Ibid.,* 39.
45. *Ibid.,* 41.
46. Excerpted from HOAR, S.B. (2001). "Identity Theft: The Crime of the New Millennium." *USA Bulletin* (March).
47. (2002). Federal Trade Commission Bulletin. "Identity Theft: When Bad Things Happen to Your Good Name." (February).
48. *Ibid.,* 41.
49. *Ibid.,* 47.
50. (2003). IFCC 2002 Internet Fraud Report.
51. *Ibid.,* 50.
52. *Ibid.,* 50.
53. *Ibid.,* 50.
54. (2001). IFCC Internet Auction Fraud Report (May).
55. *Ibid.,* 54.
56. (2003). Professionals Against Confidence Crimes. "Interpol Warning: Nigerian Crime Syndicates Letter Scheme Fraud Takes on New Dimension."
57. *Ibid.,* 56.
58. *Ibid.,* 50.
59. *http://www.scambusters.org*
60. *Ibid.,* 59.
61. *Ibid.,* 59.
62. *Ibid.,* 59.
63. (2001). *GigiLaw.Com.* "The Expanding Importance of the Computer Fraud and Abuse Act."