CHAPTER 1

The Identity Theft Explosion

Imagine seeing a disaster unfold before your very eyes, one constantly growing larger and more destructive. It continually evolves to the changing environment and resists all attempts to blunt its impact. You and thousands of others try to stop this disaster, but all actions are futile. Despite all the warnings, you are powerless to do anything but observe the massive impact on individuals, organizations, and businesses. While I could easily be describing a major earthquake, hurricane, or tsunami, the actual culprit is a crime. But this is not just any crime. It is an extraordinary wrong that is more like an unstoppable force in its devastation. The crime is identity theft, and it has grown and evolved over the last 35 years to take on a relentless life of its own.

Identity theft is the fastest-growing financial crime in the United States and the world. Several years ago CBS News reported that someone's identity is stolen every 79 seconds. A Federal Trade Commission (FTC) survey in 2006 found that 8.3 million American adults were victims of identity theft. That same study estimated the total identity theft losses to be $15.6 billion, a figure significantly down from a similar FTC study in 2003 that found total losses to be $47.6 billion. Of note, the 2006 study indicated that changes in survey methodology may be the reason for the difference, rather than an actual drop in incidence levels.

Whatever the exact losses, the growth of identity theft has been striking. *Kiplinger's Personal Finance* magazine in its July 1995 edition reported that the credit reporting bureau Experian received 600 to 700 identity theft complaints each day. MasterCard International reported that identity theft represented 96% of member banks' fraud losses in 1997. Identity theft losses grew from $450 million in 1996 to over $2 billion in 1999.

According to the FTC, fraudulent use of credit cards accounted for 50% of all identity theft complaints in 2000. Identity theft complaints involving the misuse of Social Security numbers (SSNs) jumped from 27,000 in 1998 to 73,000 in 2002, according to the Social Security Administration.

As a result of stronger data-loss notification laws, more than 500 incidents of data breaches were reported between 2005 and the first half of 2007, involving more than 155 million records. The lost data came from the theft of laptops, intrusions by hackers, and general carelessness and disregard for data security. Breaches have affected government agencies, hospitals, financial services firms, and a host of other companies.[1]

WHAT IS IDENTITY THEFT?

During identity theft, criminals acquire key pieces of personal identifying information—such as name, address, date of birth, SSN, mother's maiden name, employment information, credit information, and other vital facts—in order to impersonate and defraud the victim. This information enables the thief to commit numerous forms of fraud, including taking over the victim's financial accounts; applying for loans, credit cards, and Social Security benefits; purchasing homes and cars; and establishing services with utility and phone companies.

Simply put, identity theft is the stealing of your good name and reputation for financial gain. Yet not everyone can agree on a suitable meaning of the term. The definition of this crime differs among law enforcement, regulatory agencies, and the many studies on this subject. The United States Postal Inspection Service states that "[i]dentity theft occurs when a crook steals key pieces of personal identifying information to gain access to a person's financial accounts."[2] The United States Secret Service calls it identity crimes and defines it as "the misuse of personal or financial identifiers in order to gain something of value and/or facilitate other criminal activity."[3]

The President's Identity Theft Task Force Report issued in April 2007 stated that "[a]lthough identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud."[4] The report goes on: "Criminals must first gather personal information, either through low-tech methods—such as stealing mail or workplace records, or 'dumpster diving'—or through complex and high-tech frauds, such as hacking and the use of malicious computer codes."[5] More detailed information on the Task Force Report can be found in Chapter 18.

The October 2007 study entitled *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement* issued by the Center for Identity Management and Information Protection at Utica College in Utica, New York provided detailed new research on identity theft. For a more detailed discussion of this study, please see Chapter 19. The study agreed with the President's Task Force that the fraudulent use of personal identifying information—name, address, SSN, date of birth—are elements of identity theft but fraud involving credit cards, debit cards, and ATM cards are not. The report stated: "While the theft of a credit card may result in fraudulent charges, it does not result in the theft of an identity."[6] The study went on to quote a line from the President's Task Force: "For example, a stolen credit card may lead to

thousands of dollars in fraudulent charges, but the card generally would not provide the thief with enough information to establish a false identity."[7]

I generally agree with these definitions but respectfully disagree with the idea that a theft of a person's credit card, including name and related credit card number, is not identity theft. I take a much larger and more victim-oriented view of identity theft. Therefore, I prefer the definition used by the Federal Trade Commission's Consumer Sentinel. Consumer Sentinel is an information sharing network that provides law enforcement with access to consumer complaints received by the FTC. Identity theft is "when someone appropriates your personal identifying information (like your Social Security number or credit card account number) to commit fraud or theft."[8] When a fraudster steals a victim's credit card, the criminal poses as that person, fraudulently using the name and linked credit card number to steal money and property that will be charged to the victim's account. Although the ultimate financial loss will be borne by the financial institution or credit card issuer, the true card holder is still a victim. There are various degrees of identity theft, but I do not think there is a single person who would not be outraged knowing that someone had stolen and used his or her credit card or other financial access device.

IT IS NOT ROCKET SCIENCE

It is very easy for criminals to obtain our personal information and our identities. Everything from low-tech to high-tech thievery is readily available. It seems that not a day goes by without hearing about another news story on identity theft. Due to this publicity, almost everyone knows about this crime. It has been called everything from credit card fraud to true name fraud to identity fraud to the Crime of the '80s, and since the mid-1990s, identity theft. It was called credit card fraud first because in the early days, it primarily involved the theft of personal identifying information for submitting fraudulent credit card applications. The stolen information came from a variety of sources: Dumpster diving; insiders at banks, credit bureaus, and the post office; mail theft from collection boxes and residences were but some of the ways the fraudsters obtained personally identifiable information.

The growth of credit card fraud paralleled the rise of credit card use in this country starting in the early 1970s. Once people began to accept credit card use and heavy marketing by the banking industry spurred their growth, fraudsters had a new avenue for their criminal enterprise. These criminals would steal personal information and apply for credit cards in the victims' names. I would like to say they were ingenious, but in reality it was pretty easy to do. They used simple means to obtain identity information because then as now, personal information, the keys to our personal vault, was so readily available.

The old standby of getting down and dirty in Dumpster diving has been effective whenever individuals or businesses do not safeguard information. Unfortunately that is all too often. Dumpster divers look in the trash for discarded credit card statements, canceled checks, preapproved credit card offers, medical records, mortgage applications, and any other documents that contain your name, address, date of birth, SSN, or other information. In the days before shredders were commonplace, fraudsters found mother lode after mother lode of personal information. And they still find gold today.

Mail theft is another valuable source of personal data for identity thieves. The beauty of the mail system is that Americans receive mail delivery to their homes and businesses six days a week, 52 weeks a year. There is a never-ending supply of bank and brokerage statements, credit card bills, convenience checks, credit card offers, and a wealth of other personal and financial information for identity thieves. We lock our homes, our cars, and our businesses to protect what is inside, but how many of us have a locking mailbox?

As Internet access gets faster and cheaper, more and more people worldwide use it for business and pleasure. Do you know anyone who does not have Internet access either at home or work? Very few, I would say. Fraudsters have found how easy it is to do business—fraudulent business—using the Internet. They use spam, phishing, pharming, vishing, hacking, planting malicious codes, and whatever new technology breakthrough they can exploit to steal passwords, financial information, and other identifying data. If you are not familiar with some of these terms, you will learn all about them in Chapter 3. The increasing reporting of large-scale data breaches are the result of these technology attacks as well as plain old human failure. Story after story involves laptops left unsecured in cars or hotel rooms without encryption. No wonder we have the problem we do; we make it so easy for identity thieves.

In the early 1980s, professionals such as lawyers, stockbrokers, physicians, and others with good credit ratings were likely victims. Fraudsters often applied for jobs as night watchmen, security guards, and cleaning people at major businesses, where at night they would have free access to search through personnel files, employees' desks, and other belongings to obtain names, home addresses, job titles, and SSNs for credit card fraud. They often passed this data to confederates throughout the country for further fraud. In 1985, identity thieves did just that when they infiltrated CBS News in New York City and stole personal information on hundreds of CBS employees, including famed news anchor Walter Cronkite and *60 Minutes'* Ed Bradley.

The crime began to evolve. Fraudsters subverted postal employees so that they would turn over mail containing credit cards. Identity thieves would infiltrate Social Security offices, banks, brokerages, and credit bureaus to fraudulently access victims' credit reports and then do credit card and bank frauds with the stolen identities. They used post office boxes to obtain fraudulently ordered credit cards. Postal Inspectors would arrest these identity thieves when they came to pick up the cards at post offices. They then began to use a new business industry called commercial mail receiving agencies (CMRAs) or mail drops to open mail boxes in the names of their victims and receive the fraudulently requested credit cards.

By the mid-1980s, this crime began to hit the media's radar screen. More and more victims complained to financial institutions and law enforcement. In 1982 and 1984, Congress enacted legislation that made access device fraud, including credit and debit card fraud, specific crimes. The United States Secret Service was given primary authority for the investigation of access device fraud. Postal Inspectors who had been working credit card frauds since the 1960s were now joined by Secret Service agents. Still the crime grew.

Identity theft has grown tremendously since those early years because criminals have found out how easy it is and how available personal information is. The associated

crimes currently include identity takeovers of company names, committing insurance fraud under stolen names of physicians, and stealing information from family home-pages and resumes found online. The Internet and online databases make obtaining personal information just a mouse click away.

THOUGHT LEADER IN IDENTITY THEFT INVESTIGATION

Edward Stroz

Following a 16-year career as a Special Agent for the Federal Bureau of Investigation, Edward Stroz founded Stroz Friedberg, LLC in 2000 and now serves as its copresident. Stroz Friedberg is a technical and consulting services firm specializing in digital forensics, e-discovery, and corporate investigations. Stroz has assisted clients in responding to Internet extortions, denial-of-service attacks, hacks and unauthorized access, and theft of trade secrets and has pioneered the concept of incorporating behavioral science into the methodology for addressing computer crime and abuse.

Stroz is an expert in addressing the threat of computer crime and abuse posed by insiders and has coauthored a book on the subject. He has supervised numerous forensic assignments for federal prosecutors, defense attorneys, and civil litigants and has conducted network security audits for major public and private entities. In 1996, while still a Special Agent, he formed the FBI's Computer Crime Squad in New York City, where he supervised investigations involving computer intrusions, denial-of-service attacks, illegal Internet wiretapping, fraud, money laundering, and violations of intellectual property rights, including trade secrets. Here Stroz provides his perspective on the evils of identity theft and fighting back:

Imagine you are at home having dinner with your family and you hear an unexpected knock on the door. You answer the door and meet two FBI agents who want to question you about threatening email messages that have been traced as having originated from your home. You find it hard to believe this could be true. However, in the interview with the FBI, it becomes clear that the wireless network in your home was hacked remotely by the true perpetrator to commit a crime by making threats and extortionate demands to people completely unknown to you. In essence, your identity and that of your household were compromised, and used to provide cover to an intruder. While not an everyday occurrence, I've seen this kind of identity theft scenario played out over my career in law enforcement and as a consultant.

Identity theft is essentially the theft of information. It's information "about you" as an individual person, and there is some reason that it would be valuable to a thief. That value could be purely monetary—as simple as the thief using your credit in order to buy things. But the value of your information may have nothing to do with money, as the scenario recounted above shows.

(Continued)

And there are other forms of identity theft. Using a stolen identity can allow a wanted person to evade capture, or a suspected terrorist to pass through a security checkpoint unrecognized in order to get on an airplane. I have been involved with computer hacking cases in which stolen identities were used to make it look as though someone else was behind the crime, and to get them in serious trouble.

Each of these examples represents different types of problems, and it's important to make distinctions among them. As with any type of fight, it is important to know something about your adversary. The different types of identity thieves can be categorized into "threat agent" profiles in order to fight this problem. The term "threat agent" is often used to describe the individual behind the attack and the method used to execute the attack.

The simplest type of identity theft is targeted against consumer credit/debit cards. These are often stolen in bulk (large computer files that contain numerous card numbers) and used a few times before being discarded. This activity is more of a "property crime," which, while serious, is sometimes more manageable. This is because stealing money or credit will show up right away in business records as there is a vendor alongside you in the fight. Within days or weeks, the unauthorized activity will show up on a credit card or bank statement, bringing the problem to light. While this represents a real problem, it is probably not the biggest threat to our society.

Identity theft for the purpose of actually assuming your identity in order to move through society unimpeded is different from that of stealing a credit card number, and is harder to fight. Here you are up against a smarter and more dedicated adversary, with much greater value to a threat agent in the form of a terrorist, than a property crime thief. Fighting that type of adversary is primarily done by law enforcement.

Nobody really knows where these problems will lead. Greater security almost always comes at the price of decreased convenience and privacy. The technologies with the least inconvenience will likely be in high demand. For example, retinal scans, already in use at some airports to speed people through security, will probably gain increasing acceptance as a form of biometric (something you "are") recognition. Fingerprint scanners are increasingly featured on laptop computers. It seems that opting in for biometrics as a form of protection is going to be the most useful technology for countering identity theft without inconveniencing people to an unacceptable level.

EARLY DAYS OF CREDIT CARDS

In the early years of credit card issuance, the cards generally had very low purchasing limits. Purchasing caps of $300 to $500 were not uncommon, and it usually took a formal application with a good payment history to raise a card's limit. Although American Express offered cards that appeared to have no spending limit, the balance could not be carried over and had to be paid off by the end of the billing cycle. American Express was much more selective with regard to potential customers than other card issuers, such as Visa, MasterCard, department stores, and gasoline companies.

Initially, credit card transactions were processed manually from the merchant making an imprint on the sale or charge slip at the store to reconciling slips at the bank and

posting charges to customers' accounts. Although a card might have a limit of $500, criminals would make multiple purchases under recognized floor limits, which they learned from trial and error. When financial institutions reconciled the charges at the end of the cycle, the total charges would far exceed the card's limit. It was not uncommon for small businesses to send in charges a month or more past the normal cycle. The store might wait until it had several charges to send in its charge slips, and this would delay the posting of the particular charges. So it might take several months to determine the true losses on the card. This manual process carried through the early days of automation as many smaller merchants were not "online." The online electronic process was gradually phased in and equipment became more affordable for smaller merchants.

As local banks began to issue their own cards and more banking functions became automated, far more cards were issued, including ones mistakenly linked to other accounts. San Diego–based Postal Inspector Phil Garn related a case where a doctor applied for a $50,000 loan for a piece of diagnostic medical equipment. The bank accidentally issued a card linked to the loan account with a $50,000 limit. This card was then stolen from the mail. The crook had no idea what the limit was and, luckily for the victim, only charged a few thousand dollars. Despite the low limits on credit cards, criminals were able to run up charges so quickly that they frequently far exceeded the card's limit. It was common to find cards with $500 limits but which had over $1,800 of fraudulent charges.

At this time, both newly issued cards and reissued cards were "live cards." They could be used immediately upon arrival. There was no activation procedure, either in person or on the phone, and there was no online banking. Most merchants manually ran the card through a device that embossed an imprint of the card onto a carbon sales slip that the customer had to sign. This turned out to be a great paper trail for investigators, not only for suspects' handwriting but for fingerprints. However, these copies rapidly disappeared as banks began to microfilm the slips and destroy the originals due to the sheer quantity of slips and physical storage limits. The microfilmed copies would preclude fingerprint analysis and make it hard to get a positive forensic identification on the handwriting.

Later, merchants would be able to make queries via telephone, and larger merchants would be able to run the card through their own magnetic card readers to get an authorization code. These codes became commonplace; however, at the time, the codes could also be manually overridden at the point of sale at the merchant's discretion and liability. If access to credit was denied, criminals would often engage in social engineering, telling the merchant a story about how their vindictive ex-spouse canceled their card or had intentionally reported it stolen.

The criminal would also demand to speak to the credit card company on the telephone at the store. The criminal would then put on a dramatic one-sided conversation, finally coming up with an authorization code, usually a sequence of letters and numbers, which he or she would provide to the merchant, who would write the number down on the charge slip and finish the transaction. Although this authorization code was not valid, it would appear to have a correct sequence of numbers and letters for the particular card being used. Magnetic credit card readers would eventually come down in price and become commonly used, as they are now. Today nearly every merchant has an electronic

credit card terminal for approving purchases. There is no doubt that today's technology has helped to significantly decrease fraud at the point of sale.

LIMITING LOSSES

Detection and prevention of credit card fraud were also very much on the minds of the credit card issuers. During these years, each card issuer, such as American Express, Visa, and MasterCard, would also issue lists of lost/stolen credit card numbers, typically printed in books similar to the size of telephone books. These warning lists allowed subscribing merchants to check the account number when the customer presented a card to make a purchase. It was a time-consuming process, as the type was very small and it was hard to find a suspect card's number in the endless pages of listed numbers.

Merchants did not always check the warning lists even though they would be liable for fraudulent charges. European merchants would hang on to this countermeasure for much longer than the United States. Criminals who stole bulk shipments of new or reissued credit cards in the United States would use the cards immediately after the theft and then send the cards in bulk to criminal associates in Europe, where the printed lost/stolen lists were at least a month behind. After charging purchases up to the cards' limits in Europe, the cards were sent to Asia, where they would be reencoded. It was not unusual for a stolen Visa card to be magnetically reencoded with a MasterCard account number and fraudulently used.

In the 1970s and 1980s, billing processes were far more manual and much slower than today. Electronic point-of-sale terminals had yet to come into existence. Charges would typically post during the following month and be mailed to a customer in a statement for a 30-day period, although it was not uncommon for some charges to show up 60 or 90 days later. This was due to merchants physically mailing in their sales slips and the increased time needed for processing and posting.

When unauthorized charges appeared, a lengthy process to dispute these charges could take months. Problems even could continue for years, as sometimes these unpaid balances were not removed from people's credit histories. Inspector Garn relates how he would often get panicked calls from victims six to 18 months after he first talked to them about their stolen credit cards. The victims had filed affidavits of forgery and had cleared their accounts with the financial institutions but were now trying to buy a car or close on a house. Unfortunately, the fraudulent charges still appeared on their credit records.

Even though victims may have cleared one fraudulently used card, criminals often applied for additional cards or utility services in the names of the victims. These new cards would be sent to another address controlled by the fraudsters; then after use and nonpayment, the account would appear as unpaid and delinquent. After hearing from the first few panic-stricken callers, Inspector Garn would tell victims to check their credit histories on an ongoing basis to see if any additional charges appeared. He often felt helpless in not being able to do more for these victims; even arresting the scammers did not stop the credit problems.

Customers were also responsible for the fraud charges or some portion of them, until lawsuits and public opinion caused banks to change their policies. It became highly embarrassing when victims who had an average monthly balance of a few hundred

dollars and a history of on-time payments could show the news media thousands of dollars charged in a few days, all obvious fraud. Financial institutions also found they could pass the losses off to their customers in the form of higher interest rates. It was not until the losses from fraud cut into the banking institutions' profits that changes occurred and proactive fraud prevention became routine.

In the early 1980s, a bank investigator for a major financial institution in New York decided that he would create his own fraud detection process for the increasing number of fraudulent credit card applications his bank was receiving. These applications were being submitted using stolen identities and contained the names, birth dates, Social Security numbers, and employment histories of the victims. This bank investigator correctly assumed that the bulk of these thousands of fraudulent applications were being submitted by members of Nigerian Criminal Enterprises who were a plague on the credit card industry at the time.

At this point, credit card applications were completed by hand and mailed in for processing. After finding that the fraudsters had a very distinctive style of handwriting, this investigator began to manually review each submitted application looking for these handwriting characteristics. They included the signature being underlined, periods on both sides of middle initials in names, period after signatures, reversal of first and last names, European-style date, a colon used in place of decimals, dashes or slashes, letters A and E connected to the next letter, dashes between names or nouns, as well as other misspelled words and strange abbreviations. Although this process by itself was not totally conclusive as to the existence of fraud, this investigator was very successful in identifying suspect applications that needed additional scrutiny.

Both federal and state authorities would investigate and prosecute identity theft—although it was yet to have that name—but many considered the fraud a "victimless" crime. Banks and credit card issuers ultimately made the individuals whole for fraud losses. When I was working these cases in Brooklyn, New York, a federal prosecutor told me that he would not accept any credit card fraud cases for prosecution unless I could specifically detail the prevention efforts in place by the victim financial institution. This prosecutor felt that the banks were not doing enough to stop identity theft and that they were using law enforcement to fix the problem. I went back and told this to the bank investigators I was working with. Some banks had excellent prevention efforts; others sadly did not.

I remember making a prevention recommendation that was quickly rejected as cost prohibitive. The fraudulent credit card applications submitted by criminals contained stolen identity information, but one piece of information could be used to quickly determine the validity of the application. To ensure that an application would be approved, the thieves would include the victim's actual employer but would substitute a telephone number controlled by the suspect for the actual work number. This was done so that when a credit card issuer called to verify employment, the fraudster or his accomplice would verify employment. I recommended that when verifying the credit card application, a call be made to the named employer asking to speak directly to the named employee but not using the telephone number on the application. Instead, the employer's number would need to be obtained through the telephone directory or calling Directory Assistance. The financial institutions advised me that while my

suggestion was sound in theory and would quickly determine if a person had submitted the application in question, the extra steps and time would be financially burdensome.

There were many prosecutions in the early years, but the jail sentences were not significant enough to have a deterrent effect. The crimes continued to grow. As a consequence, although criminals were apprehended and successfully prosecuted, offenders did not receive long prison sentences, and the lure of the money brought on recidivism. A felony or even a misdemeanor conviction would have a major impact on an average person, but the short sentences the fraudsters received sent a clear message to recidivists that identity theft was extremely profitable.

JAIL ORDER FRAUD

There are always opportunities for creative and resourceful criminals to fleece an unsuspecting public. For those hardened fraudsters focused on committing identity theft, even confinement in a prison was not a barrier to committing this crime. During the summer and fall of 1981, Ricky Lee Bishop and Howard A. Jones were inmates at the Pulaski County Prison Farm in Virginia. Bishop was in prison on unrelated credit card fraud charges, serving a three-year sentence. Jones was a frequent prison guest with a history of criminal offenses including Grand Larceny and Obtaining Money by False Pretenses. Due to good behavior in prison, both Bishop and Jones were participating in a weekend furlough program where they were permitted to return home on Saturdays and Sundays.

Prison did not stop the pair from returning to a life of crime. While serving their sentences, Bishop and Jones were able to obtain the credit card numbers of people who had stayed at the Red Carpet Inn in Pulaski. Prisoners assigned to work on garbage collection details with the Pulaski County Sanitation Department obtained the stolen credit card numbers from the inn, one of the stops for the garbage pickup. The inmates would go through the trash at the hotel and recover discarded credit card receipts. It was believed that this was how Bishop and Jones found the credit card numbers used for the fraud.

Back in 1981, multiple part credit card slips with carbon paper inserts were used for sales transactions. The slips contained the purchaser's name, credit card number, expiration information, and signature. Often merchants discarded the slips after the transactions were completed. Fraudsters quickly found that Dumpster diving was a simple and easy way to obtain personal information for fraudulent purposes. It worked for these two inmates; it is no different today for those who fail to properly shred documents containing pertinent information.

After obtaining the credit card numbers, Bishop and Jones ordered merchandise by telephone from various companies located in Richmond, Chicago, Atlanta, Dallas, and Decatur. One of the companies was Best Products, a now-defunct chain of catalog sales and retail stores that was located in Richmond, Virginia. The inmates used the addresses of girlfriends and relatives as the delivery addresses for the merchandise. They would then arrange to pick up the packages on weekends when on furlough. On several occasions, Bishop would personally return the merchandise to Best Product stores located in Roanoke and Lynchburg for cash refunds.

The case was investigated by the Postal Inspection Service. The scheme lasted from July to November 1981 and Bishop and Jones received only about $4,400. The defendants used telephones to order the merchandise and the mails were used to ship the merchandise. As a result, they were charged with federal violation of Wire Fraud, Mail Fraud, and Use of Fictitious Names. Both defendants pleaded guilty in October 1982, and each received three additional years to their existing prison sentences.

There are lessons to learn from this case. Although the amount of the fraud was relatively small, and the individual credit card holders did not suffer any losses, there still was an impact. The credit card holders needed to close out their accounts and obtain new ones. The true card holders did nothing wrong yet were subject to this crime because the motel owners discarded the credit card slips. The simple act of shredding the slips would have prevented the possibility of this crime occurring. But in those years few people thought of destroying personal and financial information. There will always be hidden opportunities for criminals to defraud society. It is up to us to remove those opportunities through increased vigilance and prevention.

IDENTITY THEFT WAS NOT A HIGH PRIORITY

The owner of an alternative press wrote in 1981 that "[t]he supposed problem of 'ID fraud' generates low-level interest among law enforcement people, both state and federal. The prevailing attitude among prosecutors, born out of practice, is that laws are already in existence to combat the types of crimes associated with false ID."[9] To most people, this opinion was the correct one. It was also perceived this way because relatively small numbers of consumers had been victimized by this crime. Yet the crime was still in its infancy.

The time period between the late 1960s and early 1980s saw the birth and growth of a new crime. It was just beginning to spread and evolve to a more damaging offense. The years to come, from the mid-1980s through the new millennium, would see an explosion of identity theft that would burn the existence of this crime into everyone's mind.

NOTES

1. Byron Acohido and Jon Swartz, "Credit Bureaus Fight on State, Federal Levels against Freezes," *USA Today*, June 26, 2007, 1B.
2. United States Postal Inspection Service, Publication 280 (August 2003), www.usps.com/postalinspectors/pub280txt.htm.
3. United States Secret Service, *Financial Crimes*, www.ustreas.gov/usss/criminal.shtml.
4. President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (April 2007), 2, www.idtheft.gov/reports/StrategicPlan.pdf.
5. Ibid.
6. Gary R. Gordon, Donald J. Rebovich, Kyung-Seok Choo, and Judith B. Gordon, *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, Center for Identity Management and Information

Protection, Utica College, Utica, NY(October 2007), 10, www.utica.edu/academic/institutes/cimip/research.cfm.

7. President's Identity Theft Task Force, *Combating Identity Theft*, 3.
8. Federal Trade Commission, Consumer Fraud and Identity Theft Complaint Data, January–December 2007, February 13, 2008, 74, www.ftc.gov/opa/2008/02/fraud.pdf.
9. Barry Reid, *The Paper Trip II* (Fountain Valley, CA: Eden Press, 1985), 5.