U.S. Department of Justice
Office of Community Oriented Policing Services

Problem-Oriented Guides for Police
Problem-Specific Guides Series
No. 25

Identity Theft

by Graeme R. Newman

www.PopCenter.org

Center for Problem-Oriented Policing

Got a Problem? We've got answers!

Log onto the Center for Problem-Oriented Policing website at www.popcenter.org for a wealth of information to help you deal more effectively with crime and disorder in your community, including:

- Web-enhanced versions of all currently available Guides
- Interactive training exercises
- On-line access to research and police practices

Designed for police and those who work with them to address community problems, www.popcenter.org is a great resource in problem-oriented policing.

Supported by the Office of Community Oriented Policing Services, U.S. Department of Justice.

Problem-Oriented Guides for Police
Problem-Specific Guides Series
Guide No. 25

Identity Theft

Graeme R. Newman

This project was supported by cooperative agreement #2002CKWX0003 by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Justice.

www.cops.usdoj.gov

ISBN: 1-932582-35-5

June 2004

About the Problem-Specific Guides Series

The *Problem-Specific Guides* summarize knowledge about how police can reduce the harm caused by specific crime and disorder problems. They are guides to prevention and to improving the overall response to incidents, not to investigating offenses or handling specific incidents. The guides are written for police–of whatever rank or assignment–who must address the specific problem the guides cover. The guides will be most useful to officers who

- **Understand basic problem-oriented policing principles and methods.** The guides are not primers in problem-oriented policing. They deal only briefly with the initial decision to focus on a particular problem, methods to analyze the problem, and means to assess the results of a problem-oriented policing project. They are designed to help police decide how best to analyze and address a problem they have already identified. (An assessment guide has been produced as a companion to this series and the COPS Office has also published an introductory guide to problem analysis. For those who want to learn more about the principles and methods of problem-oriented policing, the assessment and analysis guides, along with other recommended readings, are listed at the back of this guide.)

- **Can look at a problem in depth.** Depending on the complexity of the problem, you should be prepared to spend perhaps weeks, or even months, analyzing and responding to it. Carefully studying a problem before responding helps you design the right strategy, one that is most likely to work in your community. You should not blindly adopt the responses others have used; you must decide whether they are appropriate to your local situation. What is true in one place may not be true

elsewhere; what works in one place may not work everywhere.

- **Are willing to consider new ways of doing police business.** The guides describe responses that other police departments have used or that researchers have tested. While not all of these responses will be appropriate to your particular problem, they should help give a broader view of the kinds of things you could do. You may think you cannot implement some of these responses in your jurisdiction, but perhaps you can. In many places, when police have discovered a more effective response, they have succeeded in having laws and policies changed, improving the response to the problem.

- **Understand the value and the limits of research knowledge.** For some types of problems, a lot of useful research is available to the police; for other problems, little is available. Accordingly, some guides in this series summarize existing research whereas other guides illustrate the need for more research on that particular problem. Regardless, research has not provided definitive answers to all the questions you might have about the problem. The research may help get you started in designing your own responses, but it cannot tell you exactly what to do. This will depend greatly on the particular nature of your local problem. In the interest of keeping the guides readable, not every piece of relevant research has been cited, nor has every point been attributed to its sources. To have done so would have overwhelmed and distracted the reader. The references listed at the end of each guide are those drawn on most heavily; they are not a complete bibliography of research on the subject.

- **Are willing to work with other community agencies to find effective solutions to the problem.** The police alone cannot implement many of the responses discussed in the guides. They must frequently implement them in partnership with other responsible private and public entities. An effective problem-solver must know how to forge genuine partnerships with others and be prepared to invest considerable effort in making these partnerships work.

These guides have drawn on research findings and police practices in the United States, the United Kingdom, Canada, Australia, New Zealand, the Netherlands, and Scandinavia. Even though laws, customs and police practices vary from country to country, it is apparent that the police everywhere experience common problems. In a world that is becoming increasingly interconnected, it is important that police be aware of research and successful practices beyond the borders of their own countries.

The COPS Office and the authors encourage you to provide feedback on this guide and to report on your own agency's experiences dealing with a similar problem. Your agency may have effectively addressed a problem using responses not considered in these guides and your experiences and knowledge could benefit others. This information will be used to update the guides. If you wish to provide feedback and share your experiences it should be sent via e-mail to **cops_pubs@usdoj.gov**.

For more information about problem-oriented policing, visit the Center for Problem-Oriented Policing online at www.popcenter.org or via the COPS website at www.cops.usdoj.gov. This website offers free online access to:

- the *Problem-Specific Guides* series,
- the companion *Response Guides* and *Problem-Solving Tools* series,
- instructional information about problem-oriented policing and related topics,
- an interactive training exercise, and
- online access to important police research and practices.

Acknowledgments

The *Problem-Oriented Guides for Police* are very much a collaborative effort. While each guide has a primary author, other project team members, COPS Office staff and anonymous peer reviewers contributed to each guide by proposing text, recommending research and offering suggestions on matters of format and style.

The principal project team developing the guide series comprised Herman Goldstein, professor emeritus, University of Wisconsin Law School; Ronald V. Clarke, professor of criminal justice, Rutgers University; John E. Eck, associate professor of criminal justice, University of Cincinnati; Michael S. Scott, clinical assistant professor, University of Wisconsin Law School; Rana Sampson, police consultant, San Diego; and Deborah Lamm Weisel, director of police research, North Carolina State University.

Karin Schmerler, Rita Varano and Nancy Leach oversaw the project for the COPS Office. Suzanne Fregly edited the guides. Research for the guides was conducted at the Criminal Justice Library at Rutgers University under the direction of Phyllis Schultze.

The project team also wishes to acknowledge the members of the San Diego, National City and Savannah police departments who provided feedback on the guides' format and style in the early stages of the project, as well as the line police officers, police executives and researchers who peer reviewed each guide.

Contents

The Problem of Identity Theft

This guide addresses identity theft, describing the problem and reviewing factors that increase the risks of it.[†] It then identifies a series of questions to help you analyze your local problem. Finally, it reviews responses to the problem, and what is known about them from evaluative research and police practice.

Identity theft is a new crime, facilitated through established, underlying crimes such as forgery, counterfeiting, check and credit card fraud, computer fraud, impersonation, pickpocketing, and even terrorism. It became a federal crime in the United States in 1998, with the passage of the Identity Theft Assumption and Deterrence Act.[1] This act identifies offenders as anyone who

> …knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

A significant feature of identity theft is the offender's repeated victimization of a single person. This may include repeatedly using a stolen credit card, taking over a card account, or using stolen personal information to open new accounts.[††]

[†] The term identity fraud is sometimes used to include the whole range of identity theft related crimes (Economic Crime Institute 2003).

[††] A victimization survey conducted by the Federal Trade Commission (FTC) found that 16 percent of victims whose credit cards were misused said the people responsible had also tried to "take over" the accounts by doing such things as changing the billing address or adding themselves to the card as an authorized user (Federal Trade Commission 2003a).

Congressional hearings on identity theft in the 1990s revealed that police generally did not regard those whose identities had been stolen as the true victims, since the credit card companies took the financial loss. In addition, the companies typically did not report their losses to local police (or to anyone else, for that matter). Studies also showed that victims rarely reported the loss or theft of a card to the police, since they believed that the card company would cover the loss. However, because the repeated use of a victim's identity caused serious disruption and emotional damage, more victims began to report the offense.

It is likely that your initial exposure to identity theft will be the request of a victim for a police report about the incident. Credit-reporting agencies now require that victims do so as part of the an "identity theft affidavit." Until recently, victims had a hard time getting such reports from the police. However, in response to growing media coverage and congressional testimony concerning identity theft, the International Association of Chiefs of Police (IACP) adopted a resolution in 2000 urging all police departments to provide incident reports and other assistance to identity theft victims.[†] It is also possible that people you have stopped or questioned have given you a fake ID–or a legitimate ID acquired with a false or forged document.

It is difficult, though not impossible, for local police to influence some important factors that contribute to identity theft. These concern:

[†] "WHEREAS, reports of identity theft to local law enforcement agencies are often handled with the response 'please contact your credit card company,' and often no official report is created or maintained, causing great difficulty in accounting for and tracing these crimes, and leaving the public with the impression their local police department does not care…. RESOLVED, that the International Association of Chiefs of Police calls upon all law enforcement agencies in the United States to take more positive actions in recording all incidents of identity theft and referring the victims to the Federal Trade Commission…" (International Association of Chiefs of Police 2000).

- the ways that businesses and government agencies manage clients' personal information (for example, the procedures your motor vehicle department uses to authenticate driver's license applications); and
- the policies and practices of financial institutions in dealing with fraud (for example, the ease with which they provide applicants with credit cards and convenience checks).

That said, this guide will help you determine what you *can* do to prevent identity theft and help victims in your jurisdiction.

Related Problems

The following problems are closely related to identity theft, but not specifically addressed in this guide:

- Financial crimes against the elderly.[†]
- Various telemarketing and Internet scams.[22]
- Theft of autos and auto parts aided by fraudulent documentation. As the effectiveness of car security has increased in recent years, making cars more difficult to steal, offenders have exploited weaknesses in documentation systems that link cars to their owners, including registration and owner's certificates, license plates, and vehicle identification numbers.[3]
- Thefts from autos. Offenders commonly target wallets and purses, and dispose of their contents for profit.
- Burglary. Burglaries of residences or businesses may reward offenders with a wide range of personal and business records that can be converted into loans or bank accounts, or provide access to existing accounts.

[†] See the POP Guide on *Financial Crimes Against the Elderly.*

- Pickpocketing. Even if there is no credit card in a wallet, or even if the victim notifies the credit card issuer that a card has been stolen, the offender can use the victim's driver's license or other personal information to obtain a new card, or even establish credit with banks. Health insurance cards commonly list the holder's social security number as an identifier.
- Street robbery. Personal information and credit cards are an important target of muggers, who may sell such information and cards on the street.
- Counterfeiting and forgery. Offenders use the latest technologies to reproduce credit cards, checks, driver's licenses, passports, and other means of identification.
- Trafficking in human beings. Studies have found that stolen identities and false documentation are essential to successful international trafficking in prostitution and other illegal labor markets.[4]

Harms Caused by Identity Theft

- The FTC states that nearly 5 percent of respondents to its 2003 survey reported that they had been victims of identity theft in the past year.[5] This amounts to almost 15 million victims a year in the United States.
- The FTC reports that identity theft is the major subject of consumer complaints it receives–42 percent of all those received in 2003. Such complaints numbered 214,905, up 33 percent from the previous year, although the FTC does not believe this is a true measure of the increase in identity theft.[6]
- Identity theft victims experience long-term and well-documented pain and suffering,[7] such as harassment from debt collectors, banking problems, loan rejection, utility cutoffs, and even arrest for the identity thief's other crimes. In fact, since federal and state laws often protect victims against financial loss resulting from

identity theft, it is the disruption of their lives and the psychological damage suffered that are probably the worst aspects of their victimization. Victims spend, on average, 600 hours trying to clear damaged credit or even criminal records caused by the thief.[8]

- People fear having their identities stolen. In a recent poll, only one fear topped respondents' fear of having personal data stolen: that of another attack like the one on the World Trade Center.[9]
- The financial losses to consumers and businesses are enormous. The U.S. Secret Service estimated in 1997 that of the 9,455 cases investigated, consumers lost more than $745 million due to identity theft.[10] The 2003 FTC survey found that the total annual cost of identity theft to its victims was about $5 billion. Businesses, including financial institutions, lost another $47 billion in identity theft-related costs.[11]
- The cost to law enforcement ranges from $15,000 to $25,000 to investigate each case.[12]

Sources of Identity Theft Data

Data sources vary in quality and often provide conflicting or different estimates, especially concerning the extent and cost of identity theft. A recent problem is the tendency of businesses to exaggerate the threat of identity theft to sell products tailored to prevent it, such as insurance or software. Several sources supply data on identity theft:

- Government sources. The FTC was assigned the responsibility of collecting data as a result of the Identity Theft Act of 1998. Other data sources include the U.S. General Accounting Office, Social Security Administration, Postal Service, Department of Homeland Security, FBI, Secret Service, Sentencing

Commission, and congressional hearings on identity theft and fraud.
- Popular and trade media reports. These provide mostly anecdotal information and reinterpret reports from government sources.
- Credit reporting agencies.

The FTC's 2003 victimization survey provides the most reliable information to date.[13]

Factors Contributing to Identity Theft

Understanding the factors that contribute to your problem will help you frame your own local analysis questions, determine good effectiveness measures, recognize key intervention points, and select appropriate responses. There are few scientific studies on identity theft victims, offenders, or incidents, though there are studies on some identity theft-related crimes such as check and credit card fraud.†

† See the POP Guide on *Check and Card Fraud.*

†† See the POP Guide on *Financial Crimes Against the Elderly.*

Regarding victims, the most important findings concern the time taken to discover the theft:

- The longer it takes to discover the theft, the greater the victim's loss and suffering.[14]
- Low-income, less-educated victims take longer to discover or report the crime, resulting in greater suffering, especially from harassment by debt collectors, utility cutoffs, and banking problems.[15]

Victim characteristics are probably not related to identity theft vulnerability, though more research is needed in this area. The average age of victims is 42. They most often live in a large metropolitan area, and typically don't notice the crime for 14 months. Evidence suggests that seniors are less victimized by identity theft than the rest of the population, though they can be targeted in specific financial scams that may or may not involve identity theft.†† African Americans may suffer more from non-credit card identity theft, especially theft of telephone and other utility services, and check fraud.[16]

Regarding offenders, data from the above sources suggest they are attracted to identity theft for two important reasons:

- It is easy to commit because of the ready availability of personal information on the Internet, or contained in business files accessible to dishonest employees or burglars. Many people are not vigilant in protecting their personal information, and businesses are rarely held accountable for customer information accessed by those unauthorized to do so. Opportunities are legion. There are even websites that offer guides on how to create alternative IDs and to access other people's personal identifying information.[†]
- Victims don't typically discover the crime until some time after it has occurred–in some cases, years. If a retailer has lax security, and an offender gets away with using a stolen credit card, the legitimate cardholder may not realize it until receiving the next card statement.

Familiarity between victim and offender provides opportunities for identity theft because of the availability of personal information among relatives, coworkers, and others. According to the 1999-2001 FTC complaint files (see Figure 1), close to 11 percent of the complainants knew the offender. The FTC's 2003 survey found that 86 percent of victims had no relationship with the thief.[17] However, other sources claim closer to 60 percent of victims knew or had some information about the offender.[18]

Offenders' opportunities to commit identity theft may be classified under two broad categories: *place* and *guardianship*. The trouble is that committed offenders know very well where to find personal information, and the guardianship is not too effective.

[†] You can find out anyone's social security number for a small fee. Just visit http://www.docusearch.com/overture_ssn.html, or check out Undercover Press at http://www.aaffordable.com/best-sellers.html, which promotes itself as the "no questions asked source for Birth certificates, social security cards, city ID's, press cards, Diplomas, credentials of almost any kind including badges and police ID's."

- People carry personal information on them, which offenders may obtain via pickpocketing, mugging, or, if it is lost, simply finding it. People also leave personal information in cars or other places where experienced thieves know to look.
- Burglars can get information from victims' homes, and "Internet burglars," or hackers, can obtain personal identifying data from people's home computers.
- People's trash can serve as another source of information. People often throw away credit card statements, bank statements, and other documents containing personal information. Offenders may go through people's trash looking for such information.†
- People routinely give out personal information during business transactions, such as in shops and restaurants. Businesses that fail to use modern technology to protect customers' personal information create abundant opportunities for dishonest employees to steal customers' identities.

Agency Guardianship

There is an enormous amount of personal information available, and it is incredibly easy to obtain. Government agencies and businesses keep computerized records of their clients. They may sell or freely provide that information to other organizations.†† Often, all that is needed is one form of identification, such as a driver's license, and an offender can obtain the victim's mother's maiden name, social security number, etc.††† Many identity theft crimes are committed by employees of organizations that maintain client databases. For example, a widely publicized Detroit case involved an identity theft ring in which employees of a major credit card company stole

† In a study of 400 households in Nottingham, England, 40 percent of trashcans contained documents listing full credit and debit card numbers, as well as names, addresses, and expiration dates (Davis 2002).

†† U.S. residents do not own personal information contained in agency databases, so they have little control over how that information is used. Recent "opt-out" laws allow people to prevent their information from being provided to others, but these laws are not widely publicized.

††† Social security numbers are not so secure. A recent study estimated that 4.2 million people have managed to acquire alternative numbers (Finch 2003).

customer information.[20] Procedures for authenticating individual identities are often inadequate. Establishing a given person's "true identity" is a complex task. It requires the careful assessment of

- the person's biological identity (physical features, DNA, fingerprints, etc.);
- the person's historical identity (date of birth, marriage, etc.); and
- the link between those identities.[21]

Many agencies and businesses make only a cursory attempt–if any–to assess these.

How Offenders Steal Identities

The notoriety of identity theft rose with media coverage of the dangers of buying and selling on the Internet.[†] However, the ways offenders steal identities are decidedly low-tech. Computer hackers aren't necessarily geniuses; sometimes they simply obtain a password by trickery or from a dishonest insider. Some methods are more popular than others, as is clear from Figure 1, which is based on data collected by the FTC and reported by the General Accounting Office. In general, these data indicate that offenders make the most of the easiest available opportunities:

- They steal wallets or purses from shopping bags, from cars, or by pickpocketing.
- They steal mail, by several means. They may simply take it from insecure mailboxes, submit a false change-of-address form to the post office to direct someone's mail to themselves, or collude with a postal employee to steal mail that contains personal information. Mail

[†] Available data indicate that Internet-related identity theft constitutes a small proportion of all identity theft, probably less than 20 percent. However, there are many definitional problems here. For example, just one act of hacking into a database may reap thousands of credit card numbers and other personal data. These are then used to commit thousands of identity thefts offline. So it is wise to reserve judgment on this issue for now.

that is useful to offenders includes preapproved credit card applications, energy or telephone bills, bank or credit card statements, and convenience checks.

- They rummage through residential trashcans or through business dumpsters ("dumpster diving").
- They obtain people's credit reports by posing as someone who is legally permitted to do so, such as a landlord or employer.
- They collude with or bribe employees of businesses, government agencies, or service organizations, such as hospitals and HMOs, to obtain personnel or client records, or if they are employees, they access the information themselves.
- They break into homes to find personal information on paper or on personal computers.
- They hack into corporate computers and steal customer and employee databases, then sell them on the black market or extort money from the database owners for their return.
- They call credit card issuers and change the billing address for an account. The offender immediately runs up charges on the account, knowing that the victim will not receive the bill for some time, if ever.
- They buy identities on the street for the going rate (about $25), or buy credit cards that may be either counterfeit or stolen.
- They buy counterfeit documents such as birth certificates, visas, or passports. In 2001, the U.S. Immigration and Naturalization Service intercepted over 100,000 fraudulent passports, visas, alien registration cards, and entry permits.
- They buy false or counterfeit IDs on the Internet for as little as $50.

- They counterfeit checks and credit or debit cards, using another person's name. All the technology for reproducing plastic cards, including their holograms and magnetic strips, can be bought on the Internet.
- They steal PINS and user IDs, using software available on the Internet; trick Internet users into giving their passwords and other personal information; or watch users punch in their PINs on telephones or at ATMs.
- They use a single stolen ID to obtain legitimate IDs they can use for a wide variety of additional frauds.
- They gain entry into ID-issuing agencies, such as motor vehicle departments, by using bribery or extortion, or posing as employees.

How Offenders Use Stolen Identities

Offenders use victims' personal information in countless ways. Some of the most common examples follow:

- They open a new credit card account using the victim's name. All this requires, apart from the applicant's address, is usually a few pieces of information: the victim's mother's maiden name, the victim's birth date, and, sometimes, the victim's social security number.
- They open a landline or cell phone account in the victim's name.
- They open a bank account in the victim's name. They often open multiple accounts in multiple places, and write bad checks on each.
- They file for bankruptcy under the victim's name, to avoid paying their own debts or to avoid eviction.
- They steal the victim's identity, take over his or her insurance policies, and make false claims for "pain and suffering" suffered from auto accidents.[22]

- They take out auto loans or mortgages under the victim's name and residence.
- They submit fraudulent tax returns using the victim's identity, and collect the refunds.
- They submit applications for social security using others' identities (often those of people who have died), and receive social security payments.

Types of Identity Theft

Classifying identity theft into types is difficult, as it involves a wide variety of crimes and related problems. However, the acknowledged motives for identity theft can be used to construct a simple typology. Research indicates that the two dominant motives for identity theft are financial gain and concealment (either of true identity or of a crime).[†] These motives are mediated by the offenders' level of commitment to the task and the extent to which offenders are simply opportunists taking advantage of the moment.

Professionals who seek out targets and create their own opportunities–usually in gangs–have a high level of commitment. A lot of planning and organization is involved. Some lone offenders also display considerable commitment and planning, especially in regard to concealing personal history. Offenders with low commitment take advantage of opportunities in which ID theft appears to solve an immediate problem; thus their identity thefts are "opportunistic."

[†] The FTC survey reported that 15 percent of ID theft victims in the past five years had their personal information misused in nonfinancial ways. The most common such misuse was for the offender to give the victim's name and identifying information when stopped by law enforcement or charged with a crime (Federal Trade Commission 2003a).

As seen in Table 1, there are four types of identity theft, based on the combinations of commitment and motive. Of course, any single case could reflect aspects of more than one type.

	Financial gain	**Concealment**
High commitment (lots of planning)	*Organized.* A fraud ring systematically steals personal information and uses it to generate bank accounts, obtain credit cards, etc. (See box below.) *Individual.* The offender sets up a look-alike Internet website for a major company; spams consumers, luring them to the site by saying their account information is needed to clear up a serious problem; steals the personal/financial information the consumer provides; and uses it to commit identity theft.	*Organized.* Terrorists obtain false visas and passports to avoid being traced after committing terrorist acts.† *Individual.* The offender assumes another's name to cover up past crimes and avoid capture over many years.
Opportunistic (low commitment)	An apartment manager uses personal information from rental applications to open credit card accounts.	The offender uses another's name and ID when stopped or arrested by police.

Table 1
The Four Types of Identity Theft

High Commitment, for Financial Gain

Organized. In this type of identity theft, a group or gang carefully plans and orchestrates the crimes. Indeed, while it is widely believed that committing identity theft is easy because of the numerous opportunities described above, carrying out a truly successful identity theft requires considerable organization and preparation:

- searching for an easy target,
- locating sources of personal information for that target,

† An Algerian national facing U.S. charges of identity theft allegedly stole the identities of 21 members of a Cambridge, Mass., health club and transferred the identities to one of the people convicted in the failed 1999 plot to bomb Los Angeles International Airport (Willox 2002).

- obtaining the necessary documents (legal or counterfeit) to establish legitimacy,
- choosing how to use the identity to obtain money,
- convincing officials that one is the person named in identity documents, and
- anticipating how long one can exploit the identity before the victim discovers the losses.

Research has shown that organized criminal gangs in Southeast Asia manufacture plastic cards using stolen identities. These are then marketed on the street in large U.S. and European cities. Street fraudsters tend to specialize in particular types of card fraud. They use highly sophisticated techniques to avoid detection either when using the card in a retail store or when converting purchased goods into cash. They tend to work in small gangs, deal in high volume, and operate in high-population areas, usually 50 miles or more away from where they live.

A Classic Case of Organized Identity Theft for Financial Gain

Jane Sprayberry handed over her driver's license to an American Express customer service representative who had asked for it in order to replace Jane's lost credit card. True to the Amex promise, she received the replacement card without delay. The only trouble was that the recipient was not the real Jane Sprayberry. The driver's license had her name on it, but the photograph was not of her. In no time, the imposter ran up a big bill on high-priced jewelry, clothing, and appliances. Just a week before, Jane's husband's bank account had been emptied and his credit card cloned. A coincidence? Not at all. A ring of fraudsters in Detroit had gotten jobs at large businesses and had collected reams of personal information: personnel records, credit records, old rental-car agreements. Those offenders who were eventually caught had bags and books full of such records–records they had used over several years. They had run up an average of $18,000 in credit card charges per victim. And they had sold identities on the street for around $25 each. It took the real Jane Sprayberry and her husband more than six months to clean up the mess.[23]

Individual. Individuals may become strongly committed to the crime once they discover, after casually using someone's identity, how easy it is to get away with doing so. For example, someone with a drug habit may regularly buy stolen credit cards on the street (stolen cards are cheaper if others have used them), to raise money to buy drugs.

Opportunistic, for Financial Gain

The second type of identity theft occurs when the offender takes advantage of the access he or she has to the personal information of friends, family, or others. Examples include the following:

- A college student uses his or her roommate's personal information to apply for a preapproved credit card, which comes in the mail to which they both have access.
- A restaurant worker processes a customer's credit card payment and notices that the complete card number is printed out on the receipt, along with the expiration date. The worker copies the information and later makes several large purchases over the Internet, where he or she does not need to show the card or verify his or her identity.

High Commitment, for Concealment

Organized. Terrorism is the most recently cited instance of organized groups' stealing identities to conceal illegal activities, and to make tracking their true identities much more difficult after they've committed crimes. Authorities claim that all 19 of the September 11 terrorists were

Opportunistic, for Concealment

The most common type of opportunistic identity theft for concealment occurs when an offender gives the name of an acquaintance, friend, or family member when stopped, questioned, or arrested by police. Examples include the following:

- Jefferey Williams was jailed for 10 days without bail on a warrant for drug possession and resisting arrest. The Orange County (Fla.) Sheriff's Department had issued the warrant in Orlando. Williams insisted that he was not the person the police were looking for. The trouble was that Florida authorities were seeking a relative of Williams who had passed himself off as Jefferey, giving Jefferey's name, birth date, and old home address.[25]
- Lisa Sims (alias Elisa McNabney) assumed the name of her cellmate from a prior prison term to cover up her extensive criminal past and avoid arrest on suspicion of murdering her husband. Investigation revealed that she had multiple social security numbers and other forms of identity.[26]

Understanding Your Local Problem

The information provided above is only a generalized description of identity theft. You must combine the basic facts with a more specific understanding of your local problem. Analyzing the local problem carefully will help you design a more effective response strategy.

Asking the Right Questions

The following are some critical questions you should ask in analyzing your particular problem of identity theft, even if the answers are not always readily available. Your answers to these and other questions will help you choose the most appropriate set of responses later on. In some cases, the questions you should ask will be similar to those recommended regarding check and credit card fraud. If you find that such fraud figures heavily in the identity thefts you confront, you should also consult *Check and Card Fraud*, Guide No. 21 in this series.

Incidents

- Have checks, cards, or other forms of identity been targeted in crimes such as burglaries of homes and offices, pickpocketing in shopping malls, muggings, and thefts from cars?[†]
- What do reported cases of identity fraud usually entail: check or card fraud, Internet fraud, forged documents, false drivers' licenses, theft from cars?
- Who typically reports the crimes: individual victims, retailers, banks, or credit card issuers?

[†] A study issued by the U.S. Sentencing Commission that analyzed data on identity theft related cases from 1998 found that fewer than 10 types of ID were stolen or used, the most common being credit cards, driver's licenses, social security numbers, birth certificates, checks, and alien registration cards. The majority of the cases involved a single ID use (U.S. Sentencing Commission 1999).

- Is online fraud (from credit card sales) a problem in your area? Such fraud may become apparent when offenders order online but arrange to pick up merchandise at the store. Do merchants report any such instances?
- Are there any cases of parcels stolen or "lost" during delivery of items ordered online?
- Are there known fencing operations in or near your area? If so, what kinds of items are most commonly fenced, and are they traceable to any local stores? Do new items frequently appear in pawnshops?
- Are there increases in incidents such as car repossessions or collection agency activities?
- What is the local incidence of lost mail, mail diversions, and false filings of changes of address with the post office?
- If your jurisdiction is near a national border or entry point, what data are available on attempts at illegal entry using stolen or false documents?[†]

[†] In one study, fraudsters had worked out over 100 different ways of committing credit card fraud (Jackson 1994). In another, offenders displayed considerable innovation in switching from one technique of check forgery to another (Jackson 1994; Lacoste and Tremblay 2003).

Offenders

- Do identity thieves work alone, or in groups? How many work alone? How many work with others? How and where do they get together? How do they offend together? Why do they offend together?
- What are offenders' demographic characteristics, such as age and gender? Is there an ethnic component?
- Where do they live, work, or hang out?
- Do they know, or have they studied, their victims?
- How active are they? Do particular offenders account for a few identity thefts, or for many? Do they specialize in one particular method of committing identity theft?

- What, specifically, motivates them? Do they need quick cash to party or to support a family? Do they have any expensive addictions? Are they recently jobless, or are they long-term offenders?
- Do they show evidence of planning their crimes, or do they take advantage of easy opportunities?
- What special skills and techniques do they use to commit their crimes?

Victims

- How do victims respond to identity theft?
- Are particular people repeatedly victimized? If so, why?
- What do victims expect when they contact the police? How long do they wait before reporting the crime to the police?
- How long does it take for victims to discover that their identity has been stolen? Do they also report the theft to their credit card issuer and bank?
- How do businesses respond to their victimization? Do they routinely report check and card fraud to the police? (Some may be unwilling to do so for fear that police attention will drive business away, or, in the case of card fraud, because they do not have to bear the loss.) What kinds of businesses report identity fraud: small family stores, large retail chains, supermarkets, local or regional banks, etc.? Why do they report it?
- What are merchant attitudes regarding police involvement in dealing with identity theft?
- What procedures do merchants have for detecting or preventing identity theft?
- Are particular businesses repeatedly victimized? If so, why? (They may have inadequate security procedures in place.)
- Have any local businesses reported theft or loss of company records?

Locations/Times

- Do any of the crimes related to identity theft–wallet thefts, check and card fraud, account takeovers, use of fake driver's licenses–occur in a specific area, on a particular day, and/or at a particular time?
- Can cases of identity theft be traced back to particular supermarkets, electronics stores, retail chains, restaurants, online stores, or even car dealerships?
- Do muggings or thefts from cars that entail theft of credit cards and other personal documents occur in neighborhoods where drug dealing is common?
- Does fraud occur at checkout in local stores?
- Do thieves use methods that require them to travel to and from specific places? (Some identity thieves, once they have the necessary information, may open several bank accounts in a short period of time, write several large checks, then quickly leave the area).
- Do thieves use the telephone or Internet to convert their stolen identities into cash? Do they call stores from home, or from public phones? Do they access online stores from home computers, or from those available in public places (e.g., college campuses, public libraries, Internet cafes)?

Current Practices

- What databases are available to help you prevent or reduce identity theft? You may have access to a number of useful databases, or you may need to construct your own–given, of course, the resources to do it:

a. The Privacy Rights Clearinghouse recommends establishing a central database of lost or stolen driver's licenses, so that local police officers can check IDs against it. While this may seem obvious, information-sharing among agencies continues to be difficult. If your state does not already have such a database, clearly it will require considerable collaboration with law enforcement bodies and state agencies to create one.
b. The FTC's Identity Theft Data Clearinghouse is the central national repository of identity theft complaints. All local, state, and federal law enforcement officers can have free Internet access to this secure database. After your organization signs a confidentiality agreement with the FTC, you will be provided with a user ID and password. You can search the database for complaints relating to investigations you are working on, or find clusters of reports detailing suspicious activity regarding locations or people in your community. You can also receive e-mail notifications each time a complaint that relates to your interests hits the database. To learn more about Consumer Sentinel, go to http://www.ftc.gov/sentinel/. To join Consumer Sentinel, go to http://www.ftc.gov/sentinel/cs_signup.pdf.
c. Credit-issuing and reporting companies such as Visa and MasterCard also maintain databases of lost or stolen cards. You should establish ways of accessing these databases, which will require working with local banks and businesses with ties to those companies.

- Does your crime analyst (if your department has one) track crimes that relate to and facilitate identity theft? When victims report burglaries or thefts, tracking the use of stolen identity related items such as credit cards may provide clues concerning offenders' activities, such as which stores prefer. You may then work with the stores to improve security, if it is lax, and also to identify the thieves.
- Does your department have an established procedure for verifying and recording the identities offenders give when they are stopped, questioned, or arrested? Do officers receive training in ID authentication?
- Does your department have a crime reporting system that facilitates making a police report for identity theft or fraud?
- How do local agencies respond to ID theft? Do they have established reporting procedures?

Measuring Your Effectiveness

Measurement allows you to determine to what degree your efforts have succeeded, and suggests how you might modify your responses if they are not producing the intended results. You should take measures of your problem *before* you implement responses, to determine how serious the problem is, and *after* you implement them, to determine whether they have been effective. All measures should be taken in both the target area and the surrounding area. (For more detailed guidance on measuring effectiveness, see the companion guide to this series, *Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers*.)

The following are potentially useful measures of the effectiveness of responses to identity theft:

- Increases in incident reports (if you have raised awareness of identity theft in your community, including in your police department).
- Decreases in incident reports and fewer repeat offenders (if your prevention efforts have been effective).
- Increases in favorable media coverage (resulting from your efforts to raise awareness and sensitivity to the crime, and to publicize your department's responses to it).
- Increases in interdepartmental collaborations (resulting from your efforts to coordinate prevention and enforcement activities among relevant government agencies).
- Decreases in retail losses attributed to identity theft, especially check and card fraud. Retailers may use the number of transactions, or the total amount of sales, as the base against which they compute losses.
- Increases in measures businesses take to protect employee and client records and privacy (resulting from your work with them to increase security).
- Differences in reported frauds between stores or banks where you focus your activities and those where you do not (keeping in mind that changes may be due to other factors, and that reported crime does not always reflect actual crime).
- Reductions in related crimes such as burglaries, thefts from cars, or robberies at ATMs,[†] where credit cards, bankcards, or other forms of identity may be prime targets (keeping in mind that changes may be due to other factors related to those crimes).

[†] See the POP Guide on *Robbery at Automated Teller Machines*.

- Increases in related crimes when fraudsters' efforts are thwarted and they shift to easier targets (displacement). One study has suggested that acquisitive crime may increase as credit card fraud decreases.[27] Other studies have found that fraudsters tend not to switch easily between different types of credit card fraud,[28] though they are resourceful in shifting between different types of check fraud, or at least in inventing new ways to commit it.[29]
- Reductions in the number of new products fenced or available in pawnshops.

Responses to the Problem of Identity Theft

Your analysis of your local problem should give you a better understanding of the factors contributing to it. Once you have analyzed your local problem and established a baseline for measuring effectiveness, you should consider possible responses to address the problem. As noted at the beginning of this guide, some of the risk factors relating to identity theft may lie beyond the immediate influence of local police, or they may appear to lie beyond the usual scope of local police responsibility. These include:

- preventive measures businesses should take to safeguard their records from employee misuse or from outside intrusion;
- marketing or authentication practices of credit card or retail companies that make it easier for identity thieves to open card accounts or make fraudulent purchases;
- preventive measures government agencies should take to safeguard their records from employee misuse or from outside intrusion;
- technologies that make counterfeiting cards, checks, or other forms of identity easier for offenders;
- preventive measures people should take to safeguard their personal information;
- opportunities the Internet provides for purchase or theft of personal information; and
- actions credit-reporting agencies take in response to victims' requests for help in repairing their credit records.

However, studies of successful interventions to reduce or prevent check and credit card fraud have shown that there *are* things local police can do to impact some of the above factors. It requires the development of various partnerships with local and state government agencies and with businesses.[†]

[†] See the POP Guide on *Check and Card Fraud.*

The following response strategies provide a foundation of ideas for addressing your particular problem. These strategies are drawn from a variety of research studies and police reports. Several of these strategies may apply to your community's problem. It is critical that you tailor responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Law enforcement responses alone are seldom effective in reducing or solving the problem. Do not limit yourself to considering what police can do: give careful consideration to who else in your community shares responsibility for the problem and can help police better respond to it. In the case of identity theft, there are clear implications for businesses, other government agencies, and consumer advocacy groups.

General Considerations for an Effective Response Strategy

As we have seen, identity theft is a complex crime, composed of many sub-crimes and related to many other problems. Thus, identity theft crimes fall under the authority of many different agencies, including the local police, Secret Service, Postal Inspection Service, FBI, Homeland Security, local government offices, and motor vehicle departments, to name just a few. Regional and state law enforcement agencies may have established

multiagency task forces to combat identity fraud. For example, the Financial Crimes Task Force of Southwestern Pennsylvania consists of local law enforcement, Secret Service agents, and postal inspectors. At a minimum, multiagency task forces should include motor vehicle departments and local and state government agencies that keep public records. These multiagency task forces fulfill an important need because, at present, the Secret Service, which has primary responsibility for investigating identity theft, does not accept cases unless there is a financial loss of over $200,000 and a multistate fraud ring is involved. This leaves many victims in the lurch.

Thus, it will be important for you to work with local agencies to coordinate responses, so that you can participate more fully in designing and implementing preventive strategies. In addition, if local police have the first official contact with the victim, they can be an important investigative resource. FTC data indicate that the victim often knows who the offender is, or has significant amounts of information about the offender. In 2003, 62 percent of the complaints in the FTC identity theft database contained information about the offender.

However, because of the complexity–and expense–of developing multiagency task forces, your initial efforts should focus on local factors that will help reduce or prevent identity theft and mitigate the harm done to victims. Thus, the responses listed below are divided into two sections:

- Prevention: What to do to prevent identity theft from occurring in your jurisdiction.
- Victim assistance: How to respond to victims who come to you for help.

It should be emphasized that these two stages are closely related, and that collecting information in one stage helps in addressing the other. For example, obtaining information in the victim assistance stage will help you develop prevention strategies.[†]

[†] The costs to the victim–in terms of both out-of-pocket expense and time spent resolving problems–are substantially smaller if the misuse is discovered quickly. No out-of-pocket expenses were incurred by 67 percent of those who discovered misuse of their personal information within five months (Federal Trade Commission 2003b).

Finally, since identity theft occurs in conjunction with a variety of other crimes, and given the limited resources that may be available to you, it may not be feasible to address all such crimes at once. It may be more effective to be on the lookout for rashes of specific types of identity theft, such as credit card fraud or immigration fraud (if your jurisdiction is near an entry point). Focusing on a specific crime will make it easier to collect relevant information and to measure response effectiveness.

Specific Responses to Identity Theft

Prevention

1. Raising businesses' awareness of their responsibility to protect employee and client records. Offenders steal many identities from inadequately protected business records. There are many common-sense, low-tech ways to protect databases. You may work through local business associations, or establish working relationships with local businesses. Do not assume that all, or even most, businesses are aware of the opportunities afforded identity thieves by poor protection of their records. Many businesses do not institute security procedures because they do not consider them cost-effective. Mindful of businesses' reasonable concern for

profits, you should try to convince businesses that the costs of losing data, in terms of both their reputation with clients and possible lawsuits by victims, are much higher than those of following the many simple procedures to protect private information. State and/or federal laws such as GLB (Gramm-Leach-Bliley Act), HIPAA (HealthInsurance Portability and Accountability Act of 1996), and FACTA (Fair and Accurate Credit Transactions Act) require certain businesses or institutions to protect information better. The Internet provides considerable information on how businesses should protect their records. The Privacy Rights Clearinghouse recommends the following practices:

- Develop a comprehensive privacy policy that includes responsible information-handling procedures. Use a shredder or similar document-disposal method.
- Conduct regular staff training, new-employee orientations, and spot checks on proper information care.
- Support and participate in multiagency financial-crimes task forces.
- Limit data collection to the minimum of information needed; for example, limit requests for social security numbers.
- Put limits on data disclosure. For example, must social security numbers be printed on paychecks, parking permits, staff badges, time sheets, training program rosters, staff promotion lists, monthly account statements, client reports, etc.?
- Restrict data access to only those employees with a legitimate need to know. Audit electronic trails. Impose strict penalties for browsing and illegitimate access.

- Conduct employee background checks. Screen cleaning services, temp services, etc.
- Include responsible information-handling practices in business school courses, and even in elementary schools, if children have access to computers.

2. Educating people about protecting their personal information. The Internet has an enormous amount of information on how to avoid becoming an identity theft victim (see Appendix B for a selection of the main sources). Some police departments include special sections on identity theft on their websites, all with information on how to protect one's identity. To get the message out, you need to work through the community's main support organizations: schools, consumer advocacy groups, seniors' community centers and organizations, neighborhood watch meetings, and other community service groups. If your police department has a website, include information sources on protecting identity on the site. If budget permits, print out information brochures to hand out at meetings. The best publication on preventing identity theft is available free on the Internet or from the Federal Trade Commission: *Identity Theft: When Bad Things Happen to Your Good Name*. It should be emphasized, however, that there have been no scientific evaluations of the effectiveness of the advice given in this document and on many websites. Much of the advice is "common sense" (for example, don't leave personal information such as credit card statements in your trashcan).

3. Collaborating with government and other service organizations to protect private information. Social security numbers and driver's licenses are the two most common forms of identification used in the United States.

While identity theft awareness has increased considerably since the Identity Theft Act of 1998, agencies still need support in efforts to reduce the use of social security numbers as identifiers (very common on health insurance cards, for example), and local agency personnel may need to be constantly reminded of the risks involved in lax use of private information. Although some of the following recommendations are probably beyond the scope of local police, it is important that you work with agencies concerned about these issues, since it helps solidify your relationship with those whose help you may need to investigate identity theft cases or help victims resolve the problems they face, such as getting a new driver's license. The Privacy Rights Clearinghouse recommends the following practices:

- Keep social security numbers out of general circulation.
- Prohibit the use of social security numbers to obtain a driver's license, health insurance ID, or other forms of identification.
- Prohibit the sale of social security numbers, available now on information-broker websites.
- Maintain central clearinghouses in each state for lost and stolen driver's licenses.
- Conduct better photo- and ID-checking for new, duplicate, and replacement IDs.
- Restrict access to birth certificates in states where they are now publicly accessible.
- Remove social security numbers and other sensitive information from public records, especially when accessible on the Internet.

- Improve identity checking procedures for "instant" credit, favored by identity thieves.
- Put photographs on credit cards, or other authentication indicators such as smart chips or PINS.
- Request additional ID when verifying credit card purchases at the point of sale.
- Enable customers to put passwords on credit accounts.
- Truncate digits on account numbers printed on receipts at the point of sale.
- Use account-profiling systems to detect unusual activity. Notify the consumer of possible fraud.
- Check if there is an existing account in the applicant's name.
- Check the social security master-death index.
- Reduce the number of preapproved credit applications mailed to consumers. Don't mail such offers to anyone under 18. Print an opt-out phone number prominently on all such offers (1.888.5OPTOUT).
- Prohibit convenience checks, or at least provide an opt-out to credit card and bank customers.

5. Tracking delivery. Much of identity theft depends on the delivery of documents and products. Vacant houses or apartments are prime locations for delivery of products or diverted mail. Credit applications or driver's license renewal forms are at risk in mailboxes; products bought with stolen credit cards on the Internet are delivered to such addresses. Maintaining a close relationship with local postal inspectors and delivery companies such as UPS or FedEx may help you track items back to thieves. You can work with the local post office and delivery companies to train employees to:

- take note of deliveries to houses that are vacant or up for sale;
- spot driver's license renewals and credit card statements that go to unfamiliar addresses; and
- maintain records of applications to forward mail or packages (the Postal Service now requires people to show ID to submit a change-of-address or mail-forwarding application).

Victim Assistance

6. Working with the victim. Victims have many protections under federal and state law that prevent them from being liable for unauthorized charges, withdrawals, or other unlawful activities of identity thieves. They also have rights regarding the accuracy of their credit reports. Police need to understand how consumers are protected, and provide victims with educational resources that explain their rights and the steps they need to take to assert them. The FTC's comprehensive guide, *When Bad Things Happen to Your Good Name*, and its website, www.consumer.gov/idtheft, provide consumers with the information they need to deal with fraudulent debts and any negative credit-report information resulting from identity theft.

Communicating with victims is important, as well. The most frequent complaint the Identity Theft Resource Center receives is that "the police just don't care." It is important to let victims know that the police do care and do understand. Remember that identity theft victims have been repeatedly victimized. Identity theft is an emotionally harmful crime. Furthermore, you should be aware that

victims typically uncover more evidence in a case than do investigators, and more rapidly. Thus you should quickly develop a close working relationship with the victim. The steps you can take to do so are as follows:[31]

- Assure the victim that you will take a police or incident report and give him or her a copy. This is important because many, if not all, identity theft crimes fall under several jurisdictions. For example, the offender steals the credit card in one state and uses it in another; the card company is located in yet a different state; and the victim lives elsewhere. Even though there may be many cross-jurisdictional issues involved, you should immediately respond to the victim by preparing a police or incident report. Without one, the victim will have difficulty filing an identity theft affidavit. At a minimum, file a report with the FTC Consumer Sentinel database.
- Have available the Identity Theft Victim Guide, which outlines what steps a victim should take, and how the victim should prepare for the investigator's phone call or visit. It should be mailed to the victim, as well as available on your department's website. The guide should list what steps your department takes after receiving a complaint, and exactly what information and documentation the victim needs to provide when interviewed.
- Recommend that, for the initial meeting, the victim prepare a rough written draft of the case. The victim should provide his or her name and contact details; state when he or she discovered the fraud; list any fraudulent activity to date, in chronological order; list the affected accounts; and provide facts about the imposter, if any are known.

- At your initial meeting with the victim, he or she may be frustrated and angry. Inform the victim what it's like "behind the scenes" of a fraud investigation; what the procedures will be from this point forward; how soon it will be before a copy of the police report is available; when he or she will hear from you next; and what the chances are of catching the offender.
- Help victims to understand and exercise their rights under the federal credit laws. They will have to take many steps to restore their accounts, be released from fraudulent debts, and clean up their credit reports. Many of these steps must be followed up in writing. Therefore, direct the victim to Internet resources (such as the FTC website, www.consumer.gov/idtheft), or give the victim written materials that explain how the recovery process works. Help the victim secure the necessary paperwork, such as an identity theft affidavit, and give the victim a copy of the police or incident report regarding his or her case. Also give the victim information on how to contact the credit-reporting companies.
- Enter the victim's complaint information into the FTC's Identity Theft Data Clearinghouse, letting the victim know that you are doing so on his or her behalf, or advise the victim to file a complaint with the FTC, either online at www.consumer.gov/idtheft, or by calling 1.877.ID.THEFT (1.877.438.4338). Explain to the victim that while the individual identity theft complaint may not be enough to bring to a prosecutor, putting it into the national database will enable investigators across the country to combine it with any other complaints about the same offender, making prosecution more likely.

7. Preparing a plan to prevent or minimize the harm of identity theft when large identity databases have been breached. When a business or government agency reports that its employee records or client databases have been violated, police and others must act quickly to reduce the amount of time the thief has to use the stolen identities. Such a case occurred in California when a thief broke into state government databases and stole personal information of 265,000 employees, including the governor. The following steps were taken:

- Toll-free, dedicated phone lines were set up for employees to call the three major credit bureaus to warn of the theft.
- Employees received information packets on what to do to protect their identities and reduce damage, how to read credit reports, how a fraud alert on a credit file works, and so on.
- The state held workshops for employees, distributed videos, and launched a webpage with helpful information.

The FTC has published a response guide on what a business should do if files with customers' personal information have been compromised. It sets out a step-by-step plan and includes a model letter to notify customers whose information was compromised. The guide is available online at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtbizkit.htm.

Appendix A: Summary of Responses to Identity Theft

The table below summarizes the responses to identity theft, the mechanism by which they are intended to work, the conditions under which they ought to work best, and some factors you should consider before implementing a particular response. It is critical that you tailor responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Law enforcement responses alone are seldom effective in reducing or solving the problem.

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
Prevention					
1.	32	Raising businesses' awareness of their responsibility to protect employee and client records	You work with businesses to ensure that they follow best practices for securing personal records	…you have a good working relationship with local businesses	You must overcome businesses' concerns that security practices will affect their bottom line
2.	34	Educating people about protecting their personal information	You work with local schools and citizen and consumer groups to teach theft prevention techniques	…you use the wealth of information available on the Internet and provided by many federal and state agencies	This should be made a part of your department's regular outreach activities

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
3.	34	Collaborating with government and other service organizations to protect private information	You work with service agencies to reduce the use of social security numbers as identifiers	…you have a good working relationship with the agencies, especially those that issue identification documents	Your influence may be limited, depending on your reputation for dealing with identity theft, and the size of the government bureaucracy
4.	36	Working with local banks to encourage credit card issuers to adopt improved security practices	You urge banks to demand that credit card issuers develop better identity verification techniques	…you have a good working relationship with local banks	Credit card issuers are often international in scope, so their security practices might be beyond the influence of local financial institutions
5.	37	Tracking delivery	You work with the post office and delivery companies to monitor vacant residences and diverted deliveries of mail	…you help train delivery employees to spot suspicious deliveries	This requires considerable effort to maintain monitoring and training over time
Victim Assistance					
6.	38	Working with the victim	You adopt the victim as your partner in the investigation	…you address victim concerns early and show that you care, provide the victim with a copy of the police or incident report, and direct the victim to resources outlining the self-help steps he or she needs to take	Cross-jurisdictional issues may hamper your response and frustrate the victim; the number of identity theft incidents may initially appear to rise after you adopt a policy to write reports for all victims; the victim will still need to make follow-up phone

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
6. (cont'd)					calls and send follow-up documents to resolve their identity theft problems, which may prove burdensome
7.	41	Preparing a plan to prevent or minimize the harm of identity theft when large identity databases have been breached	You work with local businesses and service agencies to develop a disaster plan should massive theft of personal records occur	…you have a good working relationship with local agencies, so that the plan can be put into effect immediately to reduce the time the thief has to use stolen records	This requires coordination and cooperation between local businesses and government, and direct contact with national credit-reporting agencies

Appendix B: Selected Identity Theft Resources

Help for Victims and Others

- Major credit reporting agencies:
  Equifax, P.O. Box 74021, Atlanta, GA 30374-0241.
  Phone: 800.916.8800. www.equifax.com
  Experian (formerly TRW), P.O. Box 8030, Layton, UT 84041-8030. Phone: 888.397.3742.
  www.experian.com.
  TransUnion, P.O. Box 390, Springfield, PA 19064.
  Phone: 800.916.8800. www.transunion.com

- To file an identity theft complaint:

  By phone, toll-free: 877.ID.THEFT (877.438.4338)
  Online: www.consumer.gov/idtheft
  By mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, DC 20580

- To opt out of prescreened credit card offers by phone, toll-free: 888.5.OPT.OUT

- To learn about privacy choices for personal financial information online:
  http://www.federalreserve.gov/pubs/privacy/default.htm

Federal Government Resources

Department of Justice:
www.usdoj.gov/criminal/fraud/idtheft.html
FBI: http://www.fbi.gov/contact/fo/fo.htm
FTC: www.consumer.gov/idtheft and www.ftc.gov

Consumer Advocacy

AARP:
http://research.aarp.org/consume/dd85_idtheft.html
CALPIRG and USPIRG: www.pirg.org
ID Theft Resource Center for Law Enforcement:
http://www.idtheftcenter.org/lawenforcement.shtml
Identity Theft Survival Kit: www.identitytheft.org
Privacy Rights Clearinghouse: www.privacyrights.org

Law Enforcement Consortia

International Association of Financial Crime Investigators: http://www.iafci.org/home.html

Useful Documents

"Coping With Identity Theft: What to Do When an Impostor Strikes," by Privacy Rights Clearinghouse (Fact Sheet 17). www.privacyrights.org.

"Identity Theft Survival Kit" and "From Victim to Victor: A Step-by-Step Guide for Ending the Nightmare of Identity Theft," by Mari Frank. Available at www.identitytheft.org

"Identity Theft: When Bad Things Happen to Your Good Name," by Federal Trade Commission (September 2002). Phone: 877.ID.THEFT. www.consumer.gov/idtheft

Endnotes

[1] U.S. Public Law 105-318 (1998).
[2] Newman and Clarke (2003).
[3] Maxfield and Clarke (in press).
[4] United Nations Interregional Crime and Justice Research Institute (2003).
[5] Federal Trade Commission (2003a).
[6] Federal Trade Commission (2003c).
[7] CALPIRG (2000) and Identity Theft Resource Center (2003).
[8] Identity Theft Resource Center (2003).
[9] Goodwin (2003).
[10] Lease and Burke (2000).
[11] Federal Trade Commission (2003a).
[12] Personal communication, John McCullough, Minnesota Financial Crimes Task Force.
[13] Federal Trade Commission (2003a).
[14] Federal Trade Commission (2003a).
[15] Federal Trade Commission (2003a).
[16] Federal Trade Commission (2003).
[17] Verton (2001); Federal Trade Commission (2003a).
[18] Burns, Ronni (2004). Citicard presentation to Identity Theft Focus Group, Major Cities Chiefs Association, May 3.
[19] Cullier (2003).
[20] Davis (2001).
[21] Willox (2000).
[22] Willox (2000).
[23] Davis (2001).
[24] Willox (2002).
[25] Whitlock (1999).
[26] North County Times (2002).
[27] Levi and Handley (n.d.).
[28] Mativat and Tremblay (1997).
[29] Lacoste and Tremblay (2003).
[30] Newman and Clarke (2003), pp. 117-118, 126.
[31] Foley (2003).

References

CALPIRG (2000). *Nowhere to Turn: Victims Speak out on Identity Theft.* A CALPIRG/PRC Report–May. Sacramento, Calif.: Privacy Rights Clearinghouse.

Cullier, D. (2003). "WSU Study Shows Washingtonians Fear Identity Theft But Want Government to Operate in the Open." Washington State University News Service. Feb. 26. http://www.wsunews.wsu.edu/detail.asp?StoryID=3750

Davis, K. (2002). "Clean up Your Trash: A Home Shredder Is Insurance Against Identity Theft." *Kiplinger Personal Finance* 56(6):102.

——— (2001). "Anatomy of a Fraud." *Kiplinger's Personal Finance* 55(3):90.

Economic Crime Institute (2003). "Identity Fraud: A Critical National and Global Threat." White Paper. A Joint Project of the Economic Crime Institute of Utica College and LexisNexis. Oct. 28. http://www.ecii.edu/identity_fraud.pdf

Finch, E. (2003). "What a Tangled Web We Weave: Identity Theft and the Internet." In Y. Jewkes (ed.), *Dot.cons: Crime, Deviance, and Identity on the Internet.* Cullompton, England: Willan.

Federal Trade Commission (2003a). *Identity Theft Report.* http://www.ftc.gov/reports/index.htm

——— (2003b). *Overview of the Identity Theft Program,* October 1998–September 2003. http://www.ftc.gov/reports/index.htm

——— (2003c). *National and State Trends in Fraud and Identity Theft,* January–December 2003. http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

Foley, L. (2003). "Enhancing Law Enforcement–Identity Theft Communication." Identity Theft Resource Center. http://www..idtheftcenter.org

Goodwin, B. (2003). "Identity Theft Is Key Cybersecurity Fear." *Computerweekly.com.* April 17. http://194.203.155.34/Article121058.htm

Identity Theft Resource Center with Dale Pletcher (2003). Identity Theft–The Aftermath. http://www.idtheftcenter.org/library.shtml

International Association of Chiefs of Police (2000). "Curbing Identity Theft." *Resolutions.* http://www.theiacp.org/Resolutions/index.cfm?fuseaction=dis_public_view&resolution_id=20&CFID=138190&CFTOKEN=34557922

Jackson, J. (1994). "Fraud Masters: Professional Credit Card Offenders and Crime." *Criminal Justice Review* 19(1):24–55.

Lacoste, J., and P. Tremblay (2003). "Crime Innovation: A Script Analysis of Patterns in Check Forgery." *Crime Prevention Studies* 16:171–198.

Lease, M., and T. Burke (2000). "Identity Theft: A Fast-Growing Crime." *FBI Law Enforcement Bulletin* 69(8).

Levi, M., and J. Handley (n.d.). *Criminal Justice and the Future of Payment Card Fraud*. London: IPPR Criminal Justice Forum.

Mativat, F., and P. Tremblay (1997). "Counterfeiting Credit Cards: Displacement Effects, Suitable Offenders, and Crime Wave Patterns." *British Journal of Criminology* 37(2):165–183.

Maxfield, M., and R. Clarke (eds.) (in press). *Understanding and Preventing Auto Theft*. Crime Prevention Studies, Vol. 17. Monsey, N.Y.: Criminal Justice Press.

Newman, G., and R. Clarke (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. London: Willan.

North County Times (2002). "Woman Hangs Self in Jail." April 1, Back Page.

Schrader, A. (2003). "Colorado's Lax Laws Attract ID Thieves." *Denver Post*, Dec.1.

United Nations Interregional Crime and Justice Research Institute (2003). *Coalitions Against Trafficking in Human Beings in the Philippines*. Research and Action Final Report: Anti-Human Trafficking Unit. Vienna, Austria: United Nations. See also http://www.unodc.org/unodc/en/publications/publications_trafficking.html

U.S. General Accounting Office (2002). "Identity Fraud: Prevalence and Links to Illegal Alien Activities." Statement of Richard M. Stana, Director of Justice Issues. GAO-02-830T.

——— (1998). "Identity Fraud." Report No. GGD-98-100BR. http://www.gao.gov

U.S. Public Law 105-318 (1998). 105th Cong.112 Stat. 3007, (October 30, 1998). *Identity Theft Assumption and Deterrence Act of 1998.*

U.S. Sentencing Commission (1999). *Identity Theft: Final Report.* Economic Crimes Policy Team. Dec. 15.

Verton, D. (2001). "Identity Thefts Skyrocket, but Less Than 1% Occur Online." *Computerworld* 35(7).

Whitlock, Craig (1999). "The Suspect Really Was Someone Else." *Washington Post*, Aug. 18.

Willox, N. (2002). "Identity Fraud: Providing a Solution." *Journal of Economic Crime Management* 1(1).

——— (2000). "Identity Theft: Authentication as a Solution." National Fraud Center, Identity Theft Summit, March 15–16.

About the Author

Graeme R. Newman

Graeme R. Newman is a distinguished teaching professor at the School of Criminal Justice, University at Albany, State University of New York. He has published works in the fields of the history and philosophy of punishment, comparative criminal justice, private security, situational crime prevention, and ecommerce crime, and has written commercial software. He was the CEO of a publishing company for 15 years and, in 1990, established the United Nations Crime and Justice Information Network. Among the books he has written or edited are *Superhighway Robbery: Preventing Ecommerce Crime* (with Ronald V. Clarke), and *Rational Choice and Situational Crime Prevention* (with Ronald V. Clarke and Shlomo Shoham).

Recommended Readings

- ***A Police Guide to Surveying Citizens and Their Environments***, Bureau of Justice Assistance, 1993. This guide offers a practical introduction for police practitioners to two types of surveys that police find useful: surveying public opinion and surveying the physical environment. It provides guidance on whether and how to conduct cost-effective surveys.

- ***Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers***, by John E. Eck (U.S. Department of Justice, Office of Community Oriented Policing Services, 2001). This guide is a companion to the *Problem-Oriented Guides for Police* series. It provides basic guidance to measuring and assessing problem-oriented policing efforts.

- ***Conducting Community Surveys***, by Deborah Weisel (Bureau of Justice Statistics and Office of Community Oriented Policing Services, 1999). This guide, along with accompanying computer software, provides practical, basic pointers for police in conducting community surveys. The document is also available at www.ojp.usdoj.gov/bjs.

- ***Crime Prevention Studies***, edited by Ronald V. Clarke (Criminal Justice Press, 1993, et seq.). This is a series of volumes of applied and theoretical research on reducing opportunities for crime. Many chapters are evaluations of initiatives to reduce specific crime and disorder problems.

- ***Excellence in Problem-Oriented Policing: The 1999 Herman Goldstein Award Winners.*** This document produced by the National Institute of Justice in collaboration with the Office of Community Oriented Policing Services and the Police Executive Research Forum provides detailed reports of the best submissions to the annual award program that recognizes exemplary problem-oriented responses to various community problems. A similar publication is available for the award winners from subsequent years. The documents are also available at www.ojp.usdoj.gov/nij.

- ***Not Rocket Science? Problem-Solving and Crime Reduction***, by Tim Read and Nick Tilley (Home Office Crime Reduction Research Series, 2000). Identifies and describes the factors that make problem-solving effective or ineffective as it is being practiced in police forces in England and Wales.

- ***Opportunity Makes the Thief: Practical Theory for Crime Prevention***, by Marcus Felson and Ronald V. Clarke (Home Office Police Research Series, Paper No. 98, 1998). Explains how crime theories such as routine activity theory, rational choice theory and crime pattern theory have practical implications for the police in their efforts to prevent crime.

- ***Problem Analysis in Policing***, by Rachel Boba (Police Foundation, 2003). Introduces and defines problem analysis and provides guidance on how problem analysis can be integrated and institutionalized into modern policing practices.

- ***Problem-Oriented Policing***, by Herman Goldstein (McGraw-Hill, 1990, and Temple University Press, 1990). Explains the principles and methods of problem-oriented policing, provides examples of it in practice, and discusses how a police agency can implement the concept.

- ***Problem-Oriented Policing and Crime Prevention***, by Anthony A. Braga (Criminal Justice Press, 2003). Provides a through review of significant policing research about problem places, high-activity offenders, and repeat victims, with a focus on the applicability of those findings to problem-oriented policing. Explains how police departments can facilitate problem-oriented policing by improving crime analysis, measuring performance, and securing productive partnerships.

- ***Problem-Oriented Policing: Reflections on the First 20 Years***, by Michael S. Scott (U.S. Department of Justice, Office of Community Oriented Policing Services, 2000). Describes how the most critical elements of Herman Goldstein's problem-oriented policing model have developed in practice over its 20-year history, and proposes future directions for problem-oriented policing. The report is also available at www.cops.usdoj.gov.

- ***Problem-Solving: Problem-Oriented Policing in Newport News,*** by John E. Eck and William Spelman (Police Executive Research Forum, 1987). Explains the rationale behind problem-oriented policing and the problem-solving process, and provides examples of effective problem-solving in one agency.

- ***Problem-Solving Tips: A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships*** by Karin Schmerler, Matt Perkins, Scott Phillips, Tammy Rinehart and Meg Townsend. (U.S. Department of Justice, Office of Community Oriented Policing Services, 1998) (also available at www.cops.usdoj.gov). Provides a brief introduction to problem-solving, basic information on the SARA model and detailed suggestions about the problem-solving process.

- ***Situational Crime Prevention: Successful Case Studies***, Second Edition, edited by Ronald V. Clarke (Harrow and Heston, 1997). Explains the principles and methods of situational crime prevention, and presents over 20 case studies of effective crime prevention initiatives.

- ***Tackling Crime and Other Public-Safety Problems: Case Studies in Problem-Solving***, by Rana Sampson and Michael S. Scott (U.S. Department of Justice, Office of Community Oriented Policing Services, 2000) (also available at www.cops.usdoj.gov). Presents case studies of effective police problem-solving on 18 types of crime and disorder problems.

- ***Using Analysis for Problem-Solving: A Guidebook for Law Enforcement***, by Timothy S. Bynum (U.S. Department of Justice, Office of Community Oriented Policing Services, 2001). Provides an introduction for police to analyzing problems within the context of problem-oriented policing.

- ***Using Research: A Primer for Law Enforcement Managers***, Second Edition, by John E. Eck and Nancy G. LaVigne (Police Executive Research Forum, 1994). Explains many of the basics of research as it applies to police management and problem-solving.

Other Problem-Oriented Guides for Police

Problem-Specific Guides series:

1. **Assaults in and Around Bars.** Michael S. Scott. 2001. ISBN: 1-932582-00-2
2. **Street Prostitution.** Michael S. Scott. 2001. ISBN: 1-932582-01-0
3. **Speeding in Residential Areas.** Michael S. Scott. 2001. ISBN: 1-932582-02-9
4. **Drug Dealing in Privately Owned Apartment Complexes**. Rana Sampson. 2001. ISBN: 1-932582-03-7
5. **False Burglar Alarms.** Rana Sampson. 2001. ISBN: 1-932582-04-5
6. **Disorderly Youth in Public Places.** Michael S. Scott. 2001. ISBN: 1-932582-05-3
7. **Loud Car Stereos.** Michael S. Scott. 2001. ISBN: 1-932582-06-1
8. **Robbery at Automated Teller Machines.** Michael S. Scott. 2001. ISBN: 1-932582-07-X
9. **Graffiti.** Deborah Lamm Weisel. 2002. ISBN: 1-932582-08-8
10. **Thefts of and From Cars in Parking Facilities.** Ronald V. Clarke. 2002. ISBN: 1-932582-09-6
11. **Shoplifting.** Ronald V. Clarke. 2002. ISBN: 1-932582-10-X
12. **Bullying in Schools.** Rana Sampson. 2002. ISBN: 1-932582-11-8
13. **Panhandling.** Michael S. Scott. 2002. ISBN: 1-932582-12-6
14. **Rave Parties.** Michael S. Scott. 2002. ISBN: 1-932582-13-4
15. **Burglary of Retail Establishments.** Ronald V. Clarke. 2002. ISBN: 1-932582-14-2
16. **Clandestine Drug Labs.** Michael S. Scott. 2002. ISBN: 1-932582-15-0
17. **Acquaintance Rape of College Students.** Rana Sampson. 2002. ISBN: 1-932582-16-9
18. **Burglary of Single-Family Houses.** Deborah Lamm Weisel. 2002. ISBN: 1-932582-17-7
19. **Misuse and Abuse of 911.** Rana Sampson. 2002. ISBN: 1-932582-18-5

20. **Financial Crimes Against the Elderly.** Kelly Dedel Johnson. 2003. ISBN: 1-932582-22-3
21. **Check and Card Fraud.** Graeme R. Newman. 2003. ISBN: 1-932582-27-4
22. **Stalking.** The National Center for Victims of Crime. 2004. ISBN: 1-932582-30-4
23. **Gun Violence Among Serious Young Offenders.** Anthony A. Braga. 2004. ISBN: 1-932582-31-2
24. **Prescription Fraud.** Julie Wartell, Nancy G. La Vigne. 2004. ISBN: 1-932582-33-9
25. **Identity Theft**. Graeme R. Newman. 2004 ISBN: 1-932582-35-3

Response Guides series:

- **The Benefits and Consequences of Police Crackdowns.** Michael S. Scott. 2003. ISBN: 1-932582-24-X

Problem-Solving Tools series:

- **Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers.** John E. Eck. 2002. ISBN: 1-932582-19-3

Upcoming Problem-Oriented Guides for Police

Problem-Specific Guides
Crimes Against Tourists
Disorder at Budget Motels
Domestic Violence
Mentally Ill Persons
Robbery of Taxi Drivers
Student Party Disturbances on College Campuses
School Break-Ins
Street Racing
Bomb Threats in Schools
Underage Drinking

Open-Air Drug Markets
Sexual Offenses in Public Places
Drunk Driving
Cruising
Bank Robbery

Response Guides
Closing Streets and Alleys to Reduce Crime

Problem-Solving Tools
Repeat Victimization
Using Offender Interviews to Inform Police Problem-Solving

Other Related COPS Office Publications

- **Using Analysis for Problem-Solving: A Guidebook for Law Enforcement.** Timothy S. Bynum.
- **Problem-Oriented Policing: Reflections on the First 20 Years.** Michael S. Scott. 2001.
- **Tackling Crime and Other Public-Safety Problems: Case Studies in Problem-Solving.** Rana Sampson and Michael S. Scott. 2000.
- **Community Policing, Community Justice, and Restorative Justice: Exploring the Links for the Delivery of a Balanced Approach to Public Safety.** Caroline G. Nicholl. 1999.
- **Toolbox for Implementing Restorative Justice and Advancing Community Policing.** Caroline G. Nicholl. 2000.
- **Problem-Solving Tips: A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships.** Karin Schmerler, Matt Perkins, Scott Phillips, Tammy Rinehart and Meg Townsend. 1998.

- **Bringing Victims into Community Policing.** The National Center for Victims of Crime and the Police Foundation. 2002.
- **Call Management and Community Policing.** Tom McEwen, Deborah Spence, Russell Wolff, Julie Wartell and Barbara Webster. 2003.
- **Crime Analysis in America.** Timothy C. O'Shea and Keith Nicholls. 2003.
- **Problem Analysis in Policing.** Rachel Boba. 2003.
- **Reducing Theft at Construction Sites: Lessons From a Problem-Oriented Project.** Ronald V. Clarke and Herman Goldstein. 2003.
- **The COPS Collaboration Toolkit: How to Build, Fix, and Sustain Productive Partnerships.** Gwen O. Briscoe, Anna T. Laszlo and Tammy A. Rinehart. 2001.
- **The Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!).** Kelly J. Harris and William H. Romesburg. 2002.
- **Theft From Cars in Center City Parking Facilities - A Case Study.** Ronald V. Clarke and Herman Goldstein. 2003.

For more information about the *Problem-Oriented Guides for Police* series and other COPS Office publications, please call the Department of Justice Response Center at 800.421.6770 or visit COPS Online at www.cops.usdoj.gov.

For More Information:

U.S. Department of Justice
Office of Community Oriented Policing Services
1100 Vermont Avenue, N.W.
Washington, D.C. 20530

To obtain details on COPS programs, call the
COPS Office Response Center at 800.421.6770

Visit COPS Online at the address listed below.

e05042360 Updated Date: July 26, 2004
ISBN: 1-932582-35-5