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.[1] The FTC estimates that nearly 8.5 million Americans were victims of some form of identity theft annually.[2] 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.[3]

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.[4,5] 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.[6] 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.[6] 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,[7] 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.[8] 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.

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. 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.
- 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.[9]

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.[10]

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, 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)[11]
- "Deter, Detect, Defend" booklet (2006)[12]
- "Identity Crisis: What to Do If Your Identity Is Stolen" (2005)[13]
- "ID Theft: What It's All About"[14]

Additional Resources for Law Enforcement

The Web site mentioned above (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 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

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

[2] Better Business Bureau, 2005.

[3] 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.

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

[5] Better Business Bureau, 2005.

[6]. Ibid.

[7] 18 U.S.C 1028, http://www.law.cornell.edu/uscode/18/usc_sec_18_00001028-000-.html.

[8] 18 U.S.C 1028A, http://www4.law.cornell.edu/uscode/18/1028A.html.

[9] IACP Matrix, http://idsafety.org/files/pdfs/state-by-state-id_crime_laws.pdf.

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

[11] Federal Trade Commission. "*Take Charge: Fighting Back Against Identity Theft*," February 2005, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

[12] http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

[13] http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.shtm.

[14] http://www.ftc.gov/bcp/conline/pubs/credit/idcrisis.shtm, August 2005.

[15] http://www.ftc.gov/bcp/conline/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 or contact project staff via e-mail at 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.