National Institute of Justice
The Research, Development, and Evaluation Agency of the U.S. Department of Justice
NIJ

Identity Theft—A Research Review

This online publication is based upon ***Identity Theft Literature Review***, by Graeme R. Newman and Megan M. McNally, final report to the National Institute of Justice, July 2005, NCJ 210459, referred to throughout this publication as “the full report.” Access the report online at http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=210459.

July 2007

Introduction

Identity theft has become perhaps the defining crime of the information age, with an estimated 9 million or more incidents each year.[1] Publicity regarding severe cases of identity theft in the print and electronic media and portrayal of the risk of identity theft in a number of effective television commercials have raised public awareness about identity theft. Arguably, however, few persons are aware of the complexities of the many issues involved with this crime, which is really a large set of fraudulent activities ranging in size from minor swindles to major crimes using stolen identities. These fraudulent actions are perpetrated by a broad spectrum of offenders, from family members to shadowy, international criminal gangs.

See also...
Section 10 of the full report: Conclusions and Recommendations, pp. 73–78

Over the past decade, the Federal Government and most States have passed legislation to impose criminal sanctions on identify theft (see Identity Theft Legislation). Efforts to combat identity theft have been hampered, however, by the elusiveness of a definition, its overlap with the elements of many other crimes, its long-term and multijurisdictional nature (including the time that may elapse before discovery), and questions as to whether law enforcement agencies or financial institutions are better equipped to combat it.

This NIJ-sponsored study drew from available scientific studies and other sources (through January 2005) to assess what is known about identity theft and what further research is needed. The study's researchers call for further research in areas relating to prevention, including reduction of harm to individual victims, financial institutions, and society.

What did the researchers find?

- Although anyone is potentially vulnerable to identity theft (particularly theft of credit card-related information), individuals are more likely to be victimized by persons who have access to their identifying information, such as family members and persons with whom they share living quarters.
- Identity theft generally involves three stages: acquisition, use, and discovery. Evidence suggests that the longer it takes to discover the theft, the greater the loss incurred and the smaller the likelihood of successful prosecution. Older persons and those with less education are less likely to discover the identity theft quickly and to report it after discovery.

- The access to personal information about potential victims and the anonymity the Internet offers would-be thieves are major facilitators of identity theft.
- More research is needed to identify the best ways to prevent identity theft crimes. Research should address the three main areas of vulnerability to identity theft—
    1. Practices and operating environments of document-issuing agencies that allow offenders to exploit opportunities to obtain identity documents.
    2. Practices and operating environments of document-authenticating agencies that allow offenders access to identity data, subsequently used for financial gain, avoiding arrest, or remaining anonymous.
    3. The structure and operations of the information systems involved with the operational procedures of agents in (1) and (2).
- Harm from identity theft crimes involves individuals and businesses. The extent of harm done to the victims and to society at large is unknown.

[1] Better Business Bureau, "New Research Shows That Identity Theft Is More Prevalent Offline With Paper Than Online," Exit Notice Press release, January 26, 2005.

Defining Identity Theft

No accepted definition of identity theft existed until Congress passed the Federal Identity Theft and Assumption Deterrence Act of 1998. This statute defines identity theft very broadly, making it easier for prosecutors to conduct their cases. It is of little help to researchers, however, because a close examination reveals that identity theft is composed of a number of disparate types of crimes committed in widely varying venues and circumstances.

The majority of States have now passed identity theft legislation, but these statutes, while often similar, do not define identity theft consistently. (See Identity Theft Legislation.)

The difficulty in defining identity theft has been the biggest impediment to conducting scientific research on identity theft and interpreting the findings of that research. This is because a considerable number of different crimes may include the use or abuse of another's identity or identity-related factors. Such crimes include—

See also...
From the full report:
Section 2, Definition of Identity Theft, pp. 1–3

Section 8, Legislation, pp. 63–65

- Check fraud.
- Plastic card fraud (credit cards, check cards, debit cards, phone cards, etc.).
- Immigration fraud.
- Counterfeiting.

- Forgery.
- Terrorism using false or stolen identities.
- Theft of various kinds (pick pocketing, robbery, burglary, or mugging to obtain the victim's personal information).
- Postal fraud.

Extent and Patterns of Identity Theft

The Federal Trade Commission (FTC) provides the best available estimates of the extent and distribution of identity theft from its victimization surveys and database of consumer complaints. A recent estimate, produced by a study modeled after the FTC's original 2003 methodology, suggests that 9.3 million adults were victims of some form of identity theft in 2004.[1] This may represent a leveling-off from the FTC's previous finding of 9.91 million in 2003.[2]

Although the incidence of identity theft differs by State, region, and, to some extent, age, the available data suggest that all persons, regardless of social or economic background, are potentially vulnerable, especially to those types of identity theft that occur when an offender steals a complete database of credit card information.

See also...
Section 4 of the full report: Extent and Patterning of Identity Theft, pp. 7–30

Evidence also indicates that individuals are more likely to be victimized by those who have easy access to their personal information (see exhibit 1). These identity thieves may include family members and relatives (who know or have access to identifying information such as date of birth, mother's maiden name, and Social Security number) or those with whom they live in close contact, such as fellow residents of college dormitories or military barracks.

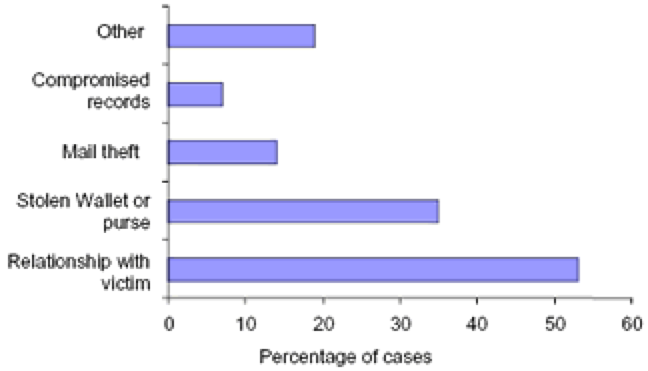
Identity thieves have developed various techniques to exploit the opportunities of the information age; however, most of the ways that offenders steal identities are relatively unsophisticated—stealing wallets or purses, stealing mail, rummaging through residential trashcans or business dumpsters, obtaining credit reports by posing as someone authorized to do so such as a landlord or employer, bribing employees of businesses, agencies, or service organizations to obtain personal information, and many other nontechnological means.

Offenders use the identities to open new credit card, phone, or bank accounts, file for bankruptcy, take over insurance policies and make false claims, obtain auto loans or mortgages, file fraudulent tax returns, etc.

There are many data and measurement issues concerning identity theft. The crime is likely underreported, both by individuals and by agencies and businesses. Discovery may occur many months or even years after the fraud was committed.

In 2004, 61 percent of identity theft victims did not report the crime to the police.[3]

Exhibit 1. How personal information is obtained



Note: Figures add up to more than 100% because one victim may report multiple methods. Shows only victims who reported to the FTC how their information was stolen during 1999 to 2001, about 20.5% of all victims who reported during that period.

Source: U.S. General Accounting Office, Identity Theft: Prevalence and Cost Appear to Be Growing, March 2002, GAO-02-363:27.

A recent study found that identity theft crimes are committed more frequently offline than online, and that victims who accessed their accounts online discovered their victimization significantly faster than those who relied on paper bill or statement monitoring.[4] As a result, the researchers recommend that individuals use Internet account management to reduce risk. The conclusion that online account monitoring is safer is problematic, however, and requires further investigation. The risk posed by online activities may increase, as their volume increases and more offenders become skilled at capitalizing upon them.

For the best sources of data (and sources used in this report), see Other Resources.

Extent of the problem: Unknown. Estimates range from three quarters of a million victims annually to more than 9 million as noted above. The source of any estimate should be scrutinized because of the many problems associated with collecting this data. As a result of the myriad of factors that affect estimates and until the issues are clearly delineated and properly recorded and resolved, the true extent of identity theft will remain unknown.

[1] Better Business Bureau, "New Research Shows That Identity Theft Is More Prevalent Offline With Paper Than Online," Press release, January 26, 2005.

[2] Synovate, "Federal Trade Commission—Identity Theft Survey Report," Report prepared for the Federal Trade Commission, McLean, VA: Federal Trade Commission, September 2003.

[3] See figure 1, Reporting to the Police, in section 4, page 10 of the full report.

[4] Better Business Bureau, "New Research Shows That Identity Theft Is More Prevalent Offline With Paper Than Online," Press release, January 26, 2005.

Types of Identity Theft

Depending on the definition of identity theft, the most common type is credit card fraud of various kinds. Evidence indicates that the extent of credit card fraud on the Internet (and by telephone) has increased because of the opportunities provided by the Internet environment. Some researchers prefer not to include credit card fraud in true identity theft, since it may occur only once and may be discovered quickly by the credit card issuing company, often even before the individual cardholder knows that the fraud has occurred. Other types of identity theft, such as account takeover, are more involved and take longer to identify and investigate.

See also...
Section 3 of the full report: Types of Identity Theft, pp. 3–7

Seven broad types of identity theft—

- Exploiting weakness in specific technologies and information systems.
- Financial scams.
- As a motive for other crimes (e.g., bribing employees to provide passwords).
- Facilitating other crimes.
- Avoiding arrest.
- Repeat victimization ("classic" identity theft).
- Organized identity theft.

Stages of Identity Theft

The researchers categorized three stages of identity theft. A particular identity theft crime may include one or all of these stages.

1. Acquisition
2. Use
3. Discovery

See also...
Executive Summary of the full report: p. v; and section 10, p. 75

Stage 1. Acquisition of the identity through theft, computer hacking, fraud, trickery, force, redirecting or intercepting mail, or even by legal means (e.g., purchasing identifying information on the Internet).

Stage 2. Use of the identity for financial gain (the most common motivation) or to avoid arrest or otherwise hide one's identity from law enforcement or other authorities (such as bill collectors). Crimes in this stage may include:

- Account takeover.
- Opening new accounts.
- Extensive use of the victim's debit or credit card.
- Sale of the identity information on the street or black market.
- Acquisition ("breeding") of additional identity-related documents such as driver's licenses, passports, visas, and health insurance cards.
- Filing fraudulent tax returns for large refunds.
- Insurance fraud.
- Stealing rental cars.

Stage 3. Discovery of the theft—although many misuses of credit cards are discovered quickly, identity theft may take from 6 months to several years to discover. Evidence suggests that the longer it takes to discover the theft, the greater the loss incurred by the victim, who may or may not involve law enforcement. Considerably more research is needed in this area.

Recording and Reporting Identity Theft

According to Federal Trade Commission research, older persons and those less educated are likely to take longer to report identify theft and are less likely to report it at all. This research also suggests that the longer it takes to discover the crime and report it to the relevant authority, the greater the loss and suffering of the victim, and, from a criminal justice perspective, the poorer the chance of successful disposition of the case.

In contrast to FTC's extensive database of consumer complaints and victimization, the criminal justice system lacks any such information related to identity theft. No criminal justice agency maintains a national database of the number of identity theft cases reported to it or those disposed of by arrest and subsequent prosecution. The FBI and the U.S. Secret Service have reported numbers of cases of identity theft that they have investigated in recent years, but these number only in the hundreds, and without State, multiagency, and local data, no means is currently available to determine the amount of identity theft confronted by the criminal justice system.

See also...
Section 7 of the full report: The Law Enforcement Response to Identity Theft, "Recording and Reporting of Identity Theft", p. 47

Criminal justice authorities, especially local police, have been thwarted in recording and reporting identity theft crimes by three significant issues:

1. The difficulty of defining identity theft because of its extensive involvement in other crimes. Most police departments lack an established mechanism to record identity-theft-related incidents as separate crimes. This is exacerbated by the lack of training of police officers in identifying and recording information concerning other crimes that also involve identity theft.
2. The cross-jurisdictional character of identity theft, which may span several geographically distant jurisdictions. This has led to jurisdictional confusion as to who is responsible for recording the crime. Although the International Association of Chiefs of Police has tried to resolve this issue, significant hurdles must still be overcome.
3. Depending on the type of identity theft, individuals are more likely to report their victimization to their bank, credit card issuing agency, or another financial agency rather than the police. Thus, a genuine issue arises as to the extent to which police are the appropriate agency to deal with this type of victimization, when many financial agencies are in a better position to attend to the victim's problems and even to investigate the crimes (which many do). For this reason, police agencies have strong motivation to avoid taking on the added responsibility for dealing with these crimes.

Law Enforcement Issues and Response

Since passage of the 1998 Federal identity theft law and subsequent legislation,[1] (see Identity Theft Legislation), much attention has been given to police response to victims. The 1998 law gave prime responsibility to the Federal Trade Commission to assist consumers who have been victimized. Legislation requiring credit reporting agencies to respond quickly to correct victims' records will likely increase the number of reports to police, since affidavits filed by victims with credit agencies require a police report.

See also...
Section 7 of the full report: The Law Enforcement Response to Identity Theft, pp. 47–63

The International Association of Chiefs of Police and Bank of America's ID Safety Web site has resources for law enforcement and other criminal justice agencies on identity theft.

Two issues need to be researched regarding police response to identity theft:

- Crime incident reporting. Information concerning identity theft lies in many different places. It may be a prime or facilitating motive in such traditional crimes as robbery, pick-pocketing, theft from cars, burglary, etc. Do police crime incident reporting systems have sufficient flexibility to collect such information, and if so, are line officers instructed to record it?

- Flexibility of information systems. Does the crime incident database structure used by the police department allow a crime analyst to check across many different crime types or incidents to pick up on any identity-theft-related issues or patterns?

What did the researchers find?

See also...
Section 7 of the full report: The Law Enforcement Response to Identity Theft, "Task Forces and Cross Jurisdictional Issues", pp. 51–56

No research has been conducted on the effectiveness of police response to victim needs. Evidence available is mostly anecdotal, either collected by various interests or victim testimony to congressional committees.

Despite the lack of research results on police awareness of identity theft, the researchers found many recommendations for police response to alleviate the harm done to victims, chiefly:

- Quick police response mitigates harm.
- Education through community outreach (such as a Web site) may help victims know where to turn and reduce their suffering.
- Effective communication is needed—the FTC reports that the most common complaint is that the police "just don't care." In responding to the victim's request for a report or an investigation, police are urged to "adopt the victim as a partner."
- A crisis response plan that will reduce the harm of a major theft of an agency or business's records is essential in minimizing the damage. The researchers ask, however, "is it the responsibility of law enforcement … to ensure that businesses and agencies have such a response plan?"

A National Strategy to Combat Identity Theft

In June 2006, the U.S. Department of Justice's Office of Community Oriented Policing Services released this report about identity theft issues and police challenges in responding to the problem. The report describes the components of the national strategy and includes best practices.

Aside from providing anonymity, identity theft offers many offenders the advantage of physical distance, a serious problem for both victims and authorities attempting to bring offenders to justice. Jurisdictional issues complicate the reporting, investigation, and prosecution of identity theft cases, as well as the creation and effectiveness of related legislation.

Identity theft is often wrapped up in other offenses that may involve intricate components. Examples of difficulties law enforcement and prosecutors face are:

- Offenders' identities may be difficult to ascertain; an offender may use several identities or aliases, which can confuse investigations.
- A single piece of information may be obtained from several different sources, which is time consuming and difficult for investigators to track.
- Offenders may commit crimes using a victim's identity, causing the victim to be arrested. One study reported that "on average, law officers surmised that only 11 percent of identity theft cases received by their departments are solved."[2]

Overall, the ability to link information in identity theft investigations is critical, and more work should be done to obtain information-sharing agreements among relevant agencies and jurisdictions.

[1] Fair Credit Reporting Act, section 609(e). 2003 amendments to this Act make it easier for police to obtain financial records of a victim without a subpoena, so long as they have the victim's consent.

[2] Gayer, J., "Policing Privacy: Law Enforcement's Response to Identity Theft," PDF California: CALPIRG Education Fund, 2003. Exit Notice

Cost of Identity Theft

Business

See also...

Section 5 of the full report: Cost of Identity Theft, pp. 30–37

Focus On: Identity Theft, Office for Victims of Crime

The cost of identity theft to business is generally unknown. Although some credit card companies publish information concerning their costs from lost or stolen cards and "card not present" losses, they do not report their financial losses concerning other aspects of identity theft, such as the cost of investigating cases, or the cost effectiveness of introducing new security procedures versus taking the losses. The two largest credit card companies estimated that "aggregated identity-theft-related losses from domestic operations rose from $79 million in 1996 to $114 million in 2000, an increase of about 43 percent."[1] Most credit card companies do not consider categories such as lost or stolen cards, never-received cards, counterfeit cards, mail order or telephone order fraud to be identity-theft-related.

A serious lack of data on these issues inhibits research into possible intervention strategies that could reduce the harm.

Since businesses routinely do not report losses resulting from identity-theft-related crimes to law enforcement agencies, the temptation is to think of them not as real crimes, but simply as a cost of doing business. This issue requires deeper consideration, particularly as it speaks directly to the question of the sharing of responsibility between law enforcement and business for the prevention and reduction of harm done to society by these crimes.

The Criminal Justice System

The researchers found three main costs or areas of cost for agencies—investigation, Federal prosecution, and corrections. No good source of data exists for determining the dollar figures of actual costs incurred by these areas. The only available prosecution data suggests an approximate cost of $11,400 per case, but this seems to have weak substantiation. The Bureau of Prisons reported that the cost of operating a minimum-security facility, where most white-collar offenders reside, averaged $17,400 per inmate in 2000. One may add to this the average cost of $2,900 per offender for community supervision after release from prison, but this figure does not include costs for special conditions such as electronic monitoring.[2]

Individuals

Much has been written about the human cost of identity theft victimization. Some individuals incur financial costs; these can range from $30 to many thousands of dollars. The report cites some findings in this regard, but acknowledges that the human costs for the victim in time lost, credit problems engendered by the crime, and lack of assistance are the most important and least quantifiable.

Societal

The extent of harm done by identity theft to society or to an economy that relies on open markets has yet to be determined. Identity theft is harmful to open markets because they depend on the very trust that identity theft violates. Other potential cost areas include national security risks or threats, burdens created by the presence of illegal immigrants, and higher premiums passed on to consumers.

[1] U.S. Government Accounting Office, *Identity Theft: Prevalence and Cost Appear To Be Growing* PDF, report to Senate Subcommittee on Technology, Terrorism, and Government Information, Washington DC, 2002.

[2] Ibid.

Issues That Need More Research

Overview

The study of identity theft provides a rich review of the myriad issues and dynamics involved with this crime. This information can be broken down by stages of identity theft [labeled as "T1" (time of offense), "T2" (the identity theft itself), and "T3" (outcomes)], in relationship to research focus, needs, and benefits. For example, for a research focus of outcomes (costs or losses), the research needs are identified as: the relationship between the losses or costs in relation to the period of misuse (time between T1 and T2 and the number of subsequent offenses before discovery); the time until discovery, differences between victims, and the lag time between the crime and its discovery; and the reciprocal nature of costs vis-à-vis individuals and businesses. The benefits of this research focus are identified as development of more reliable ways of estimating the cost of identity theft to individuals, organizations, and society—possibly leading to reduced harm.

Challenges Associated With Identity Theft Research

Several characteristics of identity theft data (or lack thereof) impede research:

- The number and variety of crimes that may be subsumed under identity theft has made defining identity theft difficult. Compounding this uncertainty, researchers disagree as to whether theft of credit card information (especially one-time thefts discovered that present little or no loss to victims) should be classed as true identify theft.
- Although the Federal Trade Commission has a database of identity theft complaints, no law enforcement entity maintains a national database of identity theft incidents reported to law enforcement or how those cases are resolved. In particular, little is known about how local law enforcement agencies respond to reports of identity theft.
- A lack of data about the indirect costs of identity theft or the cost-effectiveness of increased security measures inhibits research into possible strategies to reduce the harm from identity theft.
- Cross-jurisdictional issues make it difficult to isolate patterns of activity, and it is not entirely clear whether the information that is available pertains to the location of the incident or the residence of the victim.

The researchers list specific research recommendations in great detail. (See Conclusions and Recommendations.)

For more information, see Specific research recommendations. PDF

See also...
Section 6 of the full report: Explaining Identity Theft: The Role of Opportunity, pp. 38–47

Identity Theft Offending

Although the component behaviors of identity theft and its related crimes have been known for many years, identity theft is viewed primarily as a product of the information age, just as car theft is a product of the industrial age of mass production. Thus, research should emphasize uncovering the opportunity structure of identity theft. This requires two important steps:

1. Breaking identity theft down into carefully defined specific acts or sequences of behaviors.
2. Identifying the opportunities provided offenders by the new environment of the information age.

Although considerable research based on case studies has identified the criminogenic elements of the Internet as the prime leader of the information age, offenders have provided little information as to how exactly they carry out their crimes and identify opportunities for their commission.

Research is needed to interview offenders and investigators to learn the sequences of behaviors and decisions that offenders take in the course of their crimes. This approach will not only aid law enforcement in developing effective intervention techniques, it also will lead to insights as to future ways in which offenders may exploit and identify weaknesses in the information environment.

Identity thieves and those trying to thwart them are waging an "arms race." Although system interventions and improvements in technology (e.g., passwords for credit cards) can work wonders for prevention, offenders quickly develop techniques to overcome these defenses.

Identity Theft Prevention

The research focus recommended to identify the best ways to prevent identity theft crimes is based generally on the situational crime prevention literature and research. This requires the direct involvement of financial and commercial agencies and organizations in addition to, and sometimes instead of, criminal justice involvement. Local police, for example, can do little to affect the national marketing practices of credit card issuing companies that send out mass mailings of convenience checks. Here, interventions at a high policy level are needed.

The strategies and roles of government intervention in business practices—whether by criminal justice agencies or other government agencies—are highly complex and not very well known by researchers. Experience in other spheres such as traffic safety, car safety and security, and environmental pollution could be brought to bear in developing a strategy and program for government agencies and businesses to work together to reduce identity theft.

Local Level Prevention. At the local level, research is needed to examine ways to develop prevention programs in three main areas of vulnerability to identity theft. These are:

1. The practices and operating environments of document-issuing agencies (e.g. departments of motor vehicles, credit card issuing companies) that allow offenders to exploit opportunities to obtain identity documents of others.

See also...
Executive Summary of the full report: p. vii

2. The practices and operating environments of document-authenticating agencies that allow offenders to exploit opportunities to use the identities of others for financial gain, to avoid arrest, or to retain anonymity.
3. The structure and operations of the information systems that allow offenders to exploit opportunities to gain access to and use the identities of others.

Certifying Identity. Certification of an identity depends on two basic elements: confirmation of the unique biological features of that individual (DNA, thumbprint, etc.) and the ability to attach to those distinct features a history that certifies that the person is who he or she says he or she is. Though the former is relatively easy, especially with modern technologies now available, linking those biometrics to an individual's history (i.e., date and place of birth, marriage, driver's license, parent's names etc.) depends on information that accumulates through an individual's life. Thus, maintaining careful and secure records of that information both by the individual and by agencies that issue them is crucial to establishing an identity. It is essential that agencies issuing documentation have in place a systematic and well-tried system of establishing an applicant's identity (i.e., past history) before issuing an additional identification document.

The twin processes of establishing an identity (e.g., issuing a birth certificate) and authenticating an identity (e.g., accepting a credit card at point of sale) are inherently vulnerable to attack for a number of reasons:

- Old technologies that do not prevent tampering with cards and documents. These are apparent in many departments of motor vehicles across the Nation, and the credit card protections, though gradually improved over recent years, still fall far short what is technologically possible.
- Lack of a universally accepted and secure form of identification document. Although the Social Security number is universal, it is well known that it is not secure. Drivers' licenses are becoming a universal identifier by default, but their technological sophistication and the procedures for issuing them vary widely from State to State.
- Authentication procedures that depend on employees or staff to make decisions about identity. Employees with access to identity-related databases may be coerced or bribed or may otherwise divulge this information to identity thieves. Many may also lack training in authenticating documents.
- The availability of information and procedures for obtaining others' identities. These include, for example, the availability of personal information (e.g., Social Security numbers) free and for sale on the Internet, identity card making machines of the same quality as those used by agencies that issue legitimate identity cards, and hacking programs to intercept and break into databases.
- The ease with which electronic databases of personal information can be moved from one place to another on the Internet, which creates the opportunity for hackers (or those obtaining password information from

dishonest employees) to steal, hide, and sell the numbers on the black market.

Interventions. Research into situational crime prevention of various types of crime (e.g., shoplifting, theft from cars, check fraud) suggests a range of possible interventions that could be applied to counteract many of the above vulnerabilities. Research on adapting specific interventions to specific modes of identity theft should therefore provide significant indications for effective prevention.

Harm and Its Reduction

Identity theft involves, at a minimum, two victims: the individual whose identity is stolen and, in most cases, the financial institution that is duped by the use of the victim's stolen identity.

The issue of reducing harm to individual victims has received much attention. Congressional hearings and some limited studies of interviews with victims have exposed the psychological as well as financial suffering of individual victims. The focus has been on local police responses to identity theft, which were originally conditioned by their perception that banks, not individuals, were the true victims. Victims had great difficulty in obtaining police reports (as noted above, also caused by cross-jurisdictional problems) and, without such a report, had great difficulty convincing banks and credit reporting agencies that their identities had been stolen.

The International Association of Chiefs of Police and other organizations have taken steps to inform local police about the true suffering of identity theft victims and to introduce reporting and recording rules that will help victims get police reports. The extent to which this enlightened approach has filtered down to local police has yet to be determined. Researchers have extremely little knowledge of what local police departments do in response to individuals who report their victimization. (See Law Enforcement Issues and Response.)

Disposition of Cases. No systematic information is available concerning the results for victims in the prosecution and disposition of individual cases. Federal, State, and multiagency task forces have cutoff levels for acceptance of cases according to financial loss, time to discovery, and involvement of an organized group. It is estimated that the FBI and U.S. Secret Service together processed a few thousand cases of identity theft in 2004. Assuming that similar numbers of cases were processed in every State and in another 50 venues by multiagency major cities' task forces, this would yield a generous estimate of about 303,000 cases. Thus, of the estimated 9.3 million individuals victimized in 2004, an estimated 9 million cases never made it to the criminal justice system.

Of those cases that have been processed, available evidence suggests that the majority of offenders may have been treated leniently by the system—particularly before the establishment of identity theft as a separate criminal act. Some of these offenders continue to perpetrate acts of identity theft against both new and old victims; that is, they use both personal information from new individuals or the identity for the theft of which they had originally been prosecuted to continue victimization while being processed or serving their sentences.

The reciprocal element of identity theft has also not been examined. Because banks and card issuers take much of the financial loss, it is not known to what extent victims actually see themselves as victims and how this affects the steps they may take to avoid being victimized. Investigation into this problem hinges on the particular type of identity theft: whether the offender repeatedly victimizes an individual or the victimization is just a one-time event of a lost or stolen credit card that is quickly corrected. These factors may also affect how likely individuals are to report their victimization and, if so, to what agency. No research has been done on this or any related issues.

Identity Theft Legislation

In 1998, Congress passed the Identity Theft Assumption and Deterrence Act (the Identity Theft Act; U.S. Public Law 105–318). 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.

See also...

Section 8 of the full report: Legislation, pp. 63–65 and appendix 3, Summary of Federal Identity Theft-Related Statutes and State Identity Theft Laws

The National Conference of State Legislators' Identity Theft Web site for statutes, legislation, and other resources.

Most States have passed identity theft legislation. State statues differ in wording, the types of identity theft that are criminalized, and treatment of the crime as either a felony or a misdemeanor. For example, whereas some States have specific provisions criminalizing criminal record identity theft (use of an individual's identity to commit a crime or to give police a false identity), others have open-ended language that simply permits prosecution.

A detailed breakout of the laws on the books when the report was published (through January 2005) is given in appendix 3 of the full report PDF.

Conclusions and Recommendations

See also...

Section 10 of the full report: Conclusions and Recommendations, pp. 73–78

This study not only identified the available research on identity theft, it also identified in great detail the many areas where research is still needed. The issue of reporting and recording identity theft by local police departments emerged as a major issue in need of research:

> The imbalance ... of research that has focused on victims as against research on the actual criminal justice response to identity theft should be corrected.[1]

The researchers discuss the nearly inconceivable specter of having to handle 9 million identify theft cases within the criminal justice system and suggest that the best approach to the problem is prevention. More research needs to be done concerning the role that government can play to this end, through task forces and other partnerships. See Issues That Need More Research: Identity Theft Prevention.

Another key recommendation is that researchers separate out the many crimes that are lumped together as identity theft, i.e., credit card fraud, account takeover, "phishing," database theft, etc. and examine these crimes from the point of view of the three stages of identity theft (the initial offense of acquiring the personal information; the identity theft crime or crimes, i.e., fraud; and the outcomes, which are likely to be multiple).[2]

The report concludes with a table showing detailed assessment of research needs PDF broken out by focus and potential benefit from the research.

[1] Full Report, p. 74. PDF

[2] Full Report, Breaking down identity theft into its component parts, p. 75 PDF.

Study Methodology and Limitations

The study departed from the usual format of a literature review because of the paucity of formal research on identity theft. The researchers consulted other fields to bring in studies that seemed relevant. Identity theft fits into the literature of opportunity theory in criminology that examines how offenders take advantage of new (and old) ways of doing business and conducting the affairs of everyday life (Felson 1998 [1]; Felson and Clarke 1998 [2]). This literature review drew heavily on that approach and used it as an organizing principle for the paper.

The paper also differs from a typical literature review because it is in some places prescriptive, sometimes without adequate formal research to support such prescriptions. This applies particularly in regard to local police response. Much of the evidence in such matters lies in prescriptions and sometimes exhortations delivered by various associations and interest groups, sometimes emerging from various congressional hearings or from Federal or State legislation.

Sources consulted were wide-ranging and varied in type and quality. The researchers frequently consulted the Internet, acknowledging the dangers of treating Web-based information as "factual." The topic of identity theft has a major presence on the Internet (see appendix 5), which may indicate public interest. The best sources are described in appendix 1.

---

[1] Felson, M. *Crime and Everyday Life* (2d ed.), Thousand Oaks, CA: Pine Forge Press, 1998.

[2] Felson, M. and R.V. Clarke, *Opportunity Makes the Thief,* Police Research Series, Paper 98, London: Home Office, 1998.

Other Resources

NIJ does not exercise control over external Web sites. Read our Exit Notice

Bibliography

The report reviewed more than 160 literature sources, ranging from traditional journal articles through Web sites and presentations. Read the complete bibliography. PDF

Also reviewed were data sources such as the Federal Trade Commission Consumer Sentinel Network, the Internet Crime Complaint Center (a joint effort of the National White Collar Crime Center and the Federal Bureau of Investigation), and survey or study data from various research sources. Details are provided at Descriptions of Identity Theft Data Sources. PDF

Web Sites

In the Spotlight: Identity Theft. The National Criminal Justice Reference Service (NCJRS) sponsors this topical resource on identity theft, covering statistics, legislation, publications, programs, training and technical assistance, and grants and funding. See also NCJRS' extensive bibliography on Identity Theft.

Identity Theft, 2004. The Bureau of Justice Statistics recently added identity theft to its National Crime Victimization Survey. Its report based on 2004 data was released in April 2006.

Identity Theft and Fraud. The Department of Justice's main resource for consumers, sponsored by the Fraud Section of the agency's Criminal Division.

OVC Focus On…Identity Theft. Sponsored by the Office for Victims of Crime, this Web-only publication summarizes identity theft resources for victims and provides many useful links.

IACP Identity Theft Web Site. Sponsored by the International Association of Chiefs of Police and Bank of America, this website helps "consumers and law enforcement combat identity crime."

About the Researchers

Graeme R. Newman

Graeme R. Newman is Distinguished Teaching Professor at the School of Criminal Justice, State University of New York at Albany, where he has taught for 25 years. He has published in the fields of comparative criminal justice, private security, situational crime prevention, and e-commerce crime. In 1990, he helped establish the United Nations Crime and Justice Information Network, the first criminal justice presence on the Internet. Among the books he has co-authored are: *Superhighway Robbery: Crime Prevention and E-commerce Crime and Outsmarting the Terrorists* (with Ronald V. Clarke) and *Rational Choice and Situational Crime Prevention* (with Ronald V. Clarke and Shlomo Shoham). Professor Newman received his B.A. from the University of Melbourne in Australia and his doctorate from the University of Pennsylvania.

Megan M. McNally

Megan M. McNally has taught as an adjunct professor in several colleges since 1998 and worked as a research assistant for the Center for Problem-Oriented Policing as a senior editor for Criminal Justice Abstracts. She received her B.S. in Philosophy and Psychology from Fordham University in 1995, and her M.S. in Criminal Justice from New Jersey City University in 1997. In 2005, Ms. McNally presented on identity theft at the NIJ Conference in Washington, D.C.