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.[1] 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.[2]

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. 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.[3]
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.[4]

   Law enforcement officers should also use the Identity Theft Data Clearinghouse,[5] 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[6], 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[7] 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)."[8] 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 and on the FTC's Web site at www.ftc.gov/idtheft.

Endnotes

[1] "*2008 Identity Fraud Survey Report*." Javelin Strategy and Research. February 2008: http://www.javelinstrategy.com/products/798BBF/97/delivery.pdf

[2] Ibid.

[3] "*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

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

[5] FTC's Identity Theft Data Clearinghouse: http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen09.pdf

[6] FTC Identity Theft Affidavit: http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf

[7] FTC Complaint Input Form: https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03

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