

Identity Theft

Concepts and Issues Paper

March, 2002

I. INTRODUCTION

A. Purpose of the Document

This paper is designed to accompany the *Model Policy on Identity Theft* developed by the IACP National Law Enforcement Policy Center. This paper provides essential background material and supporting documentation to provide greater understanding of the developmental philosophy and implementation requirements for the model policy. This material will be of value to law enforcement executives in their efforts to tailor the model to the requirements and circumstances of their community and their law enforcement agency.

B. Background

At the 2001 IACP Annual Conference, identity theft was recognized as one of the fastest growing crimes in the 21st century and has become a major problem in the United States. With the continuing development in technology, it has become more widespread and more difficult to counteract. A strong law enforcement response is essential in order to arrest and prosecute perpetrators. This concept and issues paper and the model policy on which it is based are designed to assist police departments in understanding and identifying the protocols for accepting, recording, and investigating identity theft.

Identity theft is the wrongful use of another's personal information, such as credit card numbers, Social Security number, and driver's license number to commit fraud or another form of deception. This is usually done for monetary gain, although there may be other motives.

Identity theft has become a major problem in the United States. The target of identity theft is information that will enable the thief to assume the another's identity for a criminal purpose. In the last few years, personal information has become one of the commodities most sought after by criminals in this country and elsewhere. Because it is usually part of a larger criminal enterprise, the theft of personal information is one of the most serious of all crimes.

On May 31, 2001, the Washington Post reported:

Some law enforcement officials and regulators say identity theft has become one of their most pressing problems. The federal Office of the Comptroller of the Currency recently estimated that

there are half a million victims of identity theft per year in the United States. The Justice Department told Congress last week that Internet fraud, including identity theft, is one of the nation's fastest-growing white-collar crimes. And James G. Huse, Jr., the Social Security Administration's inspector general, testified that the misuse of Social Security numbers in fraudulent activity is "a national crisis."¹

Although identity theft is in itself a criminal act under both federal and most state laws, the theft is almost always a stepping stone to the commission of other crimes. Typical crimes associated with identity theft include credit card fraud, bank fraud, computer fraud, Internet fraud, fraudulent obtaining of loans, and other schemes designed to enable the perpetrator to profit from the original theft. Often, there are several types of fraud involved in, or resulting from, the initial identity theft. Furthermore, funds obtained illegally as a result of the identity theft and its resultant frauds may be used to finance other types of criminal enterprises, including drug trafficking and other major forms of criminal activity.

The escalation of identity theft in the United States is due in large part to the technology revolution that has brought the country into the so-called Information Age. The vastly expanded use of computers to store personal data and the growing use of the Internet have provided criminals with new incentives and new means to steal and misuse personal information. As the use of technology to store and transmit information increases, so too will identity theft. Consequently, identity theft will likely become an even greater problem in the future.

Financial Losses. Efforts to accurately define the financial losses of the vast number of crimes committed by means of identity theft are not possible at this time. Many identity theft crimes are not reported to police, and there is no single source of information on this issue. The U.S. Secret Service, the U.S. Postal Inspection Service, and the FBI among principal federal enforcement agencies share jurisdiction for investigation of these crimes. This does not include the thousands of reports and investigations that are handled by state and local authorities. It is fair to say, however, that the cumulative financial losses from identity theft and the various crimes that feed from it are staggering.

Financial loss statistics generated by investigations handled by the U.S. Secret Service's financial crimes division in fiscal year 2000 reveal total actual losses in closed identity theft cases totaled

\$248.1 million. However, the potential losses from identity theft cases discovered during the same period are estimated at nearly \$1.5 billion. Further, it is calculated that the average actual loss in each closed identity theft case in fiscal year 2000 was \$46,119.² These figures graphically illustrate the magnitude of the problem caused by identity theft in America today.

Personal Costs. Perhaps even more tragic than the monetary loss is the personal cost of identity theft. Because identity theft by definition involves the fraudulent obtaining of funds in the name of someone else, the victim of identity theft may sustain not only great financial loss, but also severe damage to credit standing, personal reputation, and other vital aspects of the victim's personal life. For example, the victim may suffer garnishments; attachments, civil lawsuits, and other traumatic consequences stemming from the identity theft. In some cases the victim may be forced into bankruptcy, further damaging his or her reputation and credit. In other instances, the victim may become subject to criminal prosecution because of crimes committed by the perpetrator of the identity theft in the victim's name.

Even if the victim ultimately clears his or her credit records and avoids other personal and financial consequences of identity theft, the physical and mental toll on the victim can be significant. Typically, a victim of identity theft will spend months or years trying to clear his or her credit records. Many hours of difficult and stressful effort are often necessary, because the merchants and institutions that have been defrauded in the victim's name are not easily persuaded that the victim is innocent of any wrongdoing. The frustration and distress engendered by this heavy burden often takes a significant toll on the mental well being and physical health of the victim. And, worst of all perhaps, the victim's efforts to clear him or herself may be unsuccessful, leaving the victim under a cloud for the rest of his or her life.

C. Victimology

Virtually anyone may become the victim of identity theft. Contrary to popular misconception, personal information is not stolen just from the affluent. Persons of even modest means may become victims of identity theft. In most cases all that is required is good credit, which is what identity thieves use to steal thousands upon thousands of dollars in the name of the victim.

No particular age group is immune from identity theft. Federal Trade Commission data indicates that while 6.2 percent of individuals reporting identity theft to the FTC during the period from November 1999 to March 2001 were age 65 or over, the average age of victims was 42 years, and the most commonly reported age was 33 years.³ Younger Americans may be victimized at a higher rate because they are more likely to use the Internet, which is the primary tool in many identity theft crimes. However, elderly Americans are highly vulnerable to other types of identity theft schemes, particularly the various telephone scams used by perpetrators to acquire personal information.⁴ The elderly have always been targeted by perpetrators of fraud and will no doubt continue to be frequent victims.⁵

The victims of identity theft may be residents of almost any geographical area. The Federal Trade Commission reports that between November 1999 and March 2001, complaints of identity theft were received from all 50 states and the District of Columbia. According to the same data, the largest number of complaints came from California, New York, Texas, and Florida. The highest concentration of complaints per 100,000 people reportedly came from the District of Columbia, Nevada, Arizona,

California, and Maryland. The FTC also reports that the cities with the largest number of complaints were New York City, Chicago, Los Angeles, Houston, and Miami, in that order. However, one should not conclude from this that identity theft is confined to any particular city, state, or region. The problem is national in scope, and not even the residents of the smallest locality of the least populous states are safe from it.

D. Statutes

Identity theft was not a federal crime until Congress passed the Identity Theft and Assumption Deterrence Act of 1998.⁶

*This statute makes it a federal offense when any person 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 felony under any applicable state or local law.*⁷

This crime carries a maximum penalty of 15 years' imprisonment, a fine, and criminal forfeiture of personal property used to commit the offense.

Although this provision specifically targets identity theft, identity theft usually is part of a larger criminal scheme and generally involves other federal statutes, such as statutory prohibitions against credit card fraud⁸, computer fraud⁹, mail fraud¹⁰, bank fraud or wire fraud.¹¹

As of June 2001, 43 states had also enacted statutes making identity theft a crime.¹² Other states are considering passing similar laws. These statutes impose varying penalties for identity theft. Typically, they base these penalties on the dollar amount of loss resulting from the theft: thefts involving small losses are treated as misdemeanors, while larger monetary losses are usually considered felonies of varying degrees.¹³

Local law enforcement officials should check to determine whether they have such a statute and what that statute provides. Online access to these statutes is available through the Internet.¹⁴

E. Role of Federal Investigative Agencies

Investigation of identity theft cases may be conducted by a number of federal agencies, including the Federal Bureau of Investigation, the U.S. Secret Service, and the U.S. Postal Inspection Service. The federal agency that assumes primary jurisdiction and the lead investigative role over identity theft cases and resultant crimes depends upon the nature and method of the theft. For example, the Secret Service investigates matters involving credit card fraud, bank fraud, computer fraud, and Internet fraud, while the Postal Service investigates cases involving the use of the mails. However, since identity theft and its resultant crimes often involve a wide variety of offenses and means of committing those offenses, there is often significant overlap and interaction between these agencies. These federal agencies already have jurisdiction over matters within their particular sphere that is often the product of identity theft, such as mail fraud and bank fraud. However, passage of the Identity Theft and Assumption Deterrence Act in 1998 gave these federal investigative agencies additional scope to pursue identity thieves, since under that statute identity theft itself is now a federal crime.

F. Federal Trade Commission

The Federal Trade Commission (FTC) is the federal government's principal consumer protection agency, with broad jurisdiction extending over nearly the entire economy, including busi-

ness and consumer transactions on the telephone, the Internet, and elsewhere. The FTC's mandate is to prohibit unfair or deceptive acts or practices and to promote vigorous competition in the marketplace. The FTC act authorizes the Commission to halt deception in several ways, including through civil actions filed by its own attorneys in federal district courts. Of particular importance in the realm of identity theft is the fact that the Act also gives the FTC jurisdiction over cross-border consumer transactions. Many identity theft enterprises operate outside the borders of the United States.

Of particular importance here are the provisions of the federal Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §1028, which gives the Federal Trade Commission a substantial role in the campaign against identity theft. Under the act, the FTC is empowered to act as a nationwide clearinghouse for information related to identity theft crimes. This is an important aspect of the effort to combat identity theft, for in the past one of the major factors that hampered detection, investigation, and prosecution of these cases was the lack of any central source of information about identity theft. Identity theft is widespread and a single identity theft ring may operate over great distances and in many states. Consequently, the availability of a central database is essential to enable law enforcement agencies to identify organized or widespread identity theft operations and facilitate cooperation between appropriate federal and state agencies. Special agents from the federal enforcement branches previously mentioned work closely with the FTC in this regard.

In accordance with the mandate of the Identity Theft and Assumption Deterrence Act of 1998, the Federal Trade Commission has established a number of central resources to provide information to law enforcement agencies about identity theft crimes. They also provide guidance to victims of identity theft in order to help them defend themselves against the effects of this crime.

II. POLICY RECOMMENDATIONS

A. Steps to Prevent Identity Theft

One of the steps the FTC has taken to combat identity theft is to establish the Identity Theft Hotline. Victims and potential victims of identity theft may telephone this hotline by calling 1-877-IDTHEFT (1-877-438-4338) to report identity thefts. Victims who call the hotline receive telephone counseling from specially trained personnel to help them resolve credit-related problems that may result from the misuse of their identities. In addition, the hotline counselors enter information from consumers' complaints into the Identity Theft Data Clearinghouse—a centralized database used to aid law enforcement and prevent identity theft. The hotline has been in operation since November 1999.

About 40 percent of consumers who call the FTC identity theft hotline inquire about how to guard against identity theft. The counselors suggest steps and measures that consumers can take to minimize their risk. This information has been developed from the commission's extensive experience in advising consumers on how to avoid credit and charge card fraud and maintain financial privacy. Counselors recommend the following to consumers and crime victims:

- Never reveal your personal identifying information unless you know exactly who you are dealing with and how it will be used.
- Verify the details with any government agency that's involved in an offer or a proposed plan. The phone numbers for every government agency are located in the blue pages of the

telephone directory.

- Read all your bills carefully. Call your creditors to dispute any charges you didn't make or authorize.
- It's a good idea to order a copy of your credit report from each of the three major credit reporting agencies every year to check on their accuracy and whether they include only those debts and loans you've incurred. This could be very important if you're considering a major purchase, such as a house or a car. A credit bureau may charge you up to \$8 for a copy of your credit report.

While these recommendations may appear obvious to the informed individual, it may not be surprising how often the average consumer breaks these rules. Paying bills from credit card companies and related creditors without reviewing invoices is not unusual and it is this failure of vigilance that is often counted on by those who are involved in identity theft. It is also the reason many identity theft crimes are not discovered by the victim and reported to the authorities until long after substantial financial loss has been incurred. These and related hints are useful to local law enforcement officers and agencies to promulgate within their communities during community forums, in radio and television public service announcements, and by other means in crime prevention efforts.

Consider the following as a case in point of consumer failures to abide by the foregoing advice.

According to the FTC, elderly African Americans have been targeted in various parts of the United States for identity fraud schemes through advertisements to secure monies due them under a so-called Slave Reparation Act, allegedly passed recently by Congress. Flyers circulated in many southern and mid-western African American communities attempt to trick people in to revealing their personal identifying information by claims that they can receive \$5,000 in Social Security reimbursements under the alleged act. The flyers, distributed in churches or placed on the windshields of parked cars or on bulletin boards in senior centers and nursing homes, claim that African Americans born before 1928 may be eligible for slave reparations under the so-called act, and that those born between 1917 and 1926 can apply for Social Security funds they are due because of a "fix" in the Social Security system.

These claims of reparations are false, and this fact could be verified by potential victims through contact with the local Social Security office. But, this ploy has been, and continues to be, used by skilled identity thieves who ask victims for their name, address, phone number, birth date, Social Security number, and related information in order to access their credit cards or open accounts under their names without their permission or knowledge.¹⁵

Another 60 percent of consumers who call the FTC identity theft hotline have already become victims of this crime. In these cases, the counselors give victims specific information about preventing additional harm to their finances and credit histories.

Again, law enforcement officers are well advised to be aware of the suggestions of the FTC in this regard so that they can properly investigate the crime, take accurate and complete reports, make proper referrals to state and federal agencies, and provide victims with some basic information, advice, and support.

For example, FTC counselors suggest the following to victims of identity theft:

- File a report with the police immediately. Get a copy of the case number should your bank, credit card company, or insurance company need proof of the crime. (It is important to note

here that all police agencies should be prepared to take identity theft reports in addition to any other actions that may be taken, such as referral to the FTC hotline. More than a third of victims who attempt to make such reports to their local law enforcement agency indicate that local authorities will not take a consumer-victim report of identity theft.)

- Cancel each credit and charge card. Get new cards with new account numbers.

- Call the fraud departments of the three major credit reporting agencies: Equifax (1-800-525-6285, www.equifax.com), Experian (1-888-397-3742, www.experian.com), and TransUnion (1-800-680-7289, www.tuc.com). Ask them to put a fraud alert on your account and add a victim's statement to your file requesting that creditors contact you before opening new accounts in your name. (A fraud alert is a statement or numeric code that appears on a consumer report to alert potential creditors that the consumer has reason to believe he or she is a victim of fraud.)

- Ask the credit bureaus for copies of your credit reports. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. In a few months, order new copies of your reports to verify your corrections and changes and to make sure no new fraudulent activity has occurred.

- Report the loss to your bank if bank cards or checking account information may have been stolen. Cancel existing checking and savings accounts and open new ones. Get a new ATM card, account number, personal identification number (PIN), and password, if applicable. Stop payments on outstanding checks, and contact those creditors to explain the reason for stopping payment and to make other arrangements to pay the bills.

- If you have a passport, notify the passport office to be on the lookout for anyone ordering a new passport fraudulently.

- Check with the state motor vehicle department if your driver's license number was potentially included in the identity theft. If the state uses your Social Security number as your driver's license number, request that a new identification number be substituted.

- Change the locks on your house and car if there is any indication that, by loss or other means, these may have been copied or otherwise compromised.

- If you discover that an identity thief has changed the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes be made on the account.

- Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers. Avoid the same information number when you create a Personal Identification Number (PIN).

- Keep a chart of your course of action in terms of reporting the fraudulent use of your identity. Be sure to keep track of the credit bureaus you've contacted along with the date contacted, contact person and any comments. Other areas to record include the bank and credit card issuers and any law enforcement authorities you've reported your case to.

The counselors also advise consumers to review carefully the information on the reports to detect any additional evidence of identity theft. Consumers are informed of their rights under the Fair Credit Reporting Act and given the procedures for correcting misinformation on their credit reports.

Law enforcement officers can also inform victims and concerned citizens that counselors at the FTC hotline will be able to advise them of their rights under the Fair Credit Reporting Act.

They will also provide information on procedures for correcting misinformation on their credit reports, their rights under the Fair Credit Billing Act and the Truth in Lending Act, which, among other things, limits their responsibility for unauthorized charges to \$50 in most instances. Consumers who have been contacted by a debt collector concerning debts incurred by the identity thief are advised of their rights under the Fair Debt Collection Practices Act, which prescribes debt collector's practices.

Lastly, where investigation and resolution of the identity theft falls under the jurisdiction of another federal agency that has a program in place to assist consumers, callers are referred to those agencies. For example, consumers who complain that someone has been using their Social Security number for employment are advised to report this to the Social Security Administration's fraud hotline and to request a copy of their Social Security statement to verify its accuracy.

Complaints may also be filed via the Internet at the FTC's identity theft Web site, www.consumer.gov/idtheft, which also provides tips for consumers about combating identity theft.

B. Additional Resources for Law Enforcement

The Web site mentioned above, www.consumer.gov/idtheft, also provides law enforcement agencies with reports of recent identity theft cases and schemes, and information on state identity theft laws. In 1997, the FTC established Consumer Sentinel as a Web-based law enforcement network. This network provides law enforcement agencies in the United States, Canada, and Australia with secure, password-protected access to more than 300,000 consumer complaints about telemarketing, direct mail, and Internet fraud. Law enforcement agencies can search the database by such criteria as the name, address, and telephone number of a firm, the type of fraud, and the country and state or province of the consumer.

One part of Consumer Sentinel that is accessible only to law enforcement officials provides consumer complaint data and other intelligence about particular perpetrators. This enables users to share information, avoid duplication of efforts, and formulate rapid responses to new fraud schemes.

Building on the success of Consumer Sentinel, and as part of overall efforts to combat cross-border identity and related consumer fraud, the FTC recently established www.econsumer.gov in conjunction with 12 other countries. This program allows law enforcement personnel from around the world to access a database on consumer complaints specifically about cross-border Internet transactions. Law enforcement agencies from participating countries may access the complaint database through a password-protected Web site and allow government officials to communicate with consumer protection law enforcers from other countries, to notify each of ongoing investigations and information on recent actions.

The Identity Theft Clearinghouse offers law enforcement agencies direct Internet access to consumer complaints about identity theft. Using the clearinghouse, police departments and other law enforcement agencies may find victims and perpetrators of identity theft, link reports of identity theft that might otherwise look like isolated events, and identify other federal, state, or local agencies involved in a particular investigation.¹⁶

This same service also helps law enforcement identify overall trends in identity theft.¹⁷

The FTC produces a number of publications that provide information to consumers, victims, and law enforcement agencies about identity theft. These publications include the booklet

ID Theft—When Bad Things Happen to Your Good Name, published February 2001, and Identity Theft Complaint Data, Figures and Trends on Identity Theft, November 1999 through March 2001. Both of these publications are useful for community crime prevention programs as well as for officer awareness training.

Other federal agencies participate in the efforts to combat identity theft. For example, the Social Security Administration maintains a fraud hotline (1-800-269-0271), and identity theft cases involving theft or misuse of Social Security numbers are investigated by the Social Security Administration's Office of the Inspector General. In addition, information and assistance may be provided to victims by such agencies as the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation.

A number of federal agencies sponsor periodic identity theft workshops, conferences where identity theft awareness, education, prevention, and enforcement are discussed. Agencies sponsoring these workshops include the Federal Trade Commission, the Department of Justice, the Secret Service, and the Social Security Administration.

C. Role of Local Law Enforcement

In earlier years, the involvement of local police departments in identity theft cases was typically minimal. This was caused by several factors, including the lack of state laws making identity theft a crime, the fact that most identity theft operations are multi-jurisdictional enterprises, with perpetrator and victim usually widely geographically separated, and the general lack of police expertise in investigating the crime of identity theft.

Fortunately, this situation is now rapidly being remedied. The passage of numerous state statutes has given state and local police authority to investigate and prosecute identity theft crimes, and departments everywhere are becoming more aware of the significance of identity theft and the availability of the means to combat it.

The importance of police involvement in the effort to combat identity theft is reflected in a Resolution recently adopted by the International Association of Chiefs of Police. This resolution reads in part:

*RESOLVED, that the International Association of Chiefs of Police calls upon all law enforcement agencies in the United States to take more positive actions [regarding] incidents of identity theft. . . .*¹⁸

D. Types of ID Theft and ID Theft Operations

We have already examine some of the national resources available for combating identity theft and alluded to the types of crimes that are committed as part of identity theft. In this section we will take a closer look at the various types of identity theft schemes and the nature and modus operandi of the identity theft perpetrators.

As has been noted, the key target of identity theft perpetrators is personal and confidential information of individuals. There are so many methods by which identity thieves may acquire personal information that it is impossible to catalog them all here. However, the following methods are commonly used:

- Stealing wallets and purses containing personal identification, credit cards, and bank cards.
- Stealing mail, including mail containing bank and credit cards statements, preapproved credit card offers, telephone calling cards, and tax information.
- Completion of a false change-of-address form to divert the

victim's mail to another location.

- Searching trash for personal data (a practice known as dumpster diving) found on such discarded documents as so called preapproved credit card applications or credit card slips discarded by the victim. To thwart an identity thief who may pick through your trash to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards, and credit offers you get in the mail.

- Obtaining credit reports, often by posing as a landlord, employer, or other person or entity that might have a legitimate need for, and right to, credit information.

- Obtaining personal information at the workplace or through employers of the victim.

- Discovering personal information during physical entries into the victim's home. Such entries may be unlawful, as in burglary, or initially lawful, as when friends, service personnel, or others are invited to enter the home.

- Obtaining personal information from the Internet. This may be information stolen by hackers or freely provided by the victim in the course of making purchases or other contacts. Many victims respond to unsolicited e-mail (spam) that requests personal information.

- Purchasing information from inside sources such as store employees, who may for a price provide identity thieves with information taken from applications for goods, services, or credit.¹⁹ At least one instance has been reported of an employee of a credit bureau collaborating with identity thieves to provide personal information from credit bureau records.

- *Pretexting*, in which a thief telephones the victim or contacts the victim via Internet and requests that the victim provide personal information. For example, the thief may claim to be from a survey firm and ask for personal data. Another scheme is for the thief to claim that the victim has won a prize or been selected for some special honor or privilege which requires that the victim provide personal information. Still another means of theft is for the perpetrator to call the victim and pretend to have found something that the victim has lost and then demand that the victim provide personal information in order to obtain the return of the lost item.²⁰

- *Shoulder surfing*, a practice whereby the thief positions himself or herself near a victim in order to obtain personal information by overhearing the victim or seeing the victim's actions. For example, the thief may stand near a pay telephone in a public place and listen as the victim gives telephone credit card number information or other personal information in the course of making a call. Similarly, thieves may loiter near an automated-teller machine (ATM) and visually observe the victim keying in password numbers on the machine.²¹

- "Skimming," which is the electronic lifting of the data encoded on a valid credit or ATM card and transferring that data to a counterfeit card. There are many variations of this practice. For example, an identity thief may recruit an employee of a retail store, restaurant, or other retail establishment. The employee is provided with a hand-held electronic device that can read data from a person's credit card when the consumer presents it to the employee. The collusive employee then surreptitiously "swipes" the credit card through the hand-held "reading" device, which records the electronic data from the card. The employee then returns the device to the thief and the thief extracts the recorded data from the device.²²

- Identity thieves may also purchase personal information about potential victims from persons or entities that routinely

collect such information. In some instances these entities may be legitimate, but in many cases they are criminal enterprises formed for the specific purpose of selling information to thieves.

E. How Stolen Information is Used

There are literally hundreds of ways in which identity thieves may use the information they have stolen. The following are just a few examples:

- Once they have a victim's credit card number, thieves may call the victim's credit card issuer and, pretending to be the victim, asks that the mailing address on the account be changed. The thieves then run up high charges on the credit card, and because credit card statements are no longer being sent to the victim's real address, the victim might be unaware of what is happening for weeks or even months.

- These same thieves who have obtained a victim's credit card information may also request that the credit card company send them credit card "checks," which are written for cash just as are bank checks. Again, the charges are unknown to the victim because the credit card statements are no longer coming to the victim's address.

- Having obtained personal information such as name, date of birth, Social Security number, and so on, the thieves open new credit card accounts in the victim's name and run up charges until the victim becomes aware of the fraud. Similarly, credit accounts may be opened at stores using the victim's identity.

- The thieves open bank accounts in the victim's name and write bad checks on the account.

- The thieves obtain loans, such as real estate, auto, or personal loans, using the victim's identity.

- The thieves counterfeit checks or debit cards, and drain the victim's bank accounts of funds.

- The thieves establish services such as utility, telephone, or cell phone service in the victim's name.

- The thieves make long distance calls using stolen credit card numbers.²³

- The thieves may obtain other goods and privileges by using the victim's identity and information, either in person or by telephone or via the Internet.

These are only a few of the numerous schemes that an identity thief may use to obtain money, goods, or services at the expense of the unwitting victim.

Often a web of conspirators tie these individual criminal acts together. Investigation of one individual involved in identity theft therefore often leads to others working together, often in elaborate plots. The following actual case prosecuted in the western district of Washington State illustrates this point.

Between January 27, 1999 and April 14, 2000, a woman and other persons conspired to execute a scheme to defraud several commercial businesses in western Washington and elsewhere, including financial institutions, investment companies, credit card companies, merchant banks, and merchants, and to obtain money and merchandise from these businesses by means of false and fraudulent pretenses.

The conspirators assumed the identities of third persons and fraudulently utilized the Social Security account numbers and names of these persons. The conspirators then created false identity documents such as state identification cards, driver's licenses, and immigration cards. Using the identities and names of these third persons, the conspirators obtained credit cards and opened banking and investment accounts at numerous locations.

The conspirators also prepared fraudulent and counterfeit checks using the account names and numbers for actual bank accounts. The perpetrators then deposited the counterfeit checks into accounts opened by them, using one of their assumed identities. Shortly thereafter, they would withdraw the funds fraudulently credited to their accounts at the time they deposited the counterfeit checks. Over an 8-month period, counterfeit checks totaling over \$1 million were deposited at various banks and investment firms.

In addition, the conspirators purchased legitimate cashier's checks with fraudulently obtained monies and then altered the checks to reflect much higher values than the amounts purchased. Over five months, these transactions accounted for more than \$350,000.

The scheme also included telefaxed "letters of authorization" using other identities authorizing wire transfer of funds to co-conspirators, altered credit cards and related offenses.

Such involved criminal conspiracies begin with, and are perpetuated by identity theft. The result of all of these schemes may be that bill collectors begin to dun the victim, the victim's credit standing is ruined, and legal procedures may be instituted to collect the fraudulent debts from the victim. Identity thieves may even file for bankruptcy in the victim's name to avoid paying debts incurred while using the victim's personal information, or for other reasons, such as to avoid eviction from the house or apartment they have obtained by using the victim's identity.²⁴

E. Perpetrators

Identity theft is not perpetrated only by so-called white-collar thieves. It is committed by criminals of all types. A recent report indicates that during the period November 1999 to March 2001, about 12 percent of all suspected perpetrators reported to the FTC had a personal relationship of some sort with the victim. However, the remaining 88 percent of suspects had no relationship to the victim of the theft.²⁵ Thus, while the thief may be a family member, a coworker, a friend, or someone else personally known to the victim, in the vast majority of instances the perpetrators are unknown to the victim.

In most cases the thieves are geographically located far from the victim's place of work or residence. In the foregoing case example, the perpetrators in Washington State were using the identity of a woman in Massachusetts, among others. These perpetrators may be solo operators, but more often are members of a larger criminal organization. Such organizations may be local, regional, national, or international in scope. They may be composed of specific ethnic or national groups,²⁶ or may be simply a collection of criminals of various backgrounds cooperating to obtain illegal profits at the expense of the innocent victims.

G. Law Enforcement Policies and Procedures

As previously noted, it is essential that local police departments launch a concerted effort to assist in combating identity fraud. When the victim is a resident of, or otherwise associated with, the department's jurisdiction, the department has an obligation to assist the victim in every possible way. The individual who has been the target of identity theft is as much a victim as the victim of any other type of crime. In addition, police should be in a position to find and arrest identity thieves operating in the department's jurisdiction, and to assist other agencies, including federal agencies and police departments in other jurisdictions, with information and cooperation in connection with identity theft investigations being conducted by those other agencies.

A police department's first step in combating identity theft is to ensure that its personnel have a comprehensive knowledge of what identity theft is, who commits it, and how it is committed. The department's members must also know what federal, state, and local resources are available to assist them in reporting, investigating, and prosecuting identity theft. Police departments should make an effort to acquire all available information about identity theft and ensure that the handling of identity theft cases is included in the department's training curriculum, policies, and procedures.

Because identity theft so often is a multijurisdictional crime, it is necessary for each department to cooperate closely with other agencies in identity theft cases. For example, investigation and prosecution of the illustrative case cited previously could not have been successfully undertaken without coordination and cooperation with several federal agencies. The sharing of information about identity theft cases with other agencies is essential as it may not only lead to a successful prosecution of the case in one jurisdiction but concurrent investigation in other areas of the country.

In this regard, it is essential for state and local law enforcement agencies to participate in the Federal Trade Commission's Identity Theft ClearingHouse. Such participation provides access to extensive information about identity theft activity both nationwide and in the department's own region or state.²⁷

H. Victims and Reports of Identity Theft

In the past, local police departments have often failed to respond adequately to reports of identity theft and have failed to render adequate assistance to victims. Indeed, many local police departments have refused to take complaints about identity theft because the crime was not well understood, or a state statute was lacking, or the department could not identify the venue in which the theft occurred or the perpetrator was operating. This attitude by local police often created great frustration among victims and generated considerable ill will among these victims toward the departments concerned.

Today there is no excuse for police indifference to identity theft crimes and victims. Identity theft has been identified as a major crime problem in America, most states now have statutes making identity theft a specific crime, and there now exists a relative wealth of information and assistance to deal with identity theft. These and other factors combined make it mandatory for police departments to be prepared to take identity theft complaints, initiate investigations, and prosecute violators where possible. In addition, departments have an obligation to assist the victims through counseling, advice and referral where reasonable and appropriate.

At a minimum, each police departments should do the following:

1. *Develop a standardized procedure for taking identity theft reports.* Complaints should be taken by the police department in detail and in a manner consistent with the severity of the crime. Aspects of the online reporting form used by the FTC may be useful as a guide to local law enforcement agencies in their efforts to gather all pertinent information about the crime. Victims should not be brushed off or arbitrarily referred to other agencies as a standard course of action. Thus, departments should NOT merely refer victims to prosecutors' offices or to private attorneys for civil actions. It is the department's obligation to take the complaint and act on it.

2. *Initiate criminal investigations of identity theft reports.* Police should initiate investigation of identity theft reports. Again, identity theft is as much a crime as any other offense, and should be treated

as such. Unless and until it develops that the complaint is unfounded or for some other reason the department cannot proceed further, identity theft should be aggressively and fully investigated.

3. *Prosecute violators.* Identity thieves should be prosecuted. Identity theft is not just a prank, it is a serious crime and should be prosecuted to the fullest extent of the law. Unfortunately, the maximum penalties for these types of crimes in some states is not sufficient to garner the attention of prosecutors whose caseloads may already be overloaded with more other criminal activity. In these states, a long-term effort by local police and prosecutors needs to address this by calls for harsher criminal penalties for identity theft.

4. *Cooperate with other agencies.* Investigations of multijurisdictional identity theft schemes may involve a number of agencies. Each police department should cooperate fully with any agency participating in an identity theft case. If it proves impossible to prosecute the identity thief in the department's own jurisdiction, full cooperation should be given to departments in other jurisdictions where there is a greater likelihood of successfully prosecuting the perpetrators.

5. *Assist victims by providing the victim with helpful information.* Victims of identity theft are often unaware of the proper steps to take in order to minimize the damage suffered because of the identity theft and protect themselves against further victimization. Each police department should provide every identity theft complainant with information as to the steps that the victim should take. Much of that information is available through counselors at the FTC. To summarize this and other information, police officers responding to victims of identity theft and taking crime reports on these matters should keep the following instructions in mind in order to deal most effectively with these crime victims:

- Contact the fraud departments of each of the three credit reporting agencies. Give the agency full details of the theft, a case number as provided by local police, and request that a fraud alert be placed on your file.

- Request a copy of your credit report, review the report for errors or fraudulent entries, submit any changes necessary and get a new copy at a later date to ensure that changes or problems have been corrected.

- Contact all credit card companies where you have an account and notify them of the fraud. Close existing accounts and open new accounts with new PIN numbers and passwords.

- Contact banks and financial institutions. To be safe, close accounts and open new accounts with new PINs and passwords. Major check verification companies should also be contacted and asked to notify retailers not to accept your stolen or misappropriated checks. The bank may be able and willing to do this for you. ATM cards that may have been compromised should be canceled and new ones obtained with new PINs and passwords.

- If there is reason to believe that investment or brokerage accounts have been tampered with or otherwise compromised, contact the broker or investment account manager as well as the Securities and Exchange Commission.

- If unauthorized new accounts have been opened through utility or telephone companies or if the victim's own service is being used to make unauthorized calls, contact the utility or service provider immediately. If the companies do not cooperate, contact the state's public utility commission and/or the Federal Communications Commission.

- If there is reason to believe that the Social Security number is being misused, this should be reported to the Social Security Administration's fraud hotline. In addition, it is wise to contact the Social Security Administration to verify the accuracy of the

earnings reported under the victim's Social Security number. Request a copy of your Social Security Statement.

- If a driver's license or driver's license number is involved in the identity theft, contact the jurisdiction's department of motor vehicles. The same is true if a non-driver's identity card is involved. If the driver's license number is the same as the victim's Social Security number, a different number should be substituted.

- If someone has filed bankruptcy in the victim's name, the victim should contact the U.S. Bankruptcy Trustee in the region where the bankruptcy was filed.

- In some instances, the perpetrator of the identity theft may have committed a crime in the victim's name. When this becomes known, the appropriate agencies should be contacted for information as to how the victim's name may be cleared. The procedures for this vary widely among jurisdictions, and it may be necessary for the victim to hire an attorney to accomplish the name-clearing process.

- The victim to contact other police departments where the victim resides or where the identity theft may have taken place. The victim should obtain a copy of the police report regarding the theft from each department to whom the theft has been reported. This is essential, because even if the police do not apprehend the perpetrators, the police report may assist the victim in dealing with creditors during efforts to avoid financial liability for fraudulent actions and to repair the damage done to the victim's credit. The fact that a victim has reported and personally attested to the truth of the allegations in a written police report helps other agencies verify the credibility of the victim and take measures on his or her behalf.

- The victim should contact the Federal Trade Commission via telephone or mail to report the identity theft.²⁸

- Because the types of identity theft schemes are so varied, other agencies or entities may need to be contacted. If any agency or entity not otherwise discussed above is involved in some manner, it should be contacted immediately. For example, the Internal Revenue Service should be notified if tax issues may be involved.

Many of the reports and requests discussed above may be made initially by telephone. However, all such requests should be followed up in writing, since telephone reports are often insufficient to preserve the victim's legal rights and written reports may be necessary to obtain the cooperation of the entity being contacted.

The telephone numbers, addresses, Web sites, and other appropriate data necessary to enable the victim to contact these various agencies should be kept on file in the police department and made available to complainants. These addresses, telephone numbers, web sites and related information can be found in several current guides for identity theft victims, such as the FTC publication *ID Theft—When Bad Things Happen to Your Good Name*. Police departments should consider maintaining a supply of copies of this or similar publications and distribute them to identity theft complainants for their information and assistance.

It is important that local police departments take a proactive role in the education of the public regarding identity theft and the means of preventing it. While in the Information Age no person can completely control the dissemination of his or her personal information, there are specific steps that everyone can take to minimize exposure to identity theft. Crime prevention units and community policing officers should take advantage of their roles within the community by providing citizens with information that they can use to protect themselves against identity theft. There is considerable literature available, both in printed form and on the Internet, about preventive measures. Officers should be aware of these sources and provide them to citizens whenever possible.²⁹

Endnotes

¹ "Identity Thieves Thrive in Information Age," *Washington Post*, May 31, 2001, page A01. Viewed online at <http://www.washingtonpost.com>.

² IACP notes from briefing by U.S. Secret Service, Financial Crimes Division.

³ Federal Trade Commission report *Identity Theft Complaint Data, Figures and Trends on Identity Theft*, November 1999 through March 2001, p.3.

⁴ See description of various types of identity theft schemes, infra.

⁵ An identity theft scheme that targets elderly African Americans has been discovered. This is reported at the FTC Web site: <http://www.consumer.gov/idtheft/cases.htm>.

⁶ 18 U.S.C. § 1028.

⁷ 18 U.S.C. § 1028(a)(7). Text of the act may be found on the Internet at <http://www.consumer.gov/idtheft/fedlaw.htm>.

⁸ 18 U.S.C. § 1029.

⁹ 19 U.S.C. § 1930.

¹⁰ 18 U.S.C. § 1343.

¹¹ 18 U.S.C. § 1344.

¹² See *Federal Trade Commission booklet ID Theft When Bad Things Happen to Your Good Name*, published February 2001.

¹³ See, e.g., Ohio Rev. Code Ann. 2913.49(E), which provides: Whoever violates this section is guilty of taking the identity of another. Except as otherwise provided in this division, taking the identity of another is a misdemeanor of the first degree. If the value of the credit, property, services, debt, or other legal obligation involved in the violation or course of conduct is five hundred dollars or more and is less than five thousand dollars, taking the identity of another is a felony of the fifth degree. If the value of the credit, property, services, debt or other legal obligation involved in the violation or course of conduct is five thousand dollars or more and is less than one hundred thousand dollars or more, taking the identity of another is a felony of the third degree.

¹⁴ A listing of state identity theft statutes may be found on the Internet at www.consumer.gov/idtheft/statelaw.htm.

¹⁵ *FTC Consumer Alert! Hoax Targets Elderly African Americans*. Federal Trade Commission: Washington, D.C., www.ftc.gov.

¹⁶ FTC information sheet "The Identity Theft Clearinghouse: What's In It For You?", published November 2000.

¹⁷ For information as to how local departments may utilize this service, see section VIII B., below.

¹⁸ Resolution adopted at the IACP's Annual Conference in San Diego on November 15, 2000.

¹⁹ These items are all listed in the FTC publication *ID Theft—When Bad Things Happen to Your Good Name*, published February 2001.

²⁰ FTC online publication *Pretexting: Your Personal Information Revealed*, dated January 2001, available on the Internet at <http://www.ftc.gov/bcp/online/pubs/credit/pretext.htm>.

²¹ See Department of Justice electronic publication *Identity Theft and Fraud*, available on the Internet at <http://www.usdoj.gov/criminal/fraud/text/idtheft.html>.

²² In another rather imaginative version of this type of identity theft, criminals installed a phoney ATM machine in a shopping mall, then poured glue into the slots of the legitimate machines in the mall. Customers unable to use the disabled ATM machines went to the fraudulent machine, which did not dispense money but merely recorded the data from the ATM card. This data was then recovered by the criminals and used to withdraw cash from ATM machines at other locations. See Department of the Treasury, A United States Secret Service Financial Crimes Division Briefing, @ Section IV A.

²³ All of these various schemes are described in, e.g., FTC publication *ID Theft—When Bad Things Happen to Your Good Name*, published February 2001; *Pretexting: Your Personal Information Revealed*, dated January 2001, electronic publication available on the Internet at <http://www.ftc.gov/bcp/online/pubs/credit/pretext.htm>; Department of Justice electronic publication *Identity Theft and Fraud*, @ available on the Internet at <http://www.usdoj.gov/criminal/fraud/text/idtheft.html>.

²⁴ For further discussion of consequences to the victim, see prior discussions in this document.

²⁵ Federal Trade Commission report *Identity Theft Complaint Data, Figures and Trends on Identity Theft*, November 1999 through March 2001, p. 4.

²⁶ For example, when the U.S. Secret Service received primary jurisdiction in the investigation of credit card fraud, AOne of the first groups that the Secret Service began to engage on a regular basis were loosely organized criminal elements within the growing Nigerian population in the United States. ...[T]hese Nigerian criminal groups have instituted sophisticated fraud schemes in the area of bank fraud, false identification, insurance fraud, credit card fraud, and advanced fee fraud." *Department of the Treasury, A United States Secret Service Financial Crimes Division Briefing*

²⁷ Any law enforcement agency may utilize this service by executing a confidentiality agreement between the agency and the FTC. The FTC publication *The Identity Theft Data Clearinghouse: What's In It For You?* indicates that police departments desiring to participate in the service should contact Kathleen Lund at (202) 326-3888 or on the Internet at klund@ftc.gov.

²⁸ The FTC Identity Theft Hotline is 1-877-IDTHEFT (877-438-4338).

²⁹ Two excellent sources of information about preventive measures are the FTC and Department of Justice publications cited previously, i.e., the FTC publication *ID Theft—When Bad Things Happen to Your Good Name*, published February 2001, and the Department of Justice electronic publication *Identity Theft and Fraud*. These documents are available on the Internet at <http://www.usdoj.gov/criminal/fraud/text/idtheft.html>. The FTC and other government agencies offer a number of other publications that may be useful. Much helpful information may be obtained on the Internet at <http://www.consumer.gov/idtheft>, and <http://www.usdoj.gov>.

This project was supported by Grant No. 2000-DD-VX-0020 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice or the IACP.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.