



# Training Key® #616

## Identity Crime Update: Part I (2008)

Identity crime continues to be a major problem in the United States. With the continuing development of new technologies that facilitate identity crime of all kinds, it has become more widespread and increasingly difficult to counteract. A strong law enforcement response is essential in order to arrest and prosecute perpetrators. This *Training Key®* is the first in a two-part series on this subject.

Identity crime is the illegal use of another's personal information, such as credit card numbers, social security number, or driver's license number, to gain something of value or facilitate other criminal activity. This crime can devastate the victim's credit for years. Identity crime knows no boundaries; victims and criminals can be on opposite sides of the world, making it difficult for local law enforcement agencies to investigate the crime, catch the perpetrator, or help the victim.

Because it is usually part of a larger criminal enterprise, the theft of personal information is one of the most serious of all crimes.

### Scope of the Problem

For the seventh year in a row, identity crime was the number one source of consumer fraud complaints submitted to the Federal Trade Commission (FTC). According to the agency's annual report on fraud complaints for 2007, of 813,899 total complaints received in 2007, 258,427 (32 percent) were related to identity crime.<sup>1</sup> The FTC estimates that nearly 8.5 million Americans were victims of some form of identity theft annually.<sup>2</sup> These numbers are likely to underrepresent the true number of identity crime victims, as many do not report the crime to authorities.

Identity theft, one component of some identity crimes, is in itself a criminal act under both federal and state laws, and the theft is almost always a steppingstone to the commission of other crimes. Typical crimes associated with identity theft include credit card fraud, bank fraud, fraudulent obtaining of loans, and other schemes designed to enable the perpetrator to profit from the original theft. Often, several types of fraud are involved in, or result 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 larger criminal enterprises, including terrorist, drug, and gang activities.

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

It is difficult to accurately determine the financial losses caused by identity crime. Many identity crimes are not reported to police, and there is no single source of information on this issue. Jurisdiction for investigation of these crimes is shared by the U.S. Secret Service, the U.S. Postal Inspection Service, and the Federal Bureau of Investigation (FBI), among principal federal enforcement agencies. 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 crime are staggering. The "2008 Identity Fraud Survey Report" by Javelin Strategy and Research estimated that identity crime accounted for a loss of \$45 billion in 2007. Similarly, a study of Secret Service data by Utica College's Center for Identity Management and Information Protection found that the median actual dollar loss for identity theft victims was \$31,356. This includes both business and individual consumer victims.<sup>3</sup>

## Personal Costs

Perhaps even more vexing than the monetary loss is the personal cost of identity theft. Because identity crime by definition involves the fraudulent obtaining of funds in the name of someone else, the victim of identity crime 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 crime 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 crime, the physical and mental toll on the victim can be significant. Typically, a victim of identity crime 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 who 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 can take 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 his or her credit may be unsuccessful, leaving the victim under a cloud for the rest of his or her life.

## Victimology

Virtually anyone may become the victim of identity crime. Contrary to popular misconception, personal information is not stolen only 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 criminals use to steal thousands upon thousands of dollars in the name of the victim.

No particular age group is immune from identity crime. Federal Trade Commission data indicates that 19 percent of identity theft victims were aged 20-29, 23 percent aged 30-39, 24 percent aged 40-49, and 20 percent aged 50-59. Victims 60 and older represented 12 percent of all victims, while 2 percent of victims were 19 and younger.<sup>4,5</sup> Victimization rates may be correlated to Internet use, which is a tool in many identity crimes, which accounts for the large number of younger victims. However, elderly Americans are highly vulnerable to other types of identity crimes, particularly the various telephone scams used by perpetrators to acquire personal information. The elderly have always been targeted by perpetrators of fraud and will no doubt continue to be.

The victims of identity crime may be residents of almost any geographical area. According to FTC data, the largest number of complaints came from California, Texas, New York, Florida, and Illinois, and the highest concentration of complaints per 100,000 people reportedly came from Arizona, California, Nevada, Texas, and Florida.<sup>6</sup> The problem is national in scope, and not even the residents of the smallest locality of the least populous states are safe from it. In fact, rural areas are increasingly seeing significant increases in the incidence of identity crime.

## Statutes

Identity crime was not a federal crime until Congress passed the Identity Theft and Assumption Deterrence Act of 1998.<sup>6</sup> Under the statute, it is a federal offense for any person to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law or a felony under any applicable state or local law. The statute defines "means of identification" as a name, social security number, credit card number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual. This crime carries a maximum penalty of 15 years' imprisonment, a fine, and criminal forfeiture of personal property used to commit the offense.

In 2004, Congress passed the Identity Theft Penalty Enhancement Act,<sup>7</sup> which established a mandatory two-year minimum sentence to be served in addition to the sentence that the person was already sentenced to for aggravated identity theft.

Although these laws specifically target identity theft, it is important to note that identity theft is usually part of a larger criminal scheme and generally involves other federal statutes, such as statutory prohibitions against credit card fraud, computer fraud, mail fraud, or wire fraud.

Today, all 50 states have enacted statutes making identity theft a crime. Identity theft is a felony in 37 states. In the other 13 states plus the District of Columbia, the crime may be either a felony or a misdemeanor, depending on the dollar amount of loss resulting from the theft.<sup>8</sup> Local law enforcement officials should be familiar with state laws on identity theft. For your convenience, comprehensive summaries of state laws and resources on identity theft are available on [www.idsafety.org](http://www.idsafety.org).

## Role of Federal Investigative Agencies

Investigation of identity crimes 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 crimes depends upon the nature and method of the theft. For example, the Secret Service investigates matters involving fraudulent use of currency, while the Postal Service investigates cases involving the use of the mails. However, because identity theft and its resultant crimes often involve a wide variety of offenses and means of committing those offenses, there can be 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, as under that statute identity theft itself is now a federal crime.

The Federal Trade Commission (FTC) is the federal government's principal consumer protection agency, with broad jurisdiction extending over nearly the entire economy, including business and consumer transactions on the telephone, on 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. It is authorized to halt deception in several ways, including through civil actions filed by its own attorneys in federal district courts. The FTC also has jurisdiction over cross-border consumer transactions. Many identity crime enterprises operate outside the United States.

Of particular importance here are the provisions of the federal Identity Theft and Assumption Deterrence Act of 1998, which gives the FTC a substantial role in the campaign against identity crime. Under the act, the FTC is empowered to act as a nationwide clearinghouse for information related to identity crimes. This central source of information is an important aspect of the effort to combat identity crime, because the crime is widespread and a single identity crime 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 crime 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 and to provide guidance to victims of identity theft in order to help them defend themselves against the effects of this crime.

## Identity Crime Web Site and Hotline

The FTC maintains a comprehensive Web site devoted entirely to identity theft: [www.ftc.gov/IDTheft](http://www.ftc.gov/IDTheft). It offers excellent resources on identity crime, including information for victims, businesses, and law enforcement. Its site is one of the most comprehensive of its kind among state and federal government agencies. The site for consumers includes information on how to avoid identity crime and what steps to take if their identity is stolen.

In addition, the FTC operates an identity crime hotline for victims at 1-877-IDTHEFT (1-877-438-4338). Victims who call the hotline to report identity crime 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 clearinghouse. The hotline has been in operation since November 1999.

The Web site offers many useful suggestions to consumers on how to minimize the risk of identity crime:

- Never reveal your personal identifying information on the phone, through the mail, or on the Internet unless you have initiated the contact or know exactly who you are dealing with and how it will be used.
- Before you share any personal information, confirm that you are dealing with a legitimate organization or agency.
- It is especially important to protect your social security number (SSN). Don't carry your SSN card in your wallet; store it in a secure place. Give out your SSN only when absolutely necessary, and ask to use other types of identifiers.
- Read all your bills carefully. Call your creditors to dispute any charges you didn't make or authorize.

- Order a copy of your credit report every year from each of the three major credit reporting agencies to verify that your credit information is accurate. All consumers may receive a free credit report from [www.annualcreditreport.com](http://www.annualcreditreport.com).
- Treat your mail and trash carefully. Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, have your mail held at the post office until you can pick it up or are home to receive it.
- To thwart a thief who may pick through your trash or recycling bins to capture your personal information, tear or shred any important paperwork or receipts with personal identifying information on them.
- Install and update your computer's virus protection software regularly.
- Do not open files sent to you by strangers, click on hyperlinks, or download programs from people or companies you don't know. Be cautious about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as spyware, which could capture your passwords or any other information as you type it into your keyboard.
- Make sure that Internet sites are secure before providing personal or financial information online.<sup>9</sup>

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 crime. It is also the reason many identity 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.

The FTC also offers a comprehensive guide to people who have become victims of identity crime. 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 crime:

- File a report with the police immediately. Victims will need to provide a copy of the police report to the banks, creditors, other businesses, credit bureaus, and debt collectors. (This issue will be addressed later in this *Training Key*® but 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).
- Contact any one of the three credit bureaus to report the crime of identity theft: Equifax (1-800-525-6285), Experian (1-888-397-3742), or TransUnion (1-800-680-7289). Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent

accounts from being opened. As soon as one of the bureaus places a fraud alert, the other two bureaus are automatically notified.

- Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you can't explain. Check that information like your SSN, addresses, name or initials, and employers are correct. If you find fraudulent or inaccurate information, contact the consumer reporting companies to get it removed. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.
- Close any unauthorized or compromised credit or charge accounts. Cancel each credit and charge card. Get new cards with new account numbers.
- 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.
- 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.
- Fill out an FTC ID Theft Affidavit, which is accepted by many banks, creditors, businesses, and the credit bureaus.
- File a complaint with the Federal Trade Commission. By sharing your identity crime complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity criminals and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.<sup>10</sup>

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 and 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 crime 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 on the Internet at the FTC's identity crime Web site, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), which also provides tips for consumers about combating identity theft.

The FTC also produces a number of publications that provide information to consumers, victims, and law enforcement agencies about identity theft:

- "Take Charge: Fighting Back Against Identity Theft" (2005)<sup>11</sup>
- "Deter, Detect, Defend" booklet (2006)<sup>12</sup>
- "Identity Crisis: What to Do If Your Identity Is Stolen" (2005)<sup>13</sup>
- "ID Theft: What It's All About"<sup>14</sup>

## Additional Resources for Law Enforcement

The Web site mentioned above ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) also provides law enforcement agencies with reports of recent identity crime and schemes, and information on state identity crime laws. In 1997, the FTC established Consumer Sentinel as a Web-based law enforcement network that provides law enforcement agencies in the United States, Canada, and Australia with secure, password-protected access to more than 1 million consumer complaints about telemarketing, direct mail, and Internet fraud. Law enforcement agencies, including 90 federal law enforcement organizations, more than a thousand state and local agencies, and every state attorney general's office in the country 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. This enables users to share information, avoid duplication of efforts, and formulate rapid responses to new fraud schemes.

In 2001, in order to build on the success of Consumer Sentinel, and as part of overall efforts to combat cross-border identity and related consumer fraud, the FTC established [www.econsumer.gov](http://www.econsumer.gov) in conjunction with 12 other countries. Now with a membership of 21 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, which is a part of Consumer Sentinel, offers law enforcement agencies direct Internet access to almost 300,000 consumer complaints about identity crime. Using the clearinghouse, police departments and other law enforcement agencies may find victims and perpetrators of identity crime, link reports of identity crimes that might otherwise look like isolated events, and identify other federal, state, or local agencies involved in a particular investigation. This same service also helps law enforcement identify overall trends in identity crime.

Other federal agencies participate in the efforts to combat identity crime. 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 num-

bers 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 crime workshops, conferences where identity crime 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.

## Endnotes

<sup>1</sup> Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data: January-December 2007," February 2008, <http://www.consumer.gov/sentinel/pubs/top10fraud2007.pdf>.

<sup>2</sup> Better Business Bureau, 2005.

<sup>3</sup> Utica College, Center for Identity Management and Information Protection, "*Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*," by Gary R. Gordon, Donald J. Rebovich, Kyung-Seok Choo, and Judith B. Gordon, October 2007, [http://www.utica.edu/academic/institutes/ecii/publications/media/cimip\\_id\\_theft\\_study\\_oct\\_22\\_noon.pdf](http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf).

<sup>4</sup> Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data: January-December 2007," February 2008, <http://www.consumer.gov/sentinel/pubs/top10fraud2007.pdf>.

<sup>5</sup> Better Business Bureau, 2005.

<sup>6</sup> Ibid.

<sup>7</sup> 18 U.S.C 1028, [http://www.law.cornell.edu/uscode/18/usc\\_sec\\_18\\_00001028-000-.html](http://www.law.cornell.edu/uscode/18/usc_sec_18_00001028-000-.html).

<sup>8</sup> 18 U.S.C 1028A, <http://www4.law.cornell.edu/uscode/18/1028A.html>.

<sup>9</sup> IACP Matrix, [http://idsafety.org/files/pdfs/state-by-state-id\\_crime\\_laws.pdf](http://idsafety.org/files/pdfs/state-by-state-id_crime_laws.pdf).

<sup>10</sup> Federal Trade Commission. "*ID Theft: What It's All About*," June 2005, <http://www.ftc.gov/bcp/online/pubs/credit/idtheftmini.shtm>.

<sup>11</sup> Federal Trade Commission. "*Take Charge: Fighting Back Against Identity Theft*," February 2005, <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm>.

<sup>12</sup> <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm>.

<sup>13</sup> <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth01.shtm>.

<sup>14</sup> <http://www.ftc.gov/bcp/online/pubs/credit/iderisis.shtm>, August 2005.

<sup>15</sup> <http://www.ftc.gov/bcp/online/pubs/credit/idtheftmini.shtm>

## Acknowledgment

This two-part *Training Key*® was developed by the Nationwide Strategy to Prevent and Respond to Identity Crime project. This project was made possible when the International Association of Chiefs of Police (IACP) and Bank of America (BAC) joined forces to develop the national strategy to combat identity crime, provide support to law enforcement and help improve consumer awareness and protection. For more information about the Identity Crime project visit the official Web site at: [www.idsafety.org](http://www.idsafety.org) or contact project staff via e-mail at [idsafety@theiacp.org](mailto:idsafety@theiacp.org).

# questions

The following questions are based on information in this *Training Key*®. Select the one best answer for each question.

1. Which of the following statements is true?

- (a) *The escalation of identity crime in the United States is due in large part to the information technology revolution.*
- (b) *As the use of technology to store and transmit information increases, the rate of identity crime will most likely increase.*
- (c) *The rapid expansion of computers to store personal data combined with the growing use of the Internet has provided criminals with new means to steal and misuse personal information.*
- (d) *All of the statements are true.*

2. Which of the following statements is false?

- (a) *Under the Identity Theft and Assumption Deterrence Act, the Federal Trade Commission is empowered to act as a nationwide clearinghouse for information related to identity crimes.*
- (b) *Identity theft is most often not part of a larger criminal act and is generally committed by small-time criminals.*
- (c) *The Federal Trade Commission has established a number of central resources to provide information to law enforcement agencies about identity crime as well as to provide guidance to victims of identity crime.*
- (d) *Violation of the Identity Theft and Assumption Deterrence Act gives federal investigative agencies additional scope to pursue identity thieves.*

3. Which of the following statements is true?

- (a) *Many identity crimes are not discovered by the victim and reported to the authorities until long after substantial financial loss been incurred.*
- (b) *The Identity Theft Clearinghouse is a centralized database used to aid law enforcement and prevent identity crime.*
- (c) *The Identity Theft Clearinghouse offers law enforcement agencies direct Internet access to consumer complaints about identity crime and enables them to link seemingly isolated crimes together.*
- (d) *All of the statements are true.*

# answers

- 1. (d) All of the statements are true.
- 2. (b) Identity theft is usually part of a larger criminal scheme and generally involves other federal statutes, such as criminal prohibitions against credit card fraud, computer fraud, mail fraud, or wire fraud.
- 3. (d) All of the statements are true.





# Training Key® #617

## Identity Crime Update: Part II (2008)

Identity crime continues to be a major problem in the United States. With the constant development of new technologies, it has become more widespread and increasingly difficult to counteract. A strong law enforcement response is essential in order to arrest and prosecute perpetrators. This is the second part of a two-part *Training Key®* on this subject.

### Role of Local Law Enforcement

In earlier years, the involvement of local police departments in identity crime cases was typically minimal. This was the result of several factors, including the lack of state laws making identity theft a crime, the fact that most identity crime operations are multijurisdictional enterprises, with perpetrator and victim are usually widely geographically separated, and the general lack of police expertise in investigating identity crimes. Fortunately, this situation is rapidly being remedied. The passage of state statutes has given state and local police the authority to investigate identity crimes, and departments everywhere are becoming more aware of the significance of identity crime and the availability of the means to combat it.

### Types of Identity Crime and Identity Crime Operations

Thieves obtain personal and financial identifying information in various ways. Here are some of the most common schemes:

- Theft of wallets and purses containing personal identification, credit cards, and bank cards.
- Theft of mail, including mail containing bank and credit card statements, preapproved credit offers, telephone calling cards, and tax information. Thieves can also complete a change of address form with the U.S. Postal Service to divert 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.
- 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.
- Stealing information from a home, including theft by the homeowner's friends, relatives, or employees.
- 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.
- Stealing or purchasing information from inside sources such as employees, who may for a price provide identity thieves with information taken from applications for goods, services, or credit.
- Tricking victims in providing personal or financial information over the telephone or online by pretending to be a bank or other trusted source.
- Stealing information from a loan or credit application form filed at a hospital, bank, school, or business the victim dealt with.
- Getting it from the victim's computer, especially one that lacks firewalls, through the use of viruses or spyware.
- Stealing information during a data breach at a government agency, school, or company that maintains access to the victim's private information.
- Using skimming devices designed to illegally obtain account information from the magnetic strip on credit cards.
- 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.

In addition, criminals are continually developing new and ingenious methods of obtaining personal information, and law enforcement must continually revise their investigative tactics to combat these new threats.

Although many people believe that most identity theft occurs on the Internet, research has shown that many such thefts occur in the physical world, rather than the virtual one. A recent survey by Javelin Strategy and Research found that among the 35 percent of identity theft victims who knew how their data was taken, lost or stolen wallets, checkbooks, or credit cards accounted for more than twice as many instances of theft than all online channels put together.<sup>1</sup> Specifically, the survey found that in these cases, online identity theft methods, including phishing, hacking, and spyware, constituted only 12 percent of all fraud cases. The vast majority of known cases (79 percent) occur when an identity thief makes direct contact with the consumer's personal identification, such as with stolen and lost checkbooks and wallets or credit or bank cards, shoulder surfing, and stolen mail. In addition, 17 percent of these known cases occur from so-called friendly theft, where the victim's information is stolen by family, friends, or employees.<sup>2</sup>

## How Stolen Information Is Used

Identity thieves use the information they have stolen in countless ways. It is important for law enforcement officers to understand that identity crime is often used to facilitate other crimes, such as credit card fraud, loan and mortgage fraud, mail theft and mail fraud, narcotics violations, money laundering, weapons trafficking, computer crimes, wire fraud, and terrorism. The following are just a few examples of the schemes used by identity thieves to obtain money, goods, or services at the expense of an unwitting victim:

- Once they have a victim's credit card number, thieves may call the victim's credit card issuer and, pretending to be the victim, ask that the mailing address on the account be changed. The thieves then run up high charges on the credit card. Because credit card statements are no longer being sent to the victim's real address, the victim may 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 victim is unaware of the charges because the credit card statements are no longer coming to the victim's address.
- Having obtained a victim's personal information, such as name, date of birth, and social security number, 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 obtain other goods and privileges by using the victim's identity and information, either in person or by telephone or on the Internet.

Often a web of conspirators ties these individual criminal acts together. Investigation of one individual involved in identity theft therefore often leads to others working together, often in elaborate plots. Such involved criminal conspiracies begin with, and are perpetuated by means of identity crimes.

## Perpetrators

Identity crime is not solely perpetrated by so-called white-collar thieves. It is committed by criminals of all types, and is increasingly being used as a way to fund criminal enterprises, including drug trafficking, gangs, and terrorism. Identity crime perpetrators can be divided into two main categories: opportunists and organized. The opportunist perpetrators include criminals such as purse snatchers, drug addicts, and car thieves. Identity theft is not their primary target crime, but they will use stolen information to commit identity crimes or to sell the information to identity crime perpetrators or criminal organizations, including street gangs, narcotics traffickers, fraud rings, and terrorists.

In most cases the thieves are geographically located far from the victim's place of work or residence. 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 or may be simply a collection of criminals of various backgrounds cooperating to obtain illegal profits at the expense of the innocent victims.

Some identity crimes are committed by a family member, a coworker, a friend, or someone else personally known to the victim, but in most cases the perpetrators are unknown to the victim.

## Law Enforcement Policies and Procedures

When the victim is a resident of, or otherwise associated with, a police 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 crime 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 crime investigations being conducted by those other agencies.

A police department's first step in combating identity crime is to ensure that its personnel have a comprehensive knowledge of what identity crime 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 crimes. Basic information about each of these items is provided in the preceding portions of this *Training Key*® and is also available on [www.idsafety.org](http://www.idsafety.org). Police departments should make an effort to acquire all available information about identity crime and ensure that the handling of identity crime cases is included in the department's training curriculum, policies, and procedures.

Because identity crime so often is a multijurisdictional crime, it is necessary for each department to cooperate closely with other agencies in such cases. For example, investigation and prosecution of many identity crime cases cannot be successfully undertaken without coordination and cooperation with federal agencies. The sharing of information about identity crime cases with other agencies is essential, as it can lead not only to the successful prosecution of the cases in one jurisdiction but also to concurrent investigations 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 crime activity both nationwide and in a particular region or state. Departments should also encourage victims in their jurisdiction to file a complaint with the Federal Trade Commission through their Consumer Sentinel database, which can also be used by departments during their investigations.

## Victims and Reports of Identity Crime

In the past, local law enforcement agencies have sometimes failed to respond adequately to reports of identity crime. Indeed, many local police departments have refused to take complaints about identity crime because the crime was not well understood, or a state statute was lacking, or because police could not identify the venue in which the crime occurred or the perpetrator was operating. This attitude on the part of local law enforcement often frustrated victims and generated considerable ill-will toward the departments concerned. It is important for officers to build a strong working relationship with victims, who have often been emotionally and financially devastated by the effects of the crime.

Today there is no excuse for law enforcement indifference to identity crimes and victims. Identity crime has been identified as a major problem in America, and all states now have statutes making identity crime a state crime. In addition, there is now a wealth of information about the investigation of identity crimes. This makes it imperative that police departments be prepared to take identity crime complaints, initiate investigations, and prosecute violators wherever possible. In addition, departments have an obligation to assist the victims through counseling, advice, and referral when reasonable and appropriate.

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

1. *Develop a standardized procedure for taking identity crime 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 dismissed 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. Recognizing the importance of police reports to identity crime victims, 24 states and the District of Columbia specifically require local police departments to take such an action.<sup>3</sup>

2. *Initiate criminal investigations of identity crime reports.*

The passage of state statutes has given state and local law enforcement authority to investigate and prosecute identity crimes. Unless and until it develops that the complaint is unfounded or for some other reason the department cannot proceed further, identity crimes should be aggressively and fully investigated. To facilitate investigation of the complaint, law enforcement can obtain a victim's identity crime-related transaction records from creditors without first obtaining a subpoena, once they have authorization from the victim. This right was created in 2003 as an amendment to the Fair Credit Reporting Act.<sup>4</sup>

Law enforcement officers should also use the Identity Theft Data Clearinghouse,<sup>5</sup> a national identity crime victim complaint database containing more than 815,000 complaints, to search for identity crime victim and suspect information across the country.

3. *Cooperate with other agencies as needed.* Investigations of multijurisdictional identity crime schemes may involve a number of agencies at the local, state, and federal levels. Each police department should cooperate fully with any agency participating in an identity crime 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 perpetrator.
4. *Prosecute violators.* Identity crime is not just a prank. It is a serious crime and should be prosecuted to the fullest extent of the law. Unfortunately, in some states, the maximum penalties for these crimes are insufficient to garner the attention of prosecutors whose caseloads may already be overburdened with other criminal activity. In these states, a long-term effort by local law enforcement and prosecutors needs to address this by calling for harsher criminal penalties for identity crimes.

5. *Assist victims by providing them with the information they need to minimize the damage caused by the crime and to protect themselves against further victimization.* One goal of investigating identity crimes is to help restore victims to their pre-crime status. Law enforcement agencies should provide every identity crime complainant with information as to these steps and resources they can consult for further information. Specifically, police officers responding to victims of identity crime and taking crime reports should advise victims to take the following steps:

- Contact the toll-free fraud numbers of any one of the three major credit bureaus to place a fraud alert on their credit report. Fraud alerts can help prevent an identity thief from opening additional accounts in victims' names. As soon as the credit bureau con-

firms the fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts. Once a fraud alert is placed, victims are entitled to order one free copy of their credit report from each of the three nationwide consumer reporting companies.

- Close the accounts that have been tampered with or opened fraudulently. When victims dispute new unauthorized accounts, many banks and creditors will accept the ID Theft Affidavit<sup>6</sup>, which will save victims valuable time in the recovery process.
- Request a copy of their 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 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 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. Victims should request a copy of their social security statements.
- If a driver's license or driver's license number is involved in the identity crime, contact the jurisdiction's department of motor vehicles. The same is true if a non-driver's license 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 crime may have committed another crime in the victim's name. When this becomes known, ask the appropriate agencies 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.

- Obtain a copy of the police report regarding the crime from each department to whom the crime has been reported. This is essential, because even if perpetrators have not been apprehended, the police report may help the victim deal 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 by telephone or mail to report the identity crime. A complaint can be filed using an online complaint form<sup>7</sup> or by calling the FTC's Identity Theft Hotline, toll-free, at 1-877-ID-THEFT (438-4338).
- Because the types of identity crime are so varied, contact other agencies or entities as necessary. 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 guides for identity crime victims, such as the FTC publication "Take Charge: Fighting Back Against Identity Theft" (2005).<sup>8</sup> Police departments should consider maintaining a supply of copies of this or similar publications and distributing them to identity crime complainants for their information and assistance.

It is important that local law enforcement agencies take a proactive role in the education of the public regarding identity crimes and the means of preventing it. 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 crime. Crime prevention units and community policing officers should take advantage of their roles in the community by providing citizens with information they can use to protect themselves against identity crime. There is considerable literature available, both in printed form and on the Internet, regarding preventive measures. Officers should be aware of these resources and provide them to citizens whenever possible. Excellent resources can be found on the on the IACP/Bank of America identity crime site at [www.idsafety.org](http://www.idsafety.org) and on the FTC's Web site at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

## Endnotes

<sup>1</sup> “2008 Identity Fraud Survey Report.” Javelin Strategy and Research. February 2008: <http://www.javelinstrategy.com/products/798BBF/97/delivery.pdf>

<sup>2</sup> Ibid.

<sup>3</sup> “2007 State Identity Crime Laws.” International Association of Chiefs of Police. January 2008: [http://idsafety.org/files/pdfs/state-by-state-id\\_crime\\_laws.pdf](http://idsafety.org/files/pdfs/state-by-state-id_crime_laws.pdf)

<sup>4</sup> Fair Credit Reporting Act, section 609(e): <http://www.ftc.gov/os/statutes/031224fcra.pdf> (page 38).

<sup>5</sup> FTC’s Identity Theft Data Clearinghouse: <http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen09.pdf>

<sup>6</sup> FTC Identity Theft Affidavit: <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

<sup>7</sup> FTC Complaint Input Form:

[https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z\\_ORG\\_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03)

<sup>8</sup> “Take Charge: Fighting Back Against Identity Theft.” Federal Trade Commission. February 2005: <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm>

### Acknowledgment

This two-part *Training Key*® was developed by the Nationwide Strategy to Prevent and Respond to Identity Crime project. This project was made possible when the International Association of Chiefs of Police (IACP) and Bank of America (BAC) joined forces to develop the national strategy to combat identity crime, provide support to law enforcement and help improve consumer awareness and protection. For more information about the Identity Crime project visit the official Web site at: [www.idsafety.org](http://www.idsafety.org) or contact project staff via e-mail at [idsafety@theiacp.org](mailto:idsafety@theiacp.org).

## questions

The following questions are based on information in this *Training Key*®. Select the one best answer for each question.

1. In earlier years, police involvement in identity crime cases was minimal. This was due to which of the following factors?

- (a) Many states lacked laws making identity theft a crime.
- (b) Most identity crime operations are multijurisdictional enterprises, with perpetrator and victim often widely separated geographically.
- (c) Police officials generally lacked expertise in, or even awareness of, identity crime.
- (d) All of the above.

2. It is essential that police departments launch a concerted effort to help combat identity fraud. Which of the following is not a step in efforts to do so?

- (a) Ensure that police personnel have a comprehensive knowledge of identity crime, who commits it, and how it is committed.
- (b) Acquire all available information about identity crime and ensure that the handling of identity crime cases is included in the department's training curriculum, policies, and procedures.
- (c) Avoid working closely with other departments on identity crime cases, as with other types of crime.
- (d) Participate in the Federal Trade Commission's Identity Theft Clearinghouse.

3. Which of the following statements is true?

- (a) Complaints of identity theft should be taken by a police department in detail and in a manner consistent with the severity of the crime.
- (b) Police departments should keep on file a list of telephone numbers, addresses, Web sites, and other appropriate data necessary to enable the victim to contact these various agencies.
- (c) Police departments should provide every identity theft complainant with information about the steps that he/she should take to remedy personal and financial damage caused by the crime.
- (d) All of the statements are true.

## answers

- 1. (d) All of the above.
- 2. (c) Identity theft is commonly a multi jurisdictional crime, it is necessary for each department to cooperate closely with other agencies in identity theft cases.
- 3. (d) All of the statements are true.

## have you read...?

"The Identity Theft Data Clearinghouse: What's In It For You?" published by the Federal Trade Commission.

This clearinghouse allows police departments access to extensive information about identity crime.

