IDENTITY THEFT LITERATURE REVIEW

Prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting to develop a research agenda to identify the most effective avenues of research that will impact on prevention, harm reduction and enforcement

January 27-28, 2005

Graeme R. Newman
School of Criminal Justice, University at Albany

Megan M. McNally
School of Criminal Justice, Rutgers University, Newark

This project was supported by Contract #2005-TO-008 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

CONTENTS

CONTENTS (Continued)

EXECUTIVE SUMMARY

This review draws on available scientific studies and a variety of other sources to assess what we know about identity theft and what might be done to further the research base of identity theft.

Until the federal Identity Theft and Assumption Deterrence Act of 1998, there was no accepted definition of identity theft. This statute defined identity theft very broadly and made it much easier for prosecutors to conduct their cases. However, it was of little help to researchers, because a closer examination of the problem revealed that identity theft was composed of a number of disparate kinds of crimes committed in widely varying venues and circumstances.

The majority of States have now passed identity theft legislation, and the generic crime of identity theft has become a major issue of concern. The publicity of many severe cases in the print and electronic media and the portrayal of the risk of identity theft in a number of effective television commercials have made identity theft a crime that is now widely recognized by the American public.

The Internet has played a major role in disseminating information about identity theft, both in terms of risks and information on how individuals may avoid victimization. It has also been identified as a major contributor to identity theft because of the environment of anonymity and the opportunities it provides offenders or would-be offenders to obtain basic components of other persons' identities.

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

Extent and Patterning of Identity Theft

The best available estimates of the extent and distribution of identity theft are provided by the FTC (Federal Trade Commission) from its victimization surveys and from its database of consumer complaints. The most recent estimate, produced by a study modeled after the FTC's original 2003 methodology, suggests that 9.3 million adults had been victimized by some form of identity theft in 2004 (BBB 2005), which may represent a leveling off from the FTC's previous finding of 9.91 million in 2003 (Synovate 2003).

While there are some differences in the amount of identity theft according to states and regions and to some extent age, the data available suggest that, depending on the type of identity theft, all persons, regardless of social or economic background are potentially

vulnerable to identity theft. This observation applies especially to those types of identity theft that occur when an offender steals a complete database of credit card information for example. However, there is some evidence that individuals are victimized by those who have easy access to their personal information, which may include family members and relatives (access to dates of birth, mother's maiden name, social security number etc.) or those with whom the victim lives in close contact: college dorms or military barracks, for example.

Types and stages of Identity Theft

Depending on the definition of identity theft, the most common type of identity theft is credit card fraud of various kinds and there is evidence that the extent of credit card fraud on the internet (and by telephone) has increased because of the opportunities provided by the Internet environment. However, some prefer not to include credit card fraud as "true" identity theft, since it may occur only once, and be discovered quickly by the credit card issuing company, often before even the individual card holder knows it. Other types of identity theft such as account takeover are more involved and take a longer time to complete.

Three stages of identity theft have been identified. A particular crime of identity theft may include one or all of these stages.

Stage 1: Acquisition of the identity through theft, computer hacking, fraud, trickery, force, re-directing or intercepting mail, or even by legal means (e.g. purchase 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 of new accounts, extensive use of 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 license, passport, visas, health cards etc.), filing tax returns for large refunds, insurance fraud, stealing rental cars, and many more.

Stage 3: Discovery. While many misuses of credit cards are discovered quickly, the "classic" identity theft involves a long period of time to discovery, typically from 6 months to as long as several years. Evidence suggests that the time it takes to discovery is related to the amount of loss incurred by the victim. At this point the criminal justice system may or may not be involved and it is here that considerable research is needed.

The recording and reporting of identity theft

According to the FTC research, there are differences in the extent to which individuals report their victimization (older persons and the less educated are likely to take longer to report the crime and are less likely to report the crime at all). It also suggests that the longer it takes to discovery, and therefore reporting of the crime to the relevant authority,

the greater the loss and suffering of the victim, and from the criminal justice perspective, the poorer the chance of successful disposal of the case.

However, in contrast to the FTC's extensive database of consumer complaints and victimization, the criminal justice system lacks any such information. There is no national database recorded by any criminal justice agency concerning the number of identity theft cases reported to it, or those disposed of by arrest and subsequently prosecution. The FBI and the US Secret Service have reported numbers of cases of identity theft in recent years, but these number in the hundreds and without state, multi-agency and local level data, there is at present no way to determine the amount of identity theft confronted by the criminal justice system.

The recording and reporting of identity theft as a crime by criminal justice authorities, especially local police has been thwarted by three significant issues:

1. The difficulty of defining identity theft because of its extensive involvement in other crimes. Most police departments lack any established mechanism to record identity theft related incidents as separate crimes. This is exacerbated by the lack of training of police officers to identify and record information concerning regular crimes that also involve identity theft.
2. The cross-jurisdictional character of identity theft which over the course of its commission may span many jurisdictions that may be geographically far apart. This has led to jurisdictional confusion as to whose responsibility it is to record the crime. Although efforts have been made by the IACP to resolve this issue, there are still significant hurdles to be over come.
3. Depending on the type of identity theft, individuals are more likely to report their victimization to other agencies instead of the police, such as their bank, credit card issuing agency etc. Thus, there is a genuine issue as to the extent to which police are the appropriate agency to deal with this type of victimization, when in fact it is the many financial agencies that are in a position to attend to the victim's problems and even to investigate the crimes (which many do). Therefore there is strong motivation for police agencies to avoid taking on the added responsibility for dealing with this crime.

Researching Identity Theft Offending

Although the different 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 was a product of the industrial age of mass production. Thus, the emphasis on research should be on 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, and
2. identifying the opportunities provided offenders by the new environment of the information age.

While considerable research based on case studies has identified the criminogenic elements of the Internet as the prime leader of the information age, there is little information gained directly from offenders as to how exactly they carry out their crimes, and how they identify opportunities for their commission. It is recommended, therefore that studies that interview offenders and their investigators to develop a scripting of the sequences of behaviors and decisions that offenders take in the course of their crimes is essential for developing effective intervention techniques. This approach also will lead to insights as to future ways in which offenders may exploit and identify weaknesses in the information environment. Something like an "arms race" is involved between offenders and those trying to thwart them. System interventions and improvements in technology can work wonders for prevention (e.g., passwords for credit cards), but in little time, offenders develop techniques to overcome these defenses.

Researching Identity Theft Prevention

The research focus recommended is based generally on the situational crime prevention literature and research. This requires the direct involvement of 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, following the lines of a successful program instituted in the U.K. by the Home Office to reduce credit card fraud in the 1990s. However, the strategies and roles of government intervention in business practices -- whether by criminal justice agencies or other government agencies – are highly complex and necessitate serious research on their own. Experience in other spheres such as traffic safety, car safety and car security and environmental pollution could be brought to bear in developing a strategy for the programmatic reduction of identity theft that involves government agencies and businesses working together.

At a local level, research is needed to examine ways to develop programs of prevention 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, as in Stage 1 of identity theft outlined above;
2. the practices and operating environments of document authenticating agencies that allow offenders to exploit opportunities to use the identities of others either for financial gain or to avoid arrest, or retain anonymity and
3. the structure and operations of the information systems which generally condition the operational procedures of the agencies in (1) and (2).

Because the certification of an identity depends on two basic criteria: the unique biological features of that individual (DNA, thumb print etc.) and attachment to those distinct features a history that certifies that the person is who s/he says s/he is. Though

the former is relatively easy, especially with modern technologies now available, the linking of it 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, the importance of maintaining careful and secure records of such information both by the individual and by agencies that issue them is essential to secure 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 document of identification.

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 USA, and the inadequacy of credit cards, though gradually improved over recent years, still fall far short what is technologically possible;
- Lack of a universally accepted and secure form of ID. While the social security number is universal, is well known that it is not secure. Drivers' licenses are becoming a universal ID by default, but their technological sophistication and 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 otherwise divulge this information to identity thieves. Many may also lack training in documentation authentication.
- The availability of information and procedures for obtaining the identities of others. These include, for example the availability of personal information on the Internet free and for sale (e.g. social security numbers), identity card making machines of the same quality of 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, creates the opportunity for hackers (or those obtaining password information from dishonest employees) to steal, hide and sell the numbers on the black market..

The research literature from situational crime prevention on 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 in regard to specific modes of identity theft should therefore provide significant indications for effective prevention.

Researching 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 in recent years. 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 individuals were not the true victims, but that the banks were. Victims had great difficulty in obtaining police reports (as noted above, also caused by cross-jurisdictional problems) and so, without such a report, had great difficulty convincing banks and credit reporting agencies that their identities had been stolen. Steps have been taken by the IACP and other organizations to inform local police about the true suffering of identity theft victims and to introduce reporting and recording rules that will help victims get their police reports. The extent to which this enlightened approach has filtered down to the local police level is yet to be determined and itself is in need of research. In fact, we have extremely little knowledge of what local police departments actually do in response to individuals who report their victimization,

There is no systematic information concerning how individual victims fare in the prosecution and disposition of their cases, though we do know that federal, state and multi-agency task forces have cut-off levels for acceptance of cases according to financial loss, time to discovery, and whether there is an organized group involved. We guess that the FBI and US Secret Service between them processed a few thousand cases of identity theft last year. If we guess that there have been similar numbers of cases processed in every state and add in another 50 venues to cover multi-agency task forces and major cities task forces, this would give us on the very high side an estimate of about 303,000 cases. This means that, of the estimated 9.3 million individuals victimized in 2004, some 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 such offenders may have been treated leniently by the system – particularly before the establishment of “identity theft” as a separate criminal act. A further minority of these offenders continues to perpetrate acts of identity theft against “new” and “old” victims - that is, they use both new personal information and/or the identity for 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. Since banks and card issuers take much of the financial loss, to what extent do victims actually see themselves as victims, and will this affect the steps they may take to avoid being victimized? Obviously, the investigation into this question hinges on the particular type of identity theft: whether the individual is repeatedly victimized by an offender, or whether the victimization is just a one-time event of a lost or stolen credit card that is quickly corrected. These factors may also affect the propensity of individuals to report their victimization and to what agency. There is no research on this or any related issues.

The cost of identity theft to business, is generally unknown. Although credit card companies do publish information concerning the cost to them of “lost or stolen” and

"card not present" losses, they do not report their losses concerning other aspects of identity theft, such as the cost of investigating cases, or the cost effectiveness of introducing new security procedures as against taking the losses. There is a serious lack of data on these issues that inhibits research into possible intervention strategies that could reduce the harm.

Finally, in a broader sense, the extent of harm done by identity theft to society or to the economy that relies on open markets is yet to be determined. Identity theft is harmful to open markets, because they depend on the very trust that is so obviously violated by identity theft. Since businesses routinely do not report losses resulting from identity theft related crimes to law enforcement agencies, there is the temptation to think of such crimes as not real crimes, but simply 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 this crime.

1. INTRODUCTION

This paper departs from the usual format of a literature review because there is very little formal research on identity theft *per se*. Thus we have reached out to other fields to import into this review research and other studies that seem immediately relevant to our topic. Identity theft is a product of the new age of information technology and as such fits nicely into the literature of opportunity theory in criminology which examines how offenders take advantage of new (and old) ways of doing business and conducting the affairs of everyday life (Felson 1998; Felson and Clarke 1998). We have therefore drawn 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 and on occasion emerging from federal or state legislation.

The sources of information are also rather wide-ranging and vary in type and quality, as we note below. We have made considerable use of the Internet, but are cognizant of the dangers of treating some of that information as "factual." Identity theft as a topic has a major presence on the Internet (see Appendix 5) which is perhaps an indicator of public interest, concern and entrepreneurial spirit. The better of these sources are described in Appendix 1.

2. DEFINITION OF IDENTITY THEFT

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.

The terms "identity theft" and "identity fraud" have come to be used interchangeably in popular usage, even though the two are different from a legal point of view.[1] Some consider identity theft to be a subcategory of identity fraud.

[1] Generally legal codes distinguish between theft and fraud by identifying the latter as taking from the victim by trickery or deception, such as when one borrows from the victim without intention of paying back the money. Simple theft in contrast refers to direct taking from the victim without authorization. It can be seen that the Federal law encompasses both these types of taking.

Throughout this paper we will abide by the popular usage.

Identity theft is rarely one crime, but is composed of the commission of a wide variety of other crimes, many if not all of which are crimes well known to us all. The crimes with which identity theft is commonly associated are: check and card fraud, financial crimes of various sorts, various telemarketing and Internet scams (Newman and Clarke 2003), theft of autos and auto parts aided by fraudulent documentation (Maxfield and Clarke 2004), thefts or robberies of various kinds where identification information is stolen either by coincidence or intentionally, counterfeiting and forgery, trafficking in human beings (UNICRI 2003) and terrorism.

It is clear that these identity theft related crimes are not new crimes at all, but rather are old crimes enhanced by the use of, or theft of, stolen identities. However, it is our assessment that the federal law derives not so much from those old crimes, but from the wide publicity in the late 1990s of victims of identity theft. These were victims who were repeatedly victimized over a period of time from months to sometimes years and who were unable to get back their identities or were unable to convince credit issuing and reporting authorities of their loss. The publicity gave rise to a series of Congressional hearings, which eventually resulted in the Identity Theft Act of 1998.

Three significant facts resulted from these hearings. First, local law enforcement had been slow in recognizing individuals as victims because most of the actual financial loss, such as from credit card fraud, was born by the card issuer not by the cardholder. Businesses were perceived as the victims, not the individuals. Second, testimony of individuals in the hearings revealed that their identities were used over an extended period of time until their utility was depleted. They were in effect objects of repeated victimization. Third, it was not uncommon for individuals to discover their victimization some time after the event thus making it more difficult to investigate the crime.[2]

The difficulty, therefore, in designing any research on identity theft is to investigate what portion of the long list of identity theft related crimes recounted above is related to the "classic" type of identity theft that results in repeat victimization. For example, a common type of credit card fraud is to steal an individual's credit card, such as from a handbag or coat draped over the back of a chair in a restaurant. The offender makes a quick purchase of an expensive item then discards the card. This series of events may take less than thirty minutes, probably less time than it will take the victim to discover the loss and notify the card issuer. Has the victim's identity truly been stolen? The event clearly fits within the legal definition above, but it is not the wholesale theft of the

[2] *Research note*. The question of how long it takes victims to discover their victimization and how long it takes to successfully investigate a case in relation to how much time elapses after the event has not been thoroughly researched. Although some data have been collected based on interviews with victims, these have been with small samples. Thus, much of the evidence supporting this claim is anecdotal and descriptive (U.S.GAO 1998a; CALPIRG 2000). See also Section 5 for FTC research.

victim's identity. However, should the offender be working with an accomplice, the card could be turned over several times; or should the victim either not discover the loss of the card, or not bother to contact the card issuer (since card issuers take the loss), then the card could be turned over several times and even sold on the street for a small sum. Finally, should the victim's drivers' license and other identifying documents such as a health card with a social security number on it also be in the pocket book, the basic elements for stealing an individual's identity are present.

Thus, there is a need for research that can tease out the different elements of identity theft as they relate to the many different common crimes, indeed, the specific situations in which particular aspects of these crimes are played out. At a minimum we need to know the extent to which common crimes use stolen identities or partial identities, the reasons why they are part of other crimes and whether this is increasing. As a first step in this direction, we suggest a rough typology of identity theft based on the known role of identity theft in relation to other crimes.[3]

3. TYPES OF IDENTITY THEFT

The typology offered below is a rough approximation, based on subjective impressions of cases gleaned from Internet research. It is more a way of conceptualizing the multifaceted problem. Certainly there is much overlap among the different types identified. A single case typically includes more than one of the categories below. The types are based essentially on a mixture of methods and motives used by the offender, and as such must be considered as rather primitive.[4] Research is needed on the sequence of events or steps taken by offenders from the beginning to the completion of their identity related crime. The difficulty the researcher faces in developing a typology is that identity theft is composed, not only of many different crimes, but also of many different situations and event sequences. There is a pressing need, therefore, to break down the crime "identity theft" into smaller, specific components. This has been done in part by Lacoste and Tremblay (2003) in their study of check fraud, in which they use a "script" approach to analyze the steps and choices made by check fraudsters in carrying out their crimes.

[3] *Research note*. The complicated definition or nature of identity theft has significant practical implications. Police crime incident reporting procedures have great difficulty in recording identity theft because their standard forms often do not contain any such category, and if they do, no criteria to assist in how or whether to classify a particular incident as an ID theft, as well as, say, a burglary. In regard to some crimes such as burglary, it may not be an established procedure to collect information as to whether a victim's personal information was stolen (the person may not even think of looking to see if it was) in contrast to other typical targets of burglary such as jewelry. The practical result is that the crime analyst (or a researcher) may not know whether there is a problem of identity theft unless (a) the basic information of theft of identification materials is collected and recorded for all crimes regardless of type and (b) a method is developed of analyzing the details of all crime incidents recorded to identify patterns of ID theft related information across crime types.

[4] Another attempt at a typology has been suggested by Newman (2004) which conceives of identity theft as composed of four interacting dimensions: concealment, financial gain, commitment and organization. See also further below the typology by Gayer (2004:13) and notes 48 and 49.

1. Exploiting Weakness in Specific Technologies and Information Systems. (Cases 1-2) Credit card fraud is perhaps the best example of the type of identity theft that targets a specific technology which is the plastic card and its various attributes (magnetic strip, hologram etc). Here, the fraudster, using a variety of techniques, tampers or alters credit cards that are either stolen from victims or are counterfeit but have applied to them all the identity information from a victim's financial records. As noted above, the casual or even organized theft of a credit card may not develop into "full blown" identity theft if it is used and disposed of in a short period of time. The amount of harm done to the cardholder may be minimal, beyond the nuisance of having to obtain a new credit card and stop the old one. The exploitation of the credit card is, however, a major means for thieves to convert what they steal into cash or expensive items that they purchase. Check and card fraud provide the entry into information systems that will dispose of goods and services without the serious possibility of the offender getting caught.

Other common targets of this type of identity theft are electronic databases that contain personal and financial data on customers (Cases 1-2). Some of this information has been used by offenders to access bank accounts, obtain credit cards, open telephone or utility accounts, and thus convert the information they have stolen into cash. The use of individual identities from such stolen databases (which may contain records numbering in the many thousands) is anecdotal. There is no research on the extent to which such data bases lead to abuse of individual identities. The most publicized cases of theft of databases have been those in which offenders have tried to extort money from the businesses or agencies that own the data bases. The latter may not technically be termed "identity theft" unless one defines a person's identity as being constituted by the financial or personal records contained by a credit card issuing company. The problem here is what, in fact, constitutes an "identity," (See our discussion on identity and its authentication in Section 6.)

2. Financial Scams. (Case 3-4) There is a wide variety of scams that may be committed with the goal of obtaining from victims their personal information. These types of identity theft are obviously also related to the exploiting of specific technologies and information systems. They occur in telemarketing frauds, such as requesting personal details while pretending to be doing a security check or collecting for a charity. Fraudsters place false "store fronts" on the web that imitate well known web retailers, or send tricky email or pop-up solicitations ("phishing") requesting financial and personal information in the name of well known retailers and often government departments such as the IRS. The majority of these types of fraud use relatively tried and true old scams adapted to new technologies. They all essentially depend on tricking or duping the victim.

3. As a motive for other crimes. (Cases 5-6). Offenders now recognize the monetary value of the personal information of individuals. Thus, there is some evidence that offenders may commit traditional theft related crimes with the main motive of obtaining the personal information of their victims (Home Office 2004; "The decline of the English burglary," 2004). Burglary, robbery, muggings, theft from cars, pick pocketing may all be

committed with the view to obtaining the victim's personal and financial information. Extortion and bribery may also be committed in order to access financial and personal databases or records of businesses and other agencies, such as threatening or bribing employees to provide passwords or leave doors and cabinets unlocked.

4. Facilitating Other Crimes. (Cases 7-8). Document theft or fraud are the most common identity related crimes that facilitate the commission of other crimes. A seasoned identity thief will obtain a couple of major pieces of an individual's identity: e.g., a birth date and a social security number, and use these to "breed" additional documents. The careful use of this information either over the telephone, the Internet, face to face with a bank official, or even filling in an application for credit, may assist in obtaining more information, such as bank account numbers, driver's license or visas and passports. The information may be used to forge new documents such as counterfeit credit cards which may have account numbers and names of legitimate account holders, thus making them harder to identify. New bank accounts may be opened, new credit cards obtained. An entire way of doing business and conducting necessary transactions to carry out further crime of a different sort may then be accomplished.

As noted In Section 6, the *sine qua non* of committing a crime is to carry it off without being discovered. To commit a crime under the identity of someone else therefore is an attractive proposition. It reduces the risk both in the commission of the crime and in getting caught after the crime. Breeding the necessary enabling documents to conduct business transactions reduces risks in committing a crime. For example, renting a car with a stolen identity saves having to steal one, thus reduces risk.

5. Avoiding Arrest. (Case 9). Should an offender be caught, using another's identity can avoid arrest or detention, especially if the offender already has a criminal record or if there is an arrest warrant outstanding. Committing offences in another person's name means that the police will be looking for that person, not the true offender.

6. Repeat Victimization: "Classic" Identity Theft. (Case10). As noted earlier, this type of identity theft has been the most widely publicized. It focuses more on what happens to the victim, but directly implies a consistent and repeated attempt by the offender to use the individual's identity over and over again until the identity's usefulness in generating money and opportunities for additional crimes is exhausted. While there is considerable testimony from victims that this process does occur and over a considerable period of time, there is little research collected to describe this process from the offender point of view, though there is some to suggest that experienced offenders who specialize in check and card fraud know how long to turn over a card, and when to dispose of it on the street (Mativat and Tremblay 1997).

7. Organized Identity Theft. (Cases 11-12). All the above types of identity theft may be committed either by individuals or in groups. Offenders who are committed to their enterprise usually work in groups because the sustained accomplishment of their frauds requires more than one individual to successfully perpetrate them. The limited research available on organized criminal activity to commit identity theft comes mainly from the

studies of credit card fraud (Mativat and Tremblay 1997; Newton 1994; Bury 1999:7; Steel 1995:16). In order to perpetrate credit card fraud on a large scale, considerable expertise, experience and know-how is required, along with an organization to make marketing of counterfeit credit cards possible. At a minimum, such a gang must accomplish at least the following:

- search for an easy target,
- locate sources of personal information for that target,
- obtain the necessary documents (legal or counterfeit) to establish legitimacy,
- choose how to use the identity to obtain money,
- convince officials that one is the person named in identity documents,
- anticipate how long one can exploit the identity before the victim discovers the losses,
- find easy ways to convert stolen identities into cash.

Some exploratory 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 (Newton 1994). At the street level credit card 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 (Mativat and Tremblay 1997).[5]

In the outline of types of identity theft above, some reference has been made to "experienced" or "seasoned" offenders who use identity theft either as their main motive or to facilitate other crimes. However, to our knowledge there is little research data (though many cases recounted on the Internet) that affirm whether or not such types of identity thieves exist, or if they do, what proportion of ID theft crimes they account for.

[5] *Research note*. The extent of international criminal activity in relation to identity theft is unknown. Because of globalization and the increasing use of credit and debit cards internationally, the expectation is that the weaknesses in international systems of card authentication and delivery would be exploited. It is known that the rate of credit card fraud in France has been much lower than that of the U.K. or USA in past decades (Newman and Clarke 2003). The reason usually given for this difference is the superior authentication technologies used in France (PIN required for credit card use for cards issued in France). A comparison of the authentication procedures, different technologies, and different marketing policies of card issuing companies in different countries would be particularly informative, especially as many of the same card issuing companies issue cards in multiple countries (Levi and Handley 1998a; Levi and Handley 1998b).

4. EXTENT AND PATTERNING OF IDENTITY THEFT

Sources of Data[6] and Measurement Issues

Agency Data

Although the phenomenon has existed for centuries, considering the relatively recent emergence of the actual term "identity theft" it is not altogether surprising that one of the earliest and most significant investigations of the topic discovered that there were no comprehensive or centralized national data, collected by any public[7] or private organization, on the problem of identity theft (U.S. General Accounting Office (GAO) 1998 2002a,b,c,d).[8] In the absence of explicit data, the GAO primarily relied on a number of proxies or indicators, obtained from various public and private sources, to estimate its occurrence. However, such data are often limited, and many government agencies do not have information systems that can facilitate tracking or assist in quantifying the number of existing identity theft cases (GAO 2002a,c). Thus, much of the data were specifically gathered or estimated at the request of the GAO, and their sources are not necessarily inclusive of all agencies that may be affected by the problem of identity theft. Further, the data obtained were not independently verified by the GAO, and must be taken at face value. Nevertheless, when reviewing any type of agency data, public or private, there are a number of additional caveats that must be considered:

1. Routinely collected statistics from either sector on identity theft-facilitated crimes (such as terrorism or alien smuggling) or identity theft-related crimes (such as theft or fraud), generally do not isolate the specific identity theft elements of such crimes. For example, "the Federal Reserve Board reported that…fraud involving [the] use of sensitive identifying information is often not tracked separately from other types of fraud" (GAO 1998:48-49), and not all incidents of fraud involve identity theft. Thus, the extent of identity theft can be obscured when it is not treated as a discrete crime (Gordon et al. 2004), or exaggerated if it is treated as synonymous with crimes such as fraud.

2. When it is recognized as a specific act, there is no consistent definition or use of the term "identity theft" across agencies or organizations, and few attempts are made to separate the problem of identity theft from the problem of identity fraud.

---

[6] For a description of existing data sources on identity theft see Appendix 1.

[7] Relevant government agencies have not, historically, recorded statistics related to this crime. Law enforcement agencies, for example, have generally treated identity theft as an aspect of other crimes (GAO 1998) and identity theft is not specifically recorded as an offense category within the Uniform Crime Reporting Program (GAO 2002a).

[8] *Research note*. Specifically, this series of GAO reports identified statistical deficiencies in the areas of: the prevalence of identity theft; the universe of identity theft victims; military-related identity theft cases; investigations, convictions, offenses charged, or other outcomes under the Identity Theft Act or existing state identity theft statutes; the associated or estimated costs of identity theft to either federal or state governments, the financial services industry or individuals; the use of the Internet or other advanced technologies for identity theft-related crimes; and the impact of Internet growth on opportunities for identity theft-related activity (GAO 2002a,c,d.; 1998).

This lack of a consistent definition has hindered the collection of relevant data in many sectors. Many public and private agencies also often use different indicators of the problem. Thus, when data are available, they may not be comparable.

3. Such data are also affected by a number of agency-related variables, such as policy, staffing, resources, awareness of the problem, and responses to the problem. For instance, an apparent decrease of identity theft-related cases closed by the Secret Service between 1998 and 2000 was due to the agency's decision to focus its efforts on higher-dollar-value cases of identity theft. This decrease was offset by an increase in the average amount of prevented fraud losses for this period (GAO 2002d). Similarly, one consumer reporting agency attributes increases in consumer inquiries not only to increasing occurrences of identity fraud, but to company growth and consumer outreach efforts; one payment card association attributes a decline in fraud losses between 1996 and 1997 to its antifraud efforts (GAO 1998).

4. Data that are routinely collected by agencies largely represent reported crimes, complaints, or requests for information, which are all subjective indicators of its occurrence. Increases in any one of these indicators may be due more to increased public awareness of the crime, or improved data collection efforts, rather than actual increased incidence. This is a very real possibility that cannot be underestimated in the dawn of the information age. However, the fact that people are simply now realizing their victimization does not belie its extent, only the consistent observation that its incidence is "growing."

5. Finally, there is reason to believe that identity theft is underreported, both by individuals and by agencies. Given the nature of this crime, the potential exists that a number of victims may never know that they have been victimized since their "new life" may be both statistically and geographically disjointed from their real one. This is particularly applicable for the most serious type of identity theft, sometimes called "true name fraud," which principally involves the use of personal information to open new accounts. Even if individuals ultimately become aware of their victimization, identity theft may remain undetected for considerable periods of time:

    - Victims who had new accounts opened in their name reported that the misuse took place over a longer period of time than victims experiencing other types of fraud; more than a quarter of these victimizations lasted six months or more (Synovate 2003).
    - Discovery of misuse was shortest, usually within one month, for victims who experienced the misuse of an existing credit card or non-credit card account, as many noticed unauthorized activity on their monthly statements (Synovate 2003).
    - The FTC (2001b) and Benner, Mierzwinski and Givens (2000) reported that the average amount of time to the discovery of misuse was 14

> months.[9] One study found that 24% of its surveyed victims did not find out about the crime for more than two years after the original misuse of their information (Foley 2003b). Some victims had been unaware of the misuse for as long as five years (FTC 2001b), and in at least one case 10 years (Benner et al. 2000).[10]

The issue of discovery also affects known estimates of identity theft, reporting behaviors, and data collection efforts, since the crime may have been perpetrated more than six months prior to being discovered. Discovery may also be related to a number of additional variables such as the method of theft, the total losses associated with the theft,[11] and particular victim sociodemographic characteristics. For example, those who discovered their victimization after six months were more likely to be non-white, have lower or middle household incomes, and have lower educational attainment (Synovate 2003).[12]

Nevertheless, even when the misuse is known, the best available estimate suggests that 38% of victims do not report the crime to anyone (Synovate 2003). Those who do report may not have their complaint recorded in official statistics, particularly if they report to the police[13] (FTC 2005; FTC 2004; FTC 2003b; Synovate 2003; Foley 2003b; Benner et al. 2000). However, many known estimates of victim reporting, such as those shown in Figure 1, are based on victim complaints, which are biased indicators of reporting behavior.[14]

---

[9] It is interesting that both agencies report the exact same estimate for, roughly, the year 2000. Similarly, an independent Grand Jury investigation in Florida found that the average time between the occurrence of the crime and discovery was 12.7 months (Florida 2002). FTC (2002b) data for 2001 reported the average time until discovery to be 12.3 months. Such similarities in reported averages across years should be investigated further.

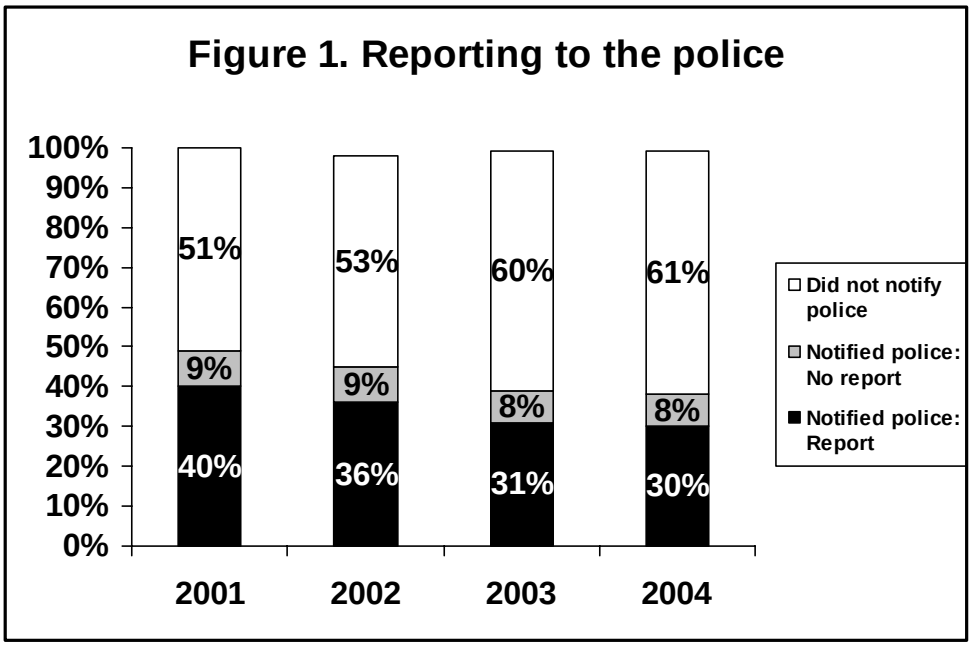
[10] An independent Grand Jury investigation in Florida similarly found that almost 10% of cases took more than 5 years to be discovered (Florida 2002).

[11] It is known that higher dollar values of loss are associated with longer periods of misuse. Conversely, these higher dollar values may be associated with the actual discovery of the crime. Some victims initially find out about the crime after being contacted by some type of collection agency demanding payment for a large outstanding balance generated by the thief, but this connection is currently uninvestigated.

[12] *Research note*. Such trends are currently unexplained, and only reported by the FTC study. Further research is necessary regarding all time-related aspects of this crime since it affects both the amount of losses incurred and the effectiveness of investigative efforts.

[13] The FTC study notes that, "[p]olice were more likely to take a report if the misuse was discovered more quickly. A report was taken in 83% of cases where the misuse was discovered within 5 months of the initial misuse of the victim's information. Where it took 6 months or more to discover the misuse, reports were only taken in 47% of cases" (Synovate 2003:60).

[14] In the FTC study, only 26% of victims reported notifying the police, and this was more likely when they were the victim of a new account or other type of fraud. A number of victims had notified other agencies, mainly credit card companies and credit bureaus (Synovate 2003). Although not directly comparable, rates of reporting to the police for property crimes in 2003, as estimated by the NCVS, are seemingly higher: 31.8% of theft victims and 43.9% of personal theft victims reported to the police; the total number of victims reporting for all property crime (including theft) was 38.4% (Catalano 2004). The FTC study (Synovate 2003) also notes that non-white victims were more likely than whites to contact the police (34% vs. 23%, respectively), but this pattern requires further investigation and comparison to known reporting behavior.



Sources: FTC, 2005, 2004, 2003b, 2002a.
Note: This figure, based on the number of individuals who reported this information (67,121 in 2001; 131,746 in 2002; 199,995 in 2003; and 239,945 in 2004), represents approximately 95% of the victims who directly contacted the FTC during each of these years. Some victims also reported that they had contacted the police, but did not indicate whether a report had been taken (2% in 2002; 1% in 2003; and 1% in 2004). Due to lack of information, data for 2000 were not included, but the FTC (2001a) indicates that 54% of the victims who provided this information did not contact the police. Nevertheless, these figures do not represent actual reporting behaviors, but the behaviors of victims who were willing to contact at least one other agency (i.e., the FTC).

Overall, it is difficult to separate the wheat from the chaff when it comes to estimating the characteristics of identity theft from existing agency data, but this does not imply that the information is unhelpful. In light of the newfound acknowledgement of identity theft as a specific crime, agencies are likely to restructure the ways in which they record information to include identity theft. Further, with regard to certain sources of agency data (e.g., Secret Service, credit card bureaus), much of it is not publicly available, and the GAO reports are the only source. It is probable that the GAO will continue their efforts to examine the phenomenon through similar reports.

Currently, the most comprehensive database is the FTC's Identity Theft Data Clearinghouse, which was established in 1999 as part of the Consumer Sentinel Network. Consumer Sentinel is a database, developed and maintained by the FTC, which collects consumer fraud and identity theft complaints from over 100 different organizations in order to assist law enforcement investigations. In addition to the Clearinghouse, the Sentinel Network is comprised of econsumer.gov, a joint effort of 13 countries created in 2001 to gather and share cross-border e-commerce complaints; and the Military Sentinel, which was established in 2002 to identify and target consumer protection issues, including identity theft, that affect members of the U.S. Armed Forces and their families (FTC 2004).

The Clearinghouse, as part of the FTC's requirement under the Identity Theft Act, is a central repository of all identity theft complaints and requests for information received through the Sentinel Network. The majority of these complaints are received from the FTC's phone hotline and web-based complaint center, although other organizations do contribute information related to identity theft.[15] The FTC's database, therefore, is subject to the caveats discussed above.

Further, although extensive, the database is not inclusive of all potentially relevant agency data on identity theft. For example, the FTC study found that 7% of victims contacted the Division of Motor Vehicles to report the misuse of their driver's license (Synovate 2004), but DMV complaint data is currently not reported in any source, and in fact may not be recorded at all.[16] A final caution in the interpretation of Clearinghouse data is that the number of complaints reported for a given year will tend to increase in subsequent years due to the continual transmission of new data, which may contain complaints from previous months (FTC 2004). Thus, for example, the number of complaints in 2002, as most recently reported, was 161,896 (FTC 2005). This number was originally reported as 161,819 (FTC 2003b).

Research Studies

Aside from the Clearinghouse and additional agency data provided by the GAO,[17] there are only a handful of studies that focus exclusively on identity theft, but they vary widely in quality and scope.[18] The best available source to date is the FTC's study conducted by Synovate in 2003[19], although private companies have conducted similar studies in the past few years (Gartner Inc. 2003; Harris Interactive 2003; Star Systems 2002). One anticipated source is the NCVS (National Crime Victim Survey), which is currently piloting a series of identity theft questions to be included in the 2005 survey (Hughes

[15] A full list of Sentinel data contributors can be found in the FTC's most recent report (2004): http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf. There is at least one other major online complaint center, the Internet Crime Complaint Center (formerly known as the Internet Fraud Complaint Center), which transmits fraud information to the Sentinel Network. However, the IFCC records specific information on identity theft that is apparently not deposited in the Clearinghouse. Further, there are additional reported categories, not counted as "identity theft" by the IFCC, which have been treated as categories of identity theft by other sources, including the FTC: e.g., credit/debit card fraud, check fraud, and communications fraud, which includes the theft of wireless and landline services (NWC3/FBI 2003; 2002).

[16] In one study, 39% of victims reported that a new driver's license was issued to the thief, and 50% reported that the thief had used personal information to create a fake license (Foley 2003b). The extent of such misuse, or for that matter the misuse of social security numbers or birth certificates in identity theft incidents, is currently unknown and requires further investigation.

[17] The Clearinghouse was one of the agency data sources used to inform the GAO reports. Other data, such as SSA/OIG complaints, began being transmitted to the FTC database in February 2001, but were also separately reported by the GAO.

[18] See Appendix 1 for a description of these studies.

[19] A new study, jointly released by the Better Business Bureau (BBB) and Javelin Strategy & Research (2005), uses an almost identical methodology to update the FTC's 2003 findings. See Appendix 1 for more information.

2004). Additional impact research with known victims has also been conducted (Foley 2003b; Benner et al. 2000[20]); and at least one university-based organization, the Identity Theft University-Business Partnership at Michigan State University, has several identity theft projects in progress. Finally, there is one known study of law enforcement perspectives on the problem of identity theft (Gayer 2003).

These studies, however, reflect only those that have focused directly on identity theft and do not include the universe of related studies on credit card/check fraud, Internet crime/cybercrime/e-commerce crime, or similarly related areas of research. Whereas additional insights may be gleaned from such research, the task of isolating identity theft related variables, as it relates to estimating the extent or characteristics of identity theft, may be difficult as they are affected by the caveats discussed above.

These research studies come with their own methodological issues:

1. Non-response bias. Victim surveys, for example, are useful for estimating the "dark figure" of identity theft; however, they are prone to non-response bias and are dependent upon victims' memory, awareness and comprehension of the crime, and comprehension of the survey questions themselves (GAO 2002c; Gordon et al. 2004; Hughes 2004). The issue of discovery also affects the ability to perform meaningful and accurate research on identity theft, particularly if short reference periods are used to screen participants.[21] The issue of non-response bias is particularly important in relation to the problem of identity theft. Many existing studies do not report their response rates, and even the results of those that do may need to be treated with caution - particularly those with rates lower than 50% (GAO 2002c:17). Known victims of identity theft may also be difficult to contact and thus fail to respond to survey attempts. Aside from some of the traditional reasons for non-response, such as victims' reluctance to discuss the incident, this issue may be further complicated by the fact that many victims of identity theft will change or must change their contact information (telephone numbers, e-mail address, etc.) as a result of the victimization itself (Foley 2003b). It may also be the case that attempts to randomly select victims may fail if individuals obtain unlisted phone numbers, or otherwise protect their contact information.

2. Sampling. Existing surveys vary with regards to their methodologies, sample sizes and population estimates. Online surveys, for example, exclude the universe of victims that do not have Internet access. Two independent surveys, each conducted in 2002 by Harris Interactive and Star Systems, respectively, use seemingly differing population estimates

[20] The GAO also conducted interviews with 10 identity theft victims - see GAO (2002c) Appendix IV.

[21] During cognitive interviews to test questions for the NCVS, 4 out of the 10 respondents experienced incidents of identity theft that occurred outside of the 6-month reference period (Hughes 2004). If similar rates are encountered in other studies, subsequent results may not reflect the experiences of all identity theft victims, particularly the victims of true name fraud, since it generally takes this group the longest to discover the misuse of their personal information.

(although the sources for these estimates are not reported) and come up with disparate estimates regarding the prevalence of identity theft.[22]

3. Individuals vs. households. Existing surveys also vary on whether they use individual or household measures of victimization, and the reference period used for reporting victimization (e.g., several asked whether the respondent or member of their household had "ever been victimized").

Anecdotal Information

Finally, additional information on identity theft can been obtained through case studies or victim testimonies, a number of which can be located within congressional hearings on the topic. Aside from being anecdotal, however, such information is often representative of the most extreme cases of identity theft. Therefore, although these sources can be informative, they do not provide a completely accurate picture.

Overall, the collection of data from so many decentralized and distinct sources is, in some ways, piecemeal, and, in other ways, duplicative (Gordon et al. 2004:9). Although this situation can be expected to improve, much more work needs to be done, particularly on the development of a centralized reporting system for identity theft. Such a system must not only accurately reflect all reported cases of identity theft/fraud across various agencies and jurisdictions (both domestic and international), it must be able to share this information with all relevant parties (Gordon et al. 2004). The FTC's Clearinghouse is undoubtedly a first step in this endeavor, which may conceivably evolve to meet this goal. Additional studies must also be conducted to more fully understand various aspects of the identity theft problem, as discussed throughout this report. Nevertheless, any data collection efforts will by frustrated by the lack of an organized definition and understanding of the concept of identity theft – a concern that should receive top billing in both research and theoretical communities.

The Extent of Identity Theft

There are no comprehensive statistics on the prevalence of identity theft since "some individuals do not even know that they have been victimized until months after the fact, and some known victims may choose not to report to the police, credit bureaus, or established hotlines" (GAO 2002c:2). Many existing estimates must also be approached with care. In addition to the cautions previously discussed:

> Some of the often-quoted estimates of prevalence range from one- quarter to three-quarters of a million victims annually. Usually, these estimates are based on limited hotline reporting or other available data, in combination with various assumptions regarding, for example, the number of victims who do not contact credit bureaus, the FTC, the SSA/OIG, or other authorities. Generally speaking,

[22] Having predated the 2003 FTC study, these surveys are often reported in public sources of information on identity theft, but information regarding their methodologies is limited. See Appendix 1 for a description of these studies.

> the higher the estimate of identity theft prevalence, the greater the (1) number of victims who are assumed not to report the crime and (2) number of hotline callers who are assumed to be victims rather than "preventative" callers. We found no information to gauge the extent to which these assumptions are valid. Additionally, there are no readily available statistics on the number of victims who may have contacted their banks or credit card issuers only and not the credit bureaus or other hotlines. (GAO 2002c:20)

While there is now reason to believe that identity theft exceedingly affects more than three-quarters of a million victims annually, the source of any readily proffered estimates of prevalence or incidence must, nonetheless, be carefully scrutinized.

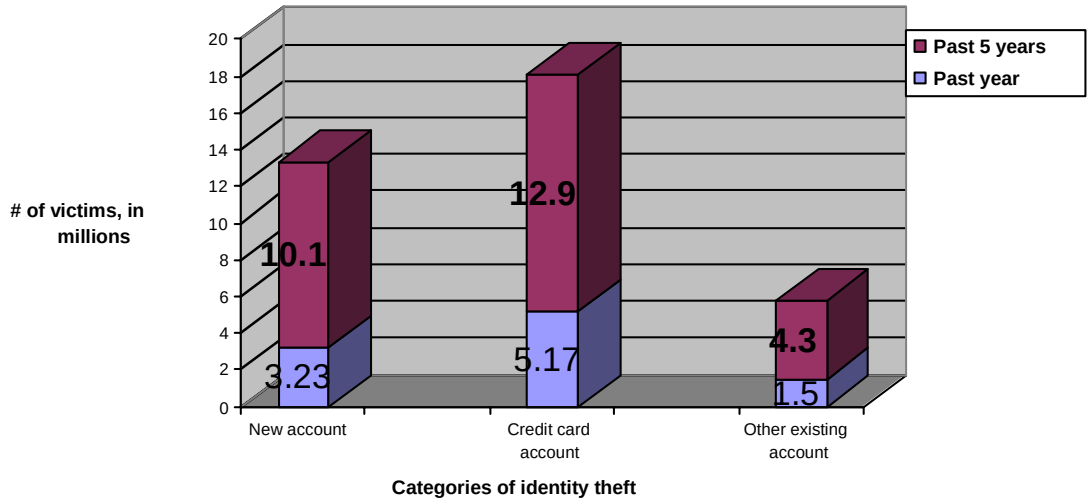
One additional stipulation should be noted, which is related to the problem of underreporting mentioned above. Some anecdotal evidence suggests that identity thieves target both children (Foley and Nelson 2003) and the deceased (Foley 2003a) to some degree. Neither group, however, is properly represented in existing estimates, which are all based on the U.S. adult population over the age of 18; nor are there evident plans to include these groups in future research attempts.

The best known estimate suggests that approximately 9.91 million adults discovered, during the past year, that they were the victims of some form of ID theft, including new accounts and other frauds, misuse of existing non-credit card accounts, and misuse of existing credit card accounts.[23] Over the past five years, approximately 27.3 million adults discovered that they were the victims of some form of ID theft (Synovate 2003). These recent figures, as illustrated in Figure 2, greatly surpass the earliest estimates of this crime, which were expected to affect between 500,000 and 700,000 individuals per year (Givens 2000a).[24] However, the FTC study was the first randomized victimization survey to estimate the number of individuals who had not reported their victimization.

[23] This figure is comparable to that found by subsequent research conducted by Javelin Strategy & Research in 2004 (Sullivan 2005); although the findings suggest, based on recalculated data from Synovate (2003), that the number of "identity fraud" victims dropped from 10.1 million in 2003 to 9.3 million in 2004 (BBB 2005). In particular, this research concluded that the rate of identity theft has leveled off, despite increasing complaints received by the FTC (2005). This apparent inconsistency may be explained by increased reporting to the FTC, but the stability of identity theft victimization patterns must be verified through additional research.

[24] Independent studies, which used similar definitions of identity theft, have also reported rates that fail to match these most recent estimates. A series of studies, conducted on behalf of Privacy and American Business, estimated that between 33.4 and 42 million American adults had been victimized by consumer identity fraud or theft in their lifetime (Harris Interactive 2003). Similar studies conducted by Star Systems (2002) and Gartner Inc. (2003) found, respectively, that 11.8 million people had been victimized by identity theft in their lifetime, and that 7 million adults alone had been victimized during one12-month period. The Star Systems survey, however, additionally asked whether the respondent personally knew someone who had ever been the victim of identity theft: 19% of respondents indicated that they had known someone, indicating that an additional 40 million people had potentially been victimized. Such disparate differences in estimates may be due to methodologies, and particularly sample sizes, which were generally much smaller than the FTC study.

Figure 2. Identity theft victimization



Source: Synovate (2003).

With regard to the reporting patterns discovered by this study:

- 43% of victims had contacted the credit grantor or company where the credit or account had been misused;
- 26% contacted the local police;
- 22% contacted a credit bureau (42% of these victims had contacted three credit bureaus);
- 12% contacted a lawyer;
- 8% contacted their state's Attorney General or other type of consumer agency;
- 7% contacted the Division of Motor Vehicles;
- 5% contacted a federal agency, such as the Postal Service or the Social Security Administration;
- 3% contacted the FTC; 8% contacted some "other" unspecified entity; and 38% did not contact anyone (Synovate 2003).
- A number of victims had also reported their victimization to more than one agency.[25]

Interesting, though unexplained, patterns were noted within reporting behavior as well[26]:

[25] *Research note*. Higher rates of reporting to credit card companies, credit bureaus or similar institutions such as banks are related to the type of identity theft experienced, but this does not explain patterns of reporting to other agencies, such as the FTC. Patterns of reporting or non-reporting may also reflect a "buy in" to the belief that the individual is not the true victim of identity theft, but additional research would be needed to examine this issue. More information is also needed on multiple reporting patterns, especially since many victims not only contact all three existing credit bureaus, but a number of other agencies in order to resolve the adverse effects of this crime. In particular, multiple reporting may be associated with the type of identity theft experienced or the extent of damage caused, but such patterns need to be explored through future research.

- Victims with household incomes of $25,000 or less were less likely to contact the company that originally issued the existing credit card or non-credit card account which had been misused, or the company that issued a new account to an offender.
- Victims of new accounts or other frauds were more likely to contact the police and more likely to contact a credit bureau; however, only 13% of victims who experienced the misuse of existing credit card accounts contacted a credit reporting agency.
- Older victims were also less likely to report their victimization than younger victims: 17% of victims aged 18-24 did not report their experience, compared to 66% of victims over the age of 65.
- When the resulting loss totaled $5,000 or more, 81% of victims reported their experience to someone; when the loss was less than $1,000, only 54% had reported their victimization.

In terms of specific types of identity theft:

- 15% of victims in the FTC survey reported that their personal information had been used in non-financial ways: 4% of victims were aware that their name and identifying information had been given to authorities or other parties when caught committing a crime;
- 3% of victims had their personal information used to obtain government documents, such as a driver's license or social security card; and
- 2% of victims had each reported that their information was used to rent housing, obtain medical care, obtain employment, or file a fraudulent tax return.

With regard to existing accounts:

- 67% of victims reported the misuse of an existing credit card,
- 19% reported the misuse of an existing checking or savings account;
- 9% reported the misuse of existing telephone service;
- 3% reported the misuse of an existing Internet account; and
- 2% reported the misuse of existing insurance account.

Finally, victims reported that various types of new accounts were opened using their information: credit cards (8%), loans (5%), telephone service (5%), checking/savings (3%), Internet (2%), other accounts (1%), and insurance (1%).[27]

Unfortunately, data from existing agency sources cannot be reconciled with the results of the FTC study, or with one another, to present a clearer picture of the problem of identity theft. For example, in 2001, the FTC reported 1,335 consumer complaints of identity theft in Los Angeles, CA, but an analysis of local police and sheriff's department records

[26] *Research note*. Such patterns require further investigation.

[27] Although the data are not comparable, complaints received by the Identity Theft Clearinghouse during 2001, 2002, 2003, and 2004 are similarly reported by type and subtype of identity theft. A summary of the data for these years can be found in Appendix 2.

indicated that there had been more than 13,000 identity theft crimes reported to the police in that year alone (Gayer 2003 citing Kathy M. Kristof, "Calif. leads nation in number of fraud complaints," *Los Angeles Times*, January 23 2003). Without more detailed information, it is impossible to know the extent to which such data converge or diverge from one another. However, some additional data provided by the GAO, offer a different perspective on identity theft, at least in terms of how it has been experienced by the three national consumer reporting companies.

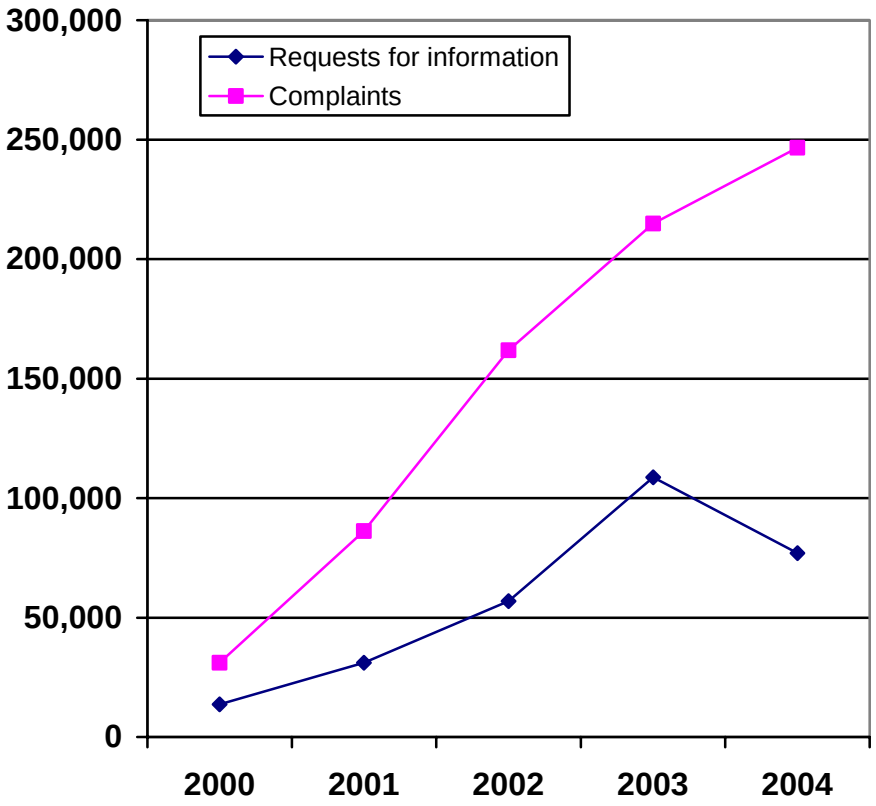
Two of the three national credit bureaus (Equifax, Inc.; Experien Information Solutions, Inc.; and Trans Union, LLC) reported increases in the placement of 7-year fraud alerts on consumer credit files, which is considered to be their most reliable indicator of the incidence of identity theft. One agency estimated that 7-year fraud alerts had increased 36% between 1999 and 2000, increasing from 65,600 to 89,000; another agency reported that its 7-year fraud alerts increased by almost 53%, increasing from 19,347 (July 1999-June 2000) to 29,593 (July 2000-June 2001); the third agency reported 92,000 fraud alerts in 2000, but was unable to provide information for 1999 (GAO 2002c:4).

Trans Union also reported that two-thirds of all consumer inquiries to its Fraud Victim Assistance Department involve identity fraud: the total number of inquiries increased from 35,235 in 1992 to 522,922 in 1997 (GAO 1998). In its first report, the GAO (1998) discovered that only one bureau (Trans Union) tracked limited fraud statistics, although all three bureaus had maintained fraud units since the early to mid 1990s. At that time, the Vice President of Associated Credit Bureaus, Inc. also noted that "the three bureaus may be willing to consider the feasibility of systematically and consistently tracking various forms of fraud, including identity fraud, if the value of such an effort outweighs the costs" (GAO 1998:39).

Correspondingly, the Identity Theft Clearinghouse reports increases in both complaints and requests for information between 2000 and 2003 as demonstrated in Figure 3; although 2004 data show a corresponding increase in complaints, the notable decrease in requests for information is currently unexplained. Overall, the FTC notes that there was substantial growth in all forms of identity theft over the past three years, and that "the number of ID theft victims who reported discovering the misuse of their personal information between 1 and 2 years ago was almost double that for the period 2-3 years ago (Synovate 2003:19). While not indicative of its extent, such collateral increases at this stage in our comprehension of the crime can only safely indicate an increased awareness of identity theft; yet these figures are likely to be augmented in upcoming years by continued public and private acceptance of, access to, and reliance on the Internet – by both offenders and victims.[28] The issue of whether the extent of identity

[28] The most recent study has suggested 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/statement monitoring (BBB 2005). As a result, the researchers recommend that individuals switch to Internet account management as a means of reducing identity theft victimization risk. Although the fact may remain that "nobody is more effective at preventing and protecting fraud than the individual" (report author James Van Dyke, quoted in Sullivan, 2005), the conclusion that online account monitoring is "safer" is problematic and requires further investigation. One

Figure 3. Identity Theft Clearinghouse activity



Sources: FTC, 2005, 2004, 2003b. See Appendix 2 for more information.

theft is increasing will have to wait until reliable standardized and centralized measurement systems are established.

Finally, in order to accurately estimate its extent, the role of identity theft as a component of other crimes such as fraud or theft, and its role as a facilitator of crimes such as terrorism, drug trafficking, alien smuggling or money laundering, must be understood. Due to the complexities involved, both its function and pervasiveness in relation to other crimes is unknown. Until such issues are clearly delineated, and properly recorded, the true extent of identity theft will likewise remain unknown.

---

analyst, for example, notes that many victims do not know how their information is obtained (although their information may in fact have been obtained online); and known estimates are biased towards victims who are likely to have been victimized by a family member or other acquaintance, thus over-representing identity theft crimes that occur offline (Sullivan 2005). Additionally, the risk posed by online activities is likely to increase - both as more individuals use such services and more offenders become skilled at capitalizing upon them. Thus, a distant "tipping point" may be reached at which online activities will not be "safer" than offline activities, if in fact they currently are. In any event, such a finding requires verification through further research.

Distribution of Identity Theft in the U.S.

Geographic patterns[29]

The FTC study is potentially the best source of geographic and trend information on identity theft, but in-depth analyses have yet to be performed, or yet to be reported if they have been conducted. Specifically, the study recorded geographic information by state, census region, Metropolitan Statistical Area, and Designated Market Area, but the actual report provides only a few scattered statistics regarding identity theft patterns within U.S. regions (Synovate 2003)[30]:

- Respondents in the West were more likely to report victimization within the past 5 years, respondents in the Midwest reported the least victimization, and residents of the South and Northeast reported at slightly higher rates than the Midwest.
- Victims in the Northeast and West were least likely to report that they knew their information had been taken before the misuse began, while victims in the South and Midwest were most likely to know.
- Respondents in the South and West were more likely to have out-of-pocket expenses as the result of the victimization and respondents in the Northeast were least likely to report such expenses.

The Identity Theft Clearinghouse Database is currently the best source for information on the geographic distribution of reported victimization data. Overall, Clearinghouse data demonstrate that the "key identity theft characteristics have remained constant except for volume" (Gordon et al. 2004:10).[31] For instance, between 2000 and 2004, identity theft was consistently the top complaint category and credit card fraud was the most commonly reported type of identity theft.

As broadly evidenced by Table 1, identity theft may also shape or be shaped by certain geographic patterns. For 2002 through 2004, the top identity theft locations were, for the most part, the largest cities within each state[32]; but this is not surprising. There are, however, potentially interesting and deeper patterns in these data waiting to be revealed. For example, in Florida, the top three "hot spots" of victim reporting between 2002 and 2004 were Miami, Orlando and Tampa. None of these cities is the largest in the state; however, they are well known tourist areas – one potentially unexplored variable in

[29] Temporal patterns are equally as important as geographic patterns of identity theft, but much less is known about them. As mentioned throughout this report, the time it takes a victim to discover the crime has a cascading effect on a number of areas including reporting, overall losses and investigation. Further research is required to uncover any additional and larger temporal patterns that may exist.

[30] Further in-depth analyses of these data should be conducted to better understand both geographic and sociodemographic patterns of identity theft across the U.S.

[31] See Appendix 2 for a summary of FTC Identity Theft Data.

[32] The top victim locations by city are reported separately for each state in 2002, 2003 and 2004 (FTC 2005 2004 2003b). More limited data are available for 2000 and 2001 (FTC 2001a,b; 2002a,b). The FTC also reports information regarding states with the largest number of aggregate complaints.

explaining patterns of identity theft.[33] Of course, many victims never need to leave their home in order to be victimized by an offender within another geographic location.

Table 1. Top 5 state victimization rates per 100,000 population

	2000*	2001	2002	2003	2004
1st	D.C.	D.C. 76.7	D.C. 123.1	Arizona** 122.4	Arizona** 142.5
2nd	Nevada	California 44.6	California 90.7	Nevada 113.4	Nevada 125.7
3rd	Arizona	Nevada 40.5	Arizona 88	California 111.2	California 122.1
4th	California	Maryland 37.3	Nevada 85.3	Texas 93.3	Texas 117.6
5th	Oregon	N.Y. 37.3	Texas 68.9	Florida 83	Colorado 95.8

*The FTC did not report the actual rates for 2000, only their ranking.
** When ordered by Metropolitan Area, Washington D.C. ranked first in both 2003 (153.4) and 2004 (183.7) - significantly surpassing the rates reported for Arizona in these years.
Sources: FTC 2005 2004 2003b 2002a 2001b.

Multiple victimization rates also vary within and among states. In 2004, multiple victimization rates varied between 15% and 23% for each state; approximately 19% of all victims reported more than one type of ID theft victimization (FTC 2005). These figures for 2003 and 2002, respectively were: 10%-23%, 19% (FTC 2004); and 15%-28%, 22% (FTC 2003b).

Specific subcategories of identity theft may also contain specific patterns. For example, new credit card account identity theft consistently dropped from 26% in 2001 to 16.5% in 2004; electronic fund transfers rose from 1.9% in 2001 to 6.6% in 2004 - more than doubling within this period (FTC 2002a 2003b 2005). However, such trends may be statistically insignificant or reflect other variations in the data – possibilities that should be investigated through further analysis.

Overall, the reasons for any geographic patterns are unclear. 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. However, data from the FTC study and the upcoming NCVS should prove invaluable for beginning to isolate the "hot spots" of identity theft activity.

Offense-specific patterns

[33] Federal law enforcement officials also note that new or different types of identity theft schemes will often originate (or appear to originate) on the west coast and then spread to the east coast (GAO 2002a). This pattern requires verification through further research.

Offenders may also follow a typical pattern of activity in order to "build validity into a stolen identity," (Cheney 2003:10) or there may be patterns concerning the uses of particular types of information, which may be similar within or across identity theft types and/or geographic regions. A social security number may present an offender with an opportunity to commit a wide variety of offenses, whereas a credit card would be more limited in terms of the time frame in which it may be reported stolen, and thus rendered defunct.[34] Although personal information may be obtained in a number of different ways, there is a seemingly finite universe of these methods, the types of information available and the ways in which it can be manipulated. Investigators, in particular, would benefit from a theoretical model (based on research findings), which maps the "life cycle" of specific forms of information (e.g., driver's licenses, social security numbers, credit cards, birth certificates), the ways in which it is obtained,[35] and the ways in which it can be used, or is typically used.

Such patterns would also be limited by the offenders' knowledge and/or ability to use the information, and by the type of information obtained. Like a rare painting, certain forms of information may be difficult to "move" for the average offender without some form of specialized knowledge. Similarly, some forms of personal information may be difficult to use without corresponding knowledge, such as the victim's mother's maiden name, which may be unknown (although it may be available if the offender knows where to look).

As mentioned throughout this report, practically nothing is known about the specific gears in the machine of identity theft, and there are a number of patterns that potentially remain unidentified or currently under-researched. More research is needed, therefore, to identify whether such patterns truly exist. In particular, such information would best be obtained from interviews with known identity theft offenders, although additional forms of data collection are also needed.

Victims

"Identity theft is a dual crime," that is, it usually affects two victims: the individual whose identity was stolen and the business whose service was stolen (Foley 2003b:5). In reality, however, individuals have not always been treated as "victims," since it was assumed that they would not take ultimate responsibility for any resulting financial loss.[36] In the words of one woman describing an attempt to report her victimization to the police, "they will lecture you, the victim, endlessly about how it's the fault of the credit card companies that you're in this position…that technically you're not the victim" (Benner et

[34] A credit card, or credit card account number, however, may give the offender access to additional personal information such as a victim's social security number or bank account number, which may then be used to commit additional offenses.

[35] See, for example, chapter 5 in Newman and Clarke (2003) and Jones (2002) for a discussion of the vulnerabilities of online transactions.

[36] See the upcoming section on the "costs" of identity theft for a discussion on the role of financial loss in victimization experiences.

al. 2000:6). Nevertheless, whether or not they are officially or technically recognized as "victims," individuals are indeed victimized by identity theft. There is also some anecdotal evidence that corporations are victimized in the same way as are individuals (Sullivan 2004).[37]

Indeed, it seems that no one is safe from this "equal opportunity crime" (Joint hearing before the Subcommittee on Oversight and Investigations 2002). The Foundation for Taxpayer and Consumer Rights, a California-based organization, reports that "it was able to purchase the Social Security numbers and home addresses for Central Intelligence Agency Director George Tenet; Attorney General John Ashcroft; Karl Rove, President Bush's chief political advisor; and other top administration officials" for $26 dollars each (Swartz 2003:16). Similarly, in 2001, a NYC dishwasher used the Internet to defraud millions of dollars from U.S. celebrities and millionaires, including Steven Spielberg, George Soros, and Ross Perot (Barrett 2002). One case involved over 100 high-ranking military officials. The lone offender was caught with a laptop containing several thousand military names, social security numbers and other types of personal information (GAO 2002a; Rusch 2001). Despite such high profile stories, however, "more often than not, identity theft is something that affects the ordinary citizen" (spoken by Darlene Hooley, Joint hearing before the Subcommittee on Oversight and Investigations 2002).

Victim demographics[38]

According to Identity Theft Clearinghouse data, which represent only those victims who reported their age, individuals aged 30-39 and 18-29 consistently reported more incidents of identity theft (FTC 2005 2004 2003b 2002a 2001a). In addition to finding that those in the 30-39 age group reported the highest incidence of identity theft, one independent survey[39] noted several additional sociodemographic trends:

- minorities reported experiencing a higher incidence of identity theft than whites;
- the incidence of identity theft increased with income;
- more males reported that someone had obtained their credit card information or forged a credit card in their name, compared to females;

[37] "…a growing number of thieves now assume the false guise of entire companies, adopting a business's employer identification number to secure commercial loans, corporate leases or expensive office products, according to analysts, security specialists and law enforcement officials" (O'Brien 2004). However, additional research would be required to determine the characteristics and extent of this form of identity theft.

[38] The FTC study reports some specific sociodemographic trends, but precious little is known about the characteristics of identity theft victims. Most of these patterns have been noted throughout this report with the exception of two findings: "Non-white victims (53%) were more likely than white victims (40%) to be concerned about future acts of misuse by an identity thief. Lower income victims were also the most likely to express concern about future victimization" (Synovate 2003:15). Collectively, such patterns are reported sporadically, both by the FTC and other sources, and are not systematically evaluated. Further research is needed, therefore, regarding specific sociodemographic variations among different types of identity theft victims. Raw data from the FTC study are available, but are largely unanalyzed (or are analyzed but largely unreported) with respect to demographic trends: http://www.ftc.gov/foia/datalayout.pdf.

[39] See Appendix 1 for more information regarding this study's methodology.

- young people, aged 18-24, more often reported that someone stole or otherwise improperly obtained a paper or computer record with their personal information and used it to forge their identity;
- blacks overwhelmingly reported that a friend, relative or co-worker had stolen their identity (P&AB 2003);
- and victims with post-graduate degrees reported being victimized more frequently than college graduates or victims with a high school degree or less (Harris Interactive 2003).

Children as victims of identity theft

There is only one source of data regarding victims under the age of 18 - the Consumer Sentinel Network. However, the data are not publicly available in disaggregated form, so the distribution of victimization across this vast age group is unknown.[40] Of the victims who reported their age to the Sentinel, there were 9,370 victims in 2004 who were under the age of 18 (4% of 234,263); 5,924 in 2003 (3% of 197,475); and 2,618 in 2002 (2% of 130,917). The Identity Theft Resource Center also reports dealing with 2 or 3 new child cases per week, which represents a minimum of 104-156 child victims per year (Davis 2004).

Child identity theft may only represent a small percentage of cases (albeit based on reported incidents), but there is some anecdotal evidence to suggest that the crime may go undetected until the victim reaches an age when (s)he begins to drive, attends college, applies for various types of loans or credit accounts, or otherwise reaches adulthood. Family members may be particularly suited to commit this type of identity theft since the parents or guardians are in control of, or have exclusive access to, the child's "identity," or pertinent identifying information. Further, some parents or guardians who detect compromises of their child's identity may only do so after repeatedly suspicious solicitations, such as receiving credit card applications in their child's name. Thus, in the absence of concrete or recurring evidence, many adults may not suspect that anything is wrong.

The deceased as victims of identity theft

The number of deceased victims in the U.S. has not been estimated, although the deceased have long been recognized as "favorite targets of identity thieves" (O'Brien 2004).[41] One U.K. fraud prevention service, CIFAS (n.d.), has dubbed identity theft of the deceased "Britain's largest growing identity theft related crime," which has grown from 5,000 cases in 2001, to16,000 in 2003, and an expected 20,000 in 2004. In one recent U.S. example, a group of thieves stole social security numbers and other credit information from 80 deceased individuals across five states. This information was sold,

[40] In at least one recent example, the identity of a 3-month-old infant was stolen (O'Brien 2004), suggesting that victimization information is needed regarding children of all ages.

[41] See the Joint Hearing before the Subcommittee on Oversight and Investigations (2002) for a discussion of this problem.

for $600 per name, to persons seeking car loans. The total losses from this Georgia-based scam were 1.5 million dollars (Teague 2004).

Not only can important personal information, such as their mother's maiden name, simply by mined from obituaries; relatives and acquaintances may once again be in a favorable position to commit this particular form of identity theft. Both children and the deceased require advocates to discover the crime and report it to authorities. However, the universe of deceased victims far surpasses that of children in the U.S. today, and is ostensibly unlimited.[42] As such, these groups require considerable attention among future research and data collection efforts.

Institutional victims

Certain groups of victims may be more vulnerable than others because of the organizations to which they belong. Students and members of the armed services may be particularly at risk. Considering the extensive use of Social Security Numbers among institutions of higher learning and students' increased opportunities for obtaining credit[43], a number of steps have been taken to specifically protect and educate college students about the dangers associated with identity theft ("Legislators try to shore up…," 2004; "ED debuts web site…," 2004; "Education department takes steps…," 2004).

> "[M]embers of the armed services may [also] be more susceptible than the general public to identity theft. Given their mobility, service members may have bank, credit, and other types of accounts in more than one state and even overseas. At times, service members may be deployed to locations far away from family members, which can increase their dependence on credit cards, automatic teller machines, and other remote-access financial services" (GAO 2002a:62).[44]

The FTC and the Department of Defense specifically established the Soldier Sentinel System (or Military Sentinel) in 2002 in response to such identity theft-related threats within the military community.

[42] The Joint hearing before the Subcommittee on Oversight and Investigations (2002) notes a range of examples regarding identity theft of the deceased. For instance, the parents of a 16 month old boy, who had died from Hurler's Syndrome, were informed by the IRS that they could not claim him on their income taxes because he was claimed by another party – their entire claim was rejected. Lofti Raisi, who was suspected of training 4 of the 19 September 11th hijackers how to fly, used the social security number of a New Jersey woman who had died in 1991.

[43] In late February 2003, hackers broke into a University of Texas computer network and stole the Social Security numbers of 55,000 students, faculty and alumni (Borrus 2003).

[44] *Research note*. The potential involvement of family members or close acquaintances in the management of a soldier's financial or otherwise mundane affairs (such as paying rent or other bills), and their potential role as offenders, suggests that additional research should examine the extent to which such positions are abused; for example, through the power of attorney.

The elderly as victims

Whereas the elderly may not be specifically targeted, they are a particularly vulnerable population in general. Specifically, they are "less likely to engage in credit dependent transactions on a frequent basis and therefore are less likely to become immediately aware that they are victims of an identity thief" (Florida 2002:3). According to complaint data, adults over the age of 65 seemingly suffer a low incidence of identity theft victimization.[45] However, the most reliable estimates now suggest that older victims may not be likely to report their victimizations: 66% of victims aged 65 and older did not tell anyone about the crime; adults aged 55 and older were also slightly less likely to report victimization within the past 5 years (9%) than the population as a whole (13%) (Synovate 2003).[46]

Repeat victimization

In relation to vulnerability, the term "repeat" or "multiple victimization" begins to take on a whole new meaning in the realm of identity theft offenses. In addition to the individual victim, several corporate victims may be involved; and any given victim may be "violated" any number of times in any number of different ways. In one study, approximately 65% of those who were victimized by the creation of a new account or other type of fraud within a five year period also experienced a different type of identity theft: 22% experienced the misuse of an existing credit card 26% experienced the misuse of an existing non-credit card account, and 16% experienced both the misuse of existing credit cards and existing non-credit card accounts. Approximately 40% of victims who experienced the misuse of an existing non credit card account or account number also experienced the misuse of an existing credit card account (Synovate 2003). Between 2001 and 2004, Identity Theft Clearinghouse data also suggest that between 19% and 22% of victims had reported more than one type of identity theft (FTC 2002a 2003b 2004 2005).[47] Such figures do not even begin to estimate the number of businesses or institutions that were simultaneously involved.

---

[45] Howard Beales (2002b), Director of the Bureau of Consumer Protection for the Federal Trade commission, noted that persons over the age of 60, representing 16% of the population, only represented 10% of identity theft complaints; although they reported credit card fraud at a slightly higher level than the population under 60 years of age. This report also notes other ways in which identity theft varies for persons over the age of 60, including a slightly lower incidence of reporting for telecommunications or utility fraud, bank fraud, employment fraud and government documents or benefits fraud. However, almost 20% of victims over the age of 60 reported that someone had attempted to misuse their information in comparison to almost 11% of victims under the age of 60. Overall, his report notes that Clearinghouse data generally show very similar experiences for those over and under the age of 60.

[46] *Research note*. Taken as a whole, further research is needed to clearly identify the most vulnerable victim groups in order to effectively direct prevention efforts.

[47] The Clearinghouse also publishes individual state estimates for victims who reported experiencing more than one type of identity theft in 2002, 2003 and 2004 (FTC 2003b 2004 2005). *Research note*. The reasons for, and patterns of, multiple victimizations among identity theft victims are currently under-developed areas of research. Further study is needed, for example, to understand whether certain types of victims are more vulnerable to "classic" identity theft victimization, or whether certain types of personal information are more conducive to multiple misuses. See Titus and Gover (2001) for an example of repeat victimization research conducted with fraud victims.

Offenders

Not surprisingly, more is known about the identities stolen by offenders than about the identities of the offenders themselves. Unfortunately, given the nature of this crime, many victims know nothing about the offender,[48] and what is known may be inaccurate or misleading. Even when some information is available, there is no indication of the basic sociodemographic characteristics of offenders.[49] As such, research in the area of identity theft offenders is critically in need of development.

The largest offender trend, noted by one survey of police officers, was their drug addiction or involvement in the narcotics scene (Gayer 2004), specifically with regard to methamphetamine.[50] According to one police officer, identity theft offenders were "[t]raditionally and initially… the white collar guy; now it is the guys that used to be in narcotics. The penalties are so stiff for drugs that they have switched over to ID theft – it is just as lucrative and much safer." (Sergeant Jim Hyde, Miami-Dade, Florida Police Department; quoted in Gayer 2004:13). Similarly, the Postal Inspection Service notes that "[m]ail theft and credit-card fraud activity frequently support drug trafficking" (GAO 1998:35). Some officers also noted a rise in organized crime rings focusing on identity theft – a pattern also observed by Postal Inspection Service investigations (GAO 1998:3). As such, the associations between identity theft and drug use, drug sale/distribution, and organized crime should be examined further.

Offender typology

A typology[51] developed for white-collar offenders may be helpful in light of the fact that the defining trait of identity thieves is that they are "opportunists" (Gayer 2004:13)[52]:

---

[48] The best known estimate suggests that only 26% of victims know who has misused their personal information (Synovate 2003). What is generally known about offenders amounts to their relationship or known contact with the victim, which is discussed below. The only exception is data from the Identity Theft Clearinghouse for 2000 and 2001. In those years, a limited number of victims provided some identifying information about the suspect. In 2001, 55% of complainants reported the state in which the suspect operated. The District of Columbia, Nevada, Florida, California and New York, respectively, had the highest number of suspects per capita (FTC 2002a,b). In 2000, 66% of complainants reported the state in which the suspect operated. New York City, Los Angeles, Chicago, Detroit and Miami had the highest number of suspects, but these results were not reported on a per capita basis (FTC 2001a,b). Aside from this tidbit, there is almost no available information, in any form, regarding the perpetrators of identity theft.

[49] Some indirect information regarding offenders may be gleaned from criminal justice outcome data related to arrests, prosecution, investigations, etc. In addition to currently being unavailable (or at worst only available for related crimes such as fraud), such data would present a skewed picture of the identity theft offender either due to the fact that (s)he was caught, or that many federal and state agencies may focus their efforts and resources on the largest cases of identity theft.

[50] ABC News reported that police in Oregon and Washington have also noticed a link between methamphetamine use and identity theft, but this connection has not been empirically established ("Meth use linked to identity theft," 2004).

[51] Most typologies of ID theft are based on method (see the typology outlined earlier in this paper) or upon motive (Newman 2004). Morris (n.d.) has attempted an identity theft typology of offender characteristics based on conversations with law enforcement officials, available data and literature reviews.

1. Low-frequency offenders
    a. "'Crisis Responders' appear to engage in criminality in response to some type of perceived crisis" (Weisburd, Waring and Chayet 2001:59). "Perceived" being the operative word, offenders in this group might range from the parent who opens a utility account in their child's name because they have ruined their own credit; or the criminal who needs to "lose" his real identity because a warrant is out for his arrest.
    b. "Opportunity Takers," respond to "the desire to take advantage of some specific criminal opportunity" (:64). This group might include the cashier who notices that a customer has left their credit card and later uses it to make an unauthorized purchase, or the ordinary person who finds a wallet on the street.
2. High-frequency offenders
    a. "Opportunity Seekers," may not only search for opportunities to commit crime, they may "create a situation amenable to committing a specific type of offense" (:78). This group would include the dumpster divers, scanners and your garden-variety thieves.
    b. "Stereotypical Criminals," are the highest-frequency offenders, "with a mixed bag of criminal conduct, and their personal histories often include difficult childhoods, substance abuse, and other problems" (:83-84). Obviously, this category of offenders may span all types of identity theft, but is particularly relevant for organized crime activities and perhaps the drug-identity theft connection mentioned above.

Organizations as offenders

If not offenders directly, businesses and other legitimate organizations contribute to the problem of identity theft. Credit bureaus, for example, facilitate identity theft by selling "credit header" information, which typically includes an individual's name, birth date, Social Security number, and current/previous address. Currently, "credit bureaus are not statutorily prohibited from releasing or selling noncredit-related, consumer-identifying information," and revenues earned from the sale of such personal information is estimated to generate "tens of millions of dollars" each year (GAO 1998:55). Similarly, "some online sites will give out your bank account balance for about $300, [and] at least a dozen sites sell Social Security numbers and other private data for a small fee." (Swartz 2003:16). Conversely, obtaining a company's identity information is not a crime, and a company has virtually no privacy rights under current law ("Companies vulnerable to

[52] Nevertheless, research using this typology with identity thieves would need to be conducted before definitive conclusions could be made about its effectiveness in compartmentalizing the characteristics of identity thieves. See Weisburd, Waring and Chayet (2001) for a full discussion of these categories and their corresponding research with white-collar offenders.

identity theft" 2003).[53] Credit card issuing companies also contribute to the problem because of their marketing practices (see Section 9).

The relationship between victims and offenders

Regarding the relationship between victims and offenders, some evidence suggests that they may know one another, although the extent of their associations is not clear. In the only year for which information is reported, the FTC (2001) notes that 19.5% of victims knew the suspect was a family member, roommate/co-habitant, neighbor, workplace co-worker/employer/employee, or some other acquaintance. Similarly, Benner et al. (2000) report that 17% of victims knew the offender, who was either a relative, business associate or other acquaintance; and the FTC study reports that of the 26% of victims who knew the identity of the person who took their information, 18% reported that it was a friend, neighbor, or in-home employee, and 16% victims reported that it was a complete stranger, although he or she later became aware of the offender's identity (Synovate 2003).[54]

Generally, the highest reported category is that of the family member. However, the results of at least one study indicate a higher number of victims who were able to track the offender back to a business (Foley 2003b). Further, as noted by one of the researchers, "friendly fraud is not only easier to detect, it also provides lenders with some recourse to recover some losses incurred. As a result many lenders will have a high percentage of reported friendly fraud incidents as other cases fall through the cracks (thus distorting the reality)" (Paul Colins in Foley 2003b:22). This comment may help to explain the pattern observed by the Economic Crimes Policy Team, which reported that, "where it was possible to determine that at least one of the unauthorized ID means used by the perpetrator/defendant corresponded to an actual individual victim, the perpetrator/defendant was related to, or acquainted with, the victim in 70 percent of such cases" (1999:15).

Some additional patterns regarding the relationship between the offender and victim have also been found. The Foley (2003b) study, for example, allowed victims to check off multiple categories of relationships with offender. As it turns out, "the imposter was active in more than one part of the victims' lives. For example, a relative could also be a caregiver, a co-worker may also be a friend" (2003b:21). Further, identity theft offenders may not only be taking advantage of close relationships with trusting victims, they may be using identity theft "as a way to abuse and manipulate a former lover, spouse or friend" (Foley 2003b:21).[55]

---

[53] *Research note*. It should also be noted that the number of organizations or employees responsible for actual cases of identity theft is unknown, although the anecdotal evidence suggests that the problem may be sizeable. This issue requires further investigation.

[54] Some victims may be unaware of the offender's identity, but later learn it as the result of a criminal investigation.

[55] *Research note*. Some anecdotal evidence also suggests that identity theft may be used as a weapon of revenge, but the roles of revenge or manipulation in identity theft have not been examined.

Finally, the FTC study (Synovate 2003) reports a wealth of information regarding victims' knowledge of the offenders' identity:

- "Knowledge of the thief's identity is more likely when the crime involves more serious cases of identity theft" (:28).[56]
- With regard to familial ties, 9% of all victims reported that "a family member or relative was the person responsible for misusing their personal information. In those cases where the ID Theft involved the opening of new accounts or the committing of other types of fraud, 52% of those who knew the thief's identity – 18% of victims of this type of ID Theft – identified a family member or relative as the perpetrator. Where the misuse involved only existing credit cards, a family member or relative was cited as the person who misused the information by only 26% of victims who said they knew who the person was" (:28-29).
- In total, 6% of all victims reported that a person who worked at a company or financial institution which had access to their information was responsible for their victimization; "[w]here the misuse involved only existing credit card accounts, someone at a company or financial institution was cited as the source of the misused information by 33% of those who knew the person's identity. In those cases that involved new accounts or other types of fraud 13% of those who knew the identity identified the perpetrator as an employee of such companies" (:29).

Nevertheless, reported estimates of victims' awareness of offenders' identities may be inaccurate or misleading to some degree.[57] Questions on the upcoming NCVS regarding the identity of the offender were dropped due to a concern about survey length and increased respondent burden. Specifically, victims misunderstood the concept of 'offender identity,' believing that they would have to know the offender's name or be able to pick them out of a line-up, rather than being able to identify the offender through their type of interaction (Hughes 2004). The questions dropped from the NCVS were very similar to the wording of the questions in the FTC study,[58] suggesting that the 26% of victims who reported knowing the identity of the offender may be under-estimated.

---

[56] This finding may also be related to the fact that more serious cases of identity theft are investigated, but more research is needed.

[57] The anonymity afforded by this crime suggests that at least some victims may believe that they know who misused their information, but that they may be incorrect. Obviously, the most reliable source of this information would result from a criminal investigation, but the extent to which victims obtain information in this manner is unknown.

[58] FTC study, question 14 reads: "Do you know the identity of the person who misused your personal information without your permission? This means you can either personally know the victim [sic] or just know the identity of the person, such as their name, etc." Any answer other than "yes" would skip the respondent to Question 16. Question 15 reads: "Was the person who misused your personal information…? A complete stranger outside your workplace; A family member or relative; Someone at your workplace? A friend, neighbor or in home employee; Someone at a company or financial institution that has your personal information; Or, someone else [specify]" (Synovate 2003). Iterations of the NCVS question regarding the identity of the offender included: "Do you or anyone in your household know who misused the (credit card account/existing account other than a credit card account/personal information) without permission?"; "Do you or anyone in your household know the identity of the person who misused the ("fill") without permission?; and "Do you or anyone in your household know the identity or anything else about the person who misused the ("fill") without permission?" Due to misinterpretation of these versions of the question, a related question, "Was the person who misused the information…A complete stranger?; A family member

5. THE COST OF IDENTITY THEFT

Estimating the "cost" of identity theft is a much more difficult task than estimating its extent. Currently, there is "[n]o comprehensive or agreed-upon way to estimate [the] economic costs," of identity theft, thus no comprehensive estimates exist (GAO 1998:48; 2002c). [59] The difficulties associated with this task are further compounded by those discussed with regard to estimating its extent, and by the interpretation of the term "cost" that is adopted.

Financial costs: Businesses

The practical and favored interpretation defines "cost" as financial. Financial costs may be both "hard," or easily calculated, such as the expected cost of a new software system to track identity theft cases; and "soft," which may include, for example, various types of management costs – costs that are much more difficult to estimate (Lucas 2004). For example, Digimarc Corporation recently contracted with the Alabama Department of Public Safety to renovate its driver's license system. The "initial procurement" (hard) cost of this contract was $9.5 million dollars, but this does not include any resources necessary to implement or maintain the new system, or any (soft) costs that can be expected to upgrade the system in later years (Boulard 2004).

Overall, one "conservative" estimate reported is that "identity theft accounts for at least tens of billions of dollars in losses…[w]hen we consider that the collective losses occasioned by credit card fraud, insurance fraud and health care fraud are in the hundreds of billions of dollars per year, and that identity theft comprises a significant part of these crimes" (Willox and Regan 2002:5). This estimate may indeed be conservative.[60] However, we currently have no way of gauging the amount of identity theft that occurs in relation to these or other associated crimes. The GAO, therefore, in the most extensive[61] attempt to estimate the costs of identity theft to date, examined various estimates provided by a number of public and private agencies.

---

or other relative?; Someone at work?; A friend?; A neighbor?; An in-home employee such as a babysitter or housekeeper?; Someone at a company or financial institution that has access to personal information?; Someone else (specify)?" was not tested and ultimately subsequently dropped (Hughes 2004).

[59] Victims are often asked to report the total value obtained by the thief, representing the loss to businesses, as well as any additional expenses incurred. However, the figures that are reported vary widely by the type of identity theft experienced and the total time of misuse until discovery. They are not helpful in determining aggregate loss amounts.

[60] A recent study conducted by Javelin Strategy & Research suggests that "the annual dollar volume of identity fraud is highly similar to 2003 figures ([reported by Synovate and] adjusted for inflation) at $52.6 billion" (BBB 2005).

[61] The sources of data collected by the GAO to estimate the financial costs of identity theft are not inclusive of all potential sources of identity theft or identity fraud information. As mentioned, not all relevant government agencies collect such information. However, the fraud losses calculated for payment cards are for MasterCard and Visa only, and do not include estimates for other general purpose cards (American Express, Diners Club and Discover), which account for about 25% of the market; other merchant-specific cards issued by retail stores; or information from various other entities such as insurance companies and securities firms, which may incur identity theft-related costs. (GAO 2002c:7)

In terms of direct losses, MasterCard and Visa, the two largest credit card companies, estimated that "aggregated identity theft-related losses from domestic operations rose from $79.9 million in 1996 to $114.3 million in 2000, an increase of about 43%" (GAO 2002c:6). These estimates, however, are based on only two recognized categories of identity theft (account takeovers and fraudulent applications). Neither MasterCard nor Visa consider categories such as lost or stolen cards, never received cards, counterfeit cards, or mail order/telephone order fraud to be identity theft-related. Including such categories, "the associations' total fraud losses from domestic operations rose from about $700 million in 1996 to about 1 billion in 2000, an increase of about 45%." However "…the annual total fraud losses represented about 1/10 of 1% or less of U.S. member banks' annual sales volume during 1996-2000" (GAO 2002c:6-7). "Certain credit-card fraud categories [also] have a larger dollar impact than other categories. Among cases involving credit-card fraud at large banks, counterfeiting, fraudulent applications, intercept in mail, and account takeover accounted for 23 percent of the cases but 44 percent of the dollar losses. Lost and stolen credit cards made up 66 percent of the fraud cases but 49 percent of the dollar losses" (GAO 1998:47).

A survey by the American Bankers Association reported that, "of the total check fraud-related losses in 1999, the percentages attributable to identity theft ranged from 56 percent for community banks (assets of $500 million) to 5 percent for superregional/money center banks (assets of $50 billion or more), and the average for all banks was 29 percent" (GAO 2002c:6). Actual losses for that year were reported to be $679 million.

Although the GAO (2002c) reported that data pertaining to direct fraud losses indicated increasing costs, data related some of the 'softer costs,' such as staffing of fraud departments, presented a mixed and/or incomplete picture. One national consumer reporting agency reported that staffing levels of fraud operators in its Consumer Services Center had remained relatively constant since 1997; another agency reported that the staffing of its fraud victim assistance department doubled between 1997 and 2001, and that the cost of the department in 2000 was $4.3 million; the third only reported that the cost of its fraud assistance staffing was "several million dollars" (GAO 2002c:7). Similarly, the American Bankers Association noted that banks devote varying resources to check fraud prevention, detection, investigation and prosecution depending upon their size. Its 2000 survey revealed that community banks, on average, spent less than $10,000 for such expenses, while superregional/money center banks each spent $10 million or more (GAO 2002c:7).

The identity theft-related costs to the credit card industry can also be expected to grow with the passage of the Fair and Accurate Credit Transactions Act of 2003, which places liability for the resolution of disputed credit report data on the provider of the data in question. "A substantial portion of these costs will fall on collections agencies, which must report consumer disputes that come to them regarding information contained in their credit report…These costs come on top of the July announcement that…Equifax and…Trans Union will charge their business customers 11 cents more per credit report

starting in December 2004…Experien followed by upping the price of a credit report for commercial clients by 8%" (Lucas 2004:52). Whereas the total dollar loss of such costs cannot be estimated, one of the anticipated "soft costs" will be incurred through increasing staff levels in order to investigate complaints. Such increases, however, are accepted in the industry as "their cost of doing business under the FACT Act" (Ibid).

Other 'soft' costs, such as those associated with the technological "arms race,"[62] are difficult to foresee, although, "[I]t is costly to add new security features to documents, as they provide relief for only as long as it takes the criminals to defeat the new system" (Gordon et al. 2004: 36)[63]. Such prevention costs are not directly reported, and may be included in estimates of management costs related to commercial fraud departments. However, the American Bankers Association did provide one estimate suggesting that the total loss avoidance costs assumed by banks alone in 1999 totaled $1.5 billion dollars (GAO 2002c:6).

In general, identity theft losses or other associated costs are swallowed by their respective financial institutions. Many consider such losses an ongoing cost of doing business, and may have found it easier to write off the loss rather than to investigate or prosecute such cases. Although it is not their only means of redress, some institutions may attempt to offset their losses by increasing their prices, thus shifting some of the burden for these costs onto consumers (Ashman et al. 2002:7). As mentioned, some companies may also decide to offset some of their costs by selling "credit header" information, which potentially generates tens of millions of dollars each year (GAO 1998:55).

In any event, the effects of identity theft on businesses in general are seemingly reciprocal since this crime may not only have "long-term negative impacts on consumers' purchasing power," (GAO 1998:45); but a similarly damaging effect on "consumer confidence in using electronic commerce and the vast benefits of the information age" (House Committee on Government Reform 2004 – spoken by Orson Swindle, Commissioner, Federal Trade Commission).

Financial costs: The criminal justice system

As noted, a number of government agencies do not maintain separate statistics related to identity theft. Many of the agencies reporting to the GAO, therefore, provided estimates based on while-collar crime or other categories of financial crimes. Many of these estimates were not directly related to costs, but to arrests, investigations or prosecutions. It can generally be assumed that higher rates of criminal justice outcomes will translate

[62] For further discussion of this concept, see the upcoming section on "The Role of Technology and the 'Arms Race.' It should also be noted that some new security features may not be completely effective until old features are phased out of the existing system, and the costs of overhauling an entire system may be prohibitive.

[63] Additional costs are also related to nested or layered security measures, sometimes referred to as "Defense in Depth" or "concentric defense," in which multiple barriers are used to "deter, help discover, or destroy" an offender's efforts to infiltrate a target (Major Cities Chiefs Association 2004:25-26).

into higher criminal justice operating costs, although such data do not present an accurate picture of the identity theft-related costs incurred by the government.

1. Investigation costs

- Between 1995 and 1997, the Secret Service estimated that actual costs associated with identity fraud arrests were $442 million, $450 million and $745 million, respectively; but these costs included losses to victimized individuals and financial institutions and reflect the agency's focus on investigating high-dollar cases (GAO 1998:29). Its best estimate of the average cost for a financial crimes investigation in 2001 was $15,000, but such cases vary so much that this estimate is actually meaningless (GAO 2002c).
- The FBI estimated the average cost of an investigation by its white-collar program to be $20,000 between 1998 and 2000, but this figure has "no practical significance" (GAO 2002c:10). Further, many cases handled by these agencies do not involve elements of identity theft, which may require considerably more resources to investigate.
- The IRS reported fraud losses from questionable tax returns decreased from $44 million in 1994 to $9 million in 1997. The reason for decline was a reduction in IRS staff (GAO 1998). There is also no way to gauge the percentage of losses that may have actually been due to identity theft.
- The Social Security Administration /OIG reports that the number of social security misuse investigation increased from 305 in 1996 to 1,153 in 1997, but this increase was due, in part, to the hiring of additional investigators (GAO 1998). Nevertheless, investigations by the SSA are focused on issues of program integrity, rather than identity theft, which is investigated by various other federal and state agencies (GAO 2002c)

2. Federal Prosecution.

The only available prosecution data suggests that federal prosecutors handled approximately 13,700 white-collar crimes in 2000, at an estimated cost of $11,400 per case – actual costs may be much higher or lower (GAO 2002c). Nevertheless, officials in several of the individual states contacted by the GAO reported that current resources to investigate and prosecute identity theft cases are often inadequate. In addition to the need for more prosecutors and support staff to prosecute cases, police agencies needed to be properly trained in the intricacies of investigating identity theft. It was also noted that "police departments are more inclined to use their limited resources for investigating violent crimes and drug offenses rather than handling complicated identity theft cases that, even if successfully prosecuted, often lead to relatively light sentences" (GAO 2002a:17). However, at least one police department uses volunteers to staff their identity theft program, which doesn't cost them a dime (Kingman 2004).

3. Corrections.

Finally, with regard to the costs of corrections, 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. Offenders are then supervised in the community by federal probation officers for a period of 3-5 years at an average cost of $2,900 per

offender – a cost that does not include any special conditions such as community service, electronic monitoring or substance abuse treatment (GAO 2003c).[64]

Financial costs: Individuals

Some individual victims do incur financial costs,[65] even though it is commonly assumed that businesses will bear the burden of financial damage. One study found that the average out-of-pocket expenses reported by victims were between $30 and $2,000, but this estimate does not included any lawyer's fees that were incurred.[66] The average loss to victims in this study was $808 dollars, but most estimated spending around $100 (Benner et al. 2000).

The average amount of out-of-pocket expenses for all types of victims, as reported by the FTC, was $500; however, the average out-of-pocket expenses for victims in cases where a new account had been opened were $1,200. Victims who quickly discovered that their information was being misused were less likely to incur out-of-pocket expenses.[67] Victims with incomes of less than $75,000 were also more likely to pay out-of-pocket expenses than victims with higher household incomes; and residents of the South and West Census regions were most likely to have paid out-of-pocket expenses than residents of the Northeast, who were the least likely to pay such expenses (Synovate 2003). Overall, one estimate provided by the National Fraud Center, "conservatively" estimates the costs of identity theft to individuals to be $50 billion dollars per year (Gordon and Curtis 2000).

Personal costs (non-financial)

Individuals suffer various types of additional "costs" as a result of their victimization:

- "Human" costs include the time and effort required to resolve various problems created by the theft, the emotional impact or feeling of "violation" that often results,[68] and the frustration of being harassed by debt collectors or dealing with various agencies in trying to resolve problems.

[64] The average cost of community supervision is $8.02 per day/$2,900 per year, but can range up to $31.46 per day/$11,400 per year.

[65] Most victims (63%) suffer no out-of-pocket expenses (Synovate 2003); however, anecdotal evidence suggests that some victims may ultimately have to file for bankruptcy as a result of their victimization.

[66] In total, 49% of victims contacted an attorney; many contacted attorneys at public interest law firms and received advice for free. Attorneys' fees, when paid, ranged from $800 to $40,000 (Benner et al. 2000:3).

[67] A recent study concluded that the financial losses of victims who monitored their accounts online were less than 1/8 of those incurred by victims who discovered their victimization through paper statement monitoring; an average of $551 compared to $4,543 (BBB 2005). These results, although interesting, require further investigation and explanation.

[68] Foley (2003b) describes a range of emotional reactions reported by victims including strain on personal relationships, sleep disturbances, overwhelming sadness, fears for financial safety, and a sense of powerlessness.

- "Opportunity costs" include the victim's inability to obtain a job, purchase a car, or qualify for various types of loans, and the loss of their job – all of which may translate into additional financial costs.

Such costs are experienced regardless of whether the individual has been held responsible for any financial losses by an institution; and many costs, both personal and financial, are interrelated. For example, "the requirement to prove fraud [to some financial institutions] leads to a delay before action can be taken to control the associated fraud exposure. This delay is crucial because it provides more time for thieves to continue the fraud associated with the stolen identity and, hence, increases the total losses realized by all parties" (Cheney 2003:13). Such delay also increases the frustration of victims who require some form of immediate help or cooperation to resolve their problem. The following additional personal problems are experienced by identity theft victims:

1. Communication problems

Victims report problems merely trying to contact various agencies for assistance.

- A number of victims experienced difficulty while attempting to submit a report to the police; a substantial percentage of victims in the FTC study who contacted the police were dissatisfied with their response (Synovate 2003) - a pattern noted in other victimization surveys.[69]
- Victims also noted difficulties in attempting to contact all three credit bureaus, particularly in trying to speak with a "live" representative (Benner et al. 2000). Victims in the FTC study reported generally low levels of satisfaction with credit bureaus. Most victims contacting their credit card companies were satisfied, but satisfaction was lower among victims who experienced the opening of a new account, and in cases where the loss exceeded $5,000 or more. Less than two-thirds of the victims in the Benner et al. (2000) study felt that the credit bureaus had been effective in removing fraudulent accounts, and despite the placement of a fraud alert on their credit report, 46% of victims reported that financial fraud reoccurred.[70]

Overall, the lack of assistance available to victims is frustrating. In the words of one victim, "[t]he current system is not created for actual assistance, it is created to perpetuate the illusion of assistance." (Benner et al. 2000:5). Victim frustrations are also increased when their cases remain unresolved or when no offender is identified or arrested. And when offenders are caught[71] they may be likely to receive little if any punishment – further increasing the frustration experienced by victims.[72]

---

[69] Benner et al. (2000), for example, noted that 76% of those who had contacted the police felt that they were unhelpful.

[70] There is currently no requirement that a fraud alert be acted upon by the credit industry (Florida 2002).

[71] In one study 21% of victims reported that the offender had been arrested, but on other charges (Benner et al. 2000).

[72] To add insult to injury, one study reported that, "[i]n 19 cases, criminals continued to use and abuse their victims' information after arrest and 10 continued after being sentenced" (Foley 2003b:19).
Research note: One inmate, who was serving a 9-year sentence for similar crimes affecting victims in Florida and Georgia, was found to be orchestrating an identity theft scheme from the gulf County Correctional Facility (FL) - using both the inmate phone service and mail system to obtain victims'

2. Loss of time.[73]
According to the FTC, 34% of victims were able to resolve all of their problems in one hour or less, 29% spent between 2 and 9 hours to resolve their problems and 36% spent more than 10 hours. 6% spent over 240 hours trying to resolve their problems.[74] Respondents over the age of 55 were significantly more likely to settle their problems sooner. The amount of time needed to resolve problems is also dependent upon how quickly the misuse is discovered: 76% of victims who discovered the misuse less than one month after it began spent less than 10 hours resolving problems. When it took longer than 6 months to discover, only 20% of victims were able to resolve their problems in this time frame (Synovate 2004).

3. Agency inflicted suffering.
Other common issues noted by victims include:

- Damage to their credit report or similar credit card and/or banking problems;
- harassment by collectors;
- rejection for a loan or insurance policy;
- having utilities cut off;
- having a law suit filed against them or having a criminal investigation filed or warrant issued for their arrest.

Such additional problems were experienced more often by victims who had a new account opened in their name (Synovate 2004), which may be related to the type of personal information originally stolen. Some actual examples include:

- One company president, who frequently travels as part of his work, has to carry a letter from law enforcement officials explaining that he is not the drug dealer using his identity (Givens 2000b).
- One victim was told that he would have to travel to Florida in order to petition its Court to remove a fraudulent account placed on his credit line in that state (Florida 2002).
- One man had to get a death certificate "undone" after a thief died using his name (Higgins 1998).

4. Shock of discovery
Benner et al. (2000) report that most victims discovered the theft in one of two ways: either through denial of some type of loan (30%), or through contact by a collection

---

personal information. The subsequent crimes committed by this offender and his five accomplices netted more than $200,000 in stolen property from their victims (GAO 2002a). The extent of identity theft committed behind bars is unknown and should be investigated, in addition to the potential involvement of corrections staff in their commission.

[73] Loss of time may also translate into financial losses for victims. One survey reported that 49% of those surveyed had missed work due to the identity theft incident. The average number of hours reported was 389, although the median was 35 (Foley 2003b). One victim noted that the process of clearing up the mess created by her victimization was "nearly a full-time job" (Benner et al. 2000:5).

[74] Findings from a recent study suggest that the average time necessary to resolve problems dropped from 33 hours in 2003 to 28 hours in 2004 (BBB 2005), but the reasons for this decrease are not clear.

agency demanding payment (29%)[75]. The type of identity theft experienced may also affect the method of discovery. Only 8% of victims who had a new account opened reported being notified by a bank or credit card agency, although 18% of these victims were notified by other parties, including debt collection companies or government agencies. Only 8% of all identity theft victims discovered the problem through a loan denial, but 18% of victims who had new accounts opened discovered their victimization in this manner (Synovate 2003).

5. Other personal suffering

There are also countless numbers of other examples that do not even begin to capture some of the unimaginable "costs" suffered by victims (see also all cases in Appendix 4):

- One victim's marriage was nearly "destroyed when the identity thief, posing as the victim, was in an automobile accident in another state with a member of the opposite sex as a passenger" (Florida 2002:24).
- In one case of "necrolarceny," a police department notified a New Jersey woman that her husband, who was believed to have died in the World Trade Center, had just committed a traffic violation in North Carolina. Unfortunately, this woman's rekindled hope soon turned back into tragedy when she realized that a thief had stolen her husband's identity (Abernathy 2003).

Finally, for some victims, there is an ever-looming threat that new offenses will surface, even after initial problems have seemingly been resolved. In the words of one victim, "It seems as if as soon as I have put out one fire another is lit. It seems as if there is no end to this infringement upon my civil liberties" (Benner et al. 2000:7).[76]

Societal costs

The difficulty of estimating such intangible costs, combined with a general reluctance to recognize the non-financial impacts of identity theft victimization, potentially provide an additional explanation as to why individuals have not historically been treated as "victims." However, there are a number of societal costs that are equally impossible to calculate, yet indirectly and indiscriminately victimize "non-victims" and society as a whole.

Such costs include:

- national security risks/threats[77];

[75] The Synovate study reported that many victims discovered the theft on their own through examination of their account statements (52%), or were otherwise notified by some type of company (26%) (Synovate 2003).

[76] Some victims spent over a year trying to disentangle themselves from the problems associated with their theft 14% of all victims were still dealing with the problem more than two years after discovery, and 17 victims were involved for 3 or more years (Foley 2003b). Benner et al. (2000) similarly note that it took victims an average of 23 months to resolve associated problems; some cases that were still open had been so for 4 years. One victim had been dealing with her problems for 13 years.

[77] See Joint hearing before the Subcommittee on Immigration, Border Security, and Claims (2002) for a full discussion of this problem.

- public safety risks/threats[78];
- burdens created by the presence of illegal immigrants;
- potential constitutional intrusions underlying proposed schemes for a national centralized information database, national ID cards, or the use of biometric methods of identification[79] - and their associated financial costs;
- higher premiums or other costs passed on by companies to consumers;
- increased paranoia, which may also result in financial costs associated with the purchase of preventive insurance[80] or other methods of personal identity theft prevention;
- and overall decreased confidence in the promised benefits of the information age.

Whereas additional research efforts should be focused on understanding all types of costs incurred by individuals, institutions and societies in relation to identity theft, this may not only be an infeasible task, it may also be "jumping the gun" with respect to the current state of data collection and theoretical development in the field of identity theft. Nevertheless, reported patterns of identity theft-related costs should be verified through continued research.

6. EXPLAINING IDENTITY THEFT: THE ROLE OF OPPORTUNTIY

The concept of opportunity[81] as it is developed in the situational crime prevention approach offers the most useful way to understand why identity theft occurs, and perhaps why it has increased in recent years. While little formal empirical research has investigated whether opportunity factors contribute to identity theft, there is a large body of research showing how opportunity contributes significantly to other types of crime.

---

[78] General public safety can be threatened by identity theft when offenders pose as "qualified" or trained professionals such as doctors or individuals with Commercial Driver's Licenses.

[79] See chapter 8 in Newman and Clarke (2003) for a discussion of privacy, surveillance and situational crime prevention.

[80] Some businesses now offer identity theft coverage free of charge, but others charge a yearly fee. The costs of such insurance can range from a modest fee to a few hundred dollars depending on the coverage offered (Block 2003; Ashman et al. 2002; "Equifax first to market…," 2003; Dugas 2003). One estimate suggests that the direct-to-consumer costs of such protection is $75 million per year, but stands to triple over the next four years ("Equifax first to market…," 2003). However, there are additional hidden "costs" to consumers. Equifax, for example, not only receives revenue from the fees associated with such programs, it requests additional information from consumers who sign up for service. Equifax reserves the right to sell this additional information unless the consumer "opts out" – an option that is neatly and discretely contained in the disclosure notice for the service (May 2002).

[81] *Research note*. There is some confusion in the popular literature as to the meaning of "opportunistic" in contrast to planned or organized. It generally has two meanings, though these are related. First, it may mean that the offense is carried out on the spur of the moment, when an opportunity presents itself. For example, an individual at the checkout counter may leave a credit card behind. The next person in line may take the card and use it. The second meaning is that offenders are constantly scanning for opportunities to exploit, looking for weaknesses in the security systems that contain their targets. In this case, offenders actually plan their offenses, exploiting opportunities that present themselves. Thus it is possible to think of both planned and unplanned offenses as "opportunistic." A significant research question may be to establish the extent to which identity theft may be spur of the moment or a one-time event as against carefully planned and organized. The answer to this question also has important implications for prevention, as noted below.

Newman and Clarke (2003) have recently applied this approach to an analysis of ecommerce crime where they argue that information is the target and information systems the tool by which offenders may perpetrate their ecommerce crimes. In particular, they suggest that information may be conceived of as a "hot product." Thus, since a person's identity is composed primarily of information, this approach may also apply to identity theft.

Identity and its Authentication as the Targets of Theft

What is an "identity"? What is it that is stolen in an identity theft? There are many different ways to answer this question, depending on the perspective.[82] The popular view of identity is that it is primarily a psychological construct used by individuals to refer to themselves as "a person" and used by others to identify them as unique or particular individuals. It is the idea that identity is a psychological construct that lies at the base of the claim that individual victims of identity theft have lost something more than simply money or suffered even more than the annoyance of having to straighten out their credit records and bank accounts: something bad has happened to their good name.

Establishing a person's identity is extremely difficult, which is why victims of identity theft have great difficulty in "getting back" their identities. A brief review of this process reveals the weaknesses in establishing identities that can be exploited by offenders. The authentication process generally isolates two primary parts to an identity: biology (what we are) and life history (who we are).[83] In order to authenticate an identity we must be able to assess each of the two, and then clearly establish the link between them. This is a difficult task. We know, for example, that individuals have many attributes that are unique to them such as retinal patterns, finger prints, DNA etc. Verifying the name of this unique person is the problem. Our rather meager attempt to link what we are to who we are is typically a photograph of the individual attached to a piece of paper or plastic, issued by an authoritative body which depends on documents issued by other authoritative bodies that issue documents pertaining to the applicant's life history. There are basically four sources of these: public databases (records of birth, marriage, tax records etc.), commercial databases (energy or telephone bill, mortgage papers), professional and employment history (school or university, educational degrees), and family records (family referees, parents or guardians). A short list of documents deriving from these sources includes (Jones and Levi 2000):

- Social security card
- Electoral register entries
- Passport
- Employment information from

[82] The meaning of identity and its relationship to anonymity in economies and civil society is complex and fascinating. Anonymity for centuries has been a cornerstone of the trust required in the market place for the exchange of goods and services (Newman and Clarke 2003; Seabright 2004). Yet at the same time it has been necessary for societies to develop complex organizations and procedures that collect detailed information about every individual (Marx 2001; Newman and Clarke 2003). It is this paradox that makes authenticating identities so difficult, particularly in "open societies" (Jones and Levi 2000).

[83] Some argue that there is a third, such as a signature, which lies somewhere in between biology and life history since it is a behavior that is learned early in life.

- Mortgage account information
- Property ownership and leasehold
- Credit account and other financial facilities information
- Insurance policies
- Marriage and financial associations
- Higher educational qualifications
- Payment systems facilities – debit/credit/check/charge cards, virtual wallets, "PayPal," etc.
- Energy and tax bills
- applications for financial services
- Previous addresses
- Previous authentication events
- Telephone numbers – fixed and mobile
- Library cards and other memberships
- Records of birth, marriage and death
- E-mail address
- Forwarding addresses – re-directions
- Health cards
- Driving license

One can see, however, that there is a circularity in this authentication process. What documents provide more authenticity than others? Which are "primary" and which are "secondary"? Very few, if any, are truly primary, that is, provide a direct link between who one is and what one is. Thus, the great difficulty in establishing a primary document that links the life history of the individual to his or her biology is a very serious point of weakness in establishing identity. If an offender can obtain just one or two of these documents, it is possible to "breed" additional documents. The short list of sources above also shows clearly that very large amounts of personal information reside in many places. The huge change that has occurred in the last twenty years is that this information no longer exists in large rooms full of filing cabinets, but in a small room in a single computer. It would have taken many trucks to remove the personnel records of the State of California employees 20 years ago. A few years ago, the entire database was stolen by a computer hacker.

In sum, if we conceive of identity as composed primarily of information that is linked to a biological reference via an information system or specific technology, then it is possible to analyze the opportunity structure that makes it easy to steal this information and that reveals weaknesses in the process of authentication. We may begin with the observation that "Hot products attract theft" (Clarke 1999:2).

Identity as a "Hot Product"

The notion of "hot products" developed by Clarke (1999) demonstrates how particular products are more prone to theft than others. The attributes that such products have are described by the acronym CRAVED: the products are Concealable, Removable Available, Valuable, Enjoyable and Disposable. Clarke and Newman (2003) have demonstarted the uncanny fit of information as a hot product to this model which we adapt here to fit identity theft. CRAVED identities are:

> ***C****oncealable*. Thieves may have thought it easy to remove a magazine from a stand in a store and conceal it under their coat. On the Internet one can steal information including the personal information of others without ever having personally to possess it, and can do so from half way around the world.

***R**emovable*. The whole raison d'être of the Internet is that information is removable. In fact, it is constantly on the move. It is therefore intrinsically vulnerable to interception and deflection to places that it was not originally intended. Files are removable and replicable countless times. Millions of individuals' identities are embedded in those files.

***A**vailable*. Some argue that the true revolution of the Internet is that it has made *all* information potentially available to *everyone*. Personal information and records are there for the taking. In fact, one does not even have to steal them. One can buy identification information such as social security numbers cheaply, breed other identification documents from them, and then convert these into cash.

***V**aluable*. In the information society, information is like money (actually, in the case of banks it *is* money). There is much information on the Internet that has immediate value to criminals: valuable credit card numbers, bank accounts passwords etc., which they can use to commit a wide variety of fraudulent crimes in someone else's name.

***E**njoyable*. Joyriding was a favorite delinquency when automobiles became all pervasive in the 20th century. The literature on hackers, who are often clever schoolboys (and sometimes mischievous adults), clearly demonstrates the joy they experience in overcoming the challenge of breaking into protected computer environments (Levy 1984). For the identity thief, the rewards come when stolen identities are converted into cash or when they commit crimes in another person's name.

Disposable. The literature on disposal of stolen goods has suggested that the availability of a fencing operation enhances the chances of particular items being stolen (Sutton 1995). Disposal of stolen identities takes on a slightly different meaning than the traditional notion of disposal of hot products. The latter are called "hot" of course, because continued possession of the stolen goods increases the risks of getting caught. In the case of the identity thief the immediate disposal of the identity is not so pressing. Rather, what is needed are convenient outlets where the identity may be used and reused until it is no longer of value. As we have seen above, the time available to use an identity may stretch from days to years. So in this case, the value of the identity to the thief lies in its continued use, rather that its disposal. For the identity thief, fences aren't needed.

Newman and Clarke (2004) also argue that the system in which much personal and business information resides – very often connected to the Internet – may be described as a "hot system" that offers substantial opportunity for crime. The characteristics of the information systems they summarize with the acronym **SCAREM**:

***S**tealth.* The thieves, in fact anyone, can make themselves invisible on the Internet, a perfect condition for carrying out a crime (Denning and Baugh 2000).

Identity theft is a logical choice.

C*hallenge.* The literature on computer criminals who are hackers is replete with one primary motivation: to "beat" the computing system (Clough and Mungo 1992).[84] Taking on another's identity adds even more to the thrill of the crime.

A*nonymity*. Anonymity abounds on the Internet. It differs from Stealth which is sneaky and secretive, whereas anonymity is a common way of doing business, such as, for example, when one pays for an item with cash in a retail store. There is research evidence linking anonymity to deindividuation, a psychological condition that allows individuals to act irresponsibly or criminally (Wortley 1997).

R*econnaissance.* Perhaps the most important element in the choices that a criminal makes in carrying out a crime is the choice of a suitable target. The Internet makes it possible to scan thousands of web servers and even millions of personal computers that are connected to the web, looking for "holes" or gaps in security. Fraudsters can peddle their scams to millions of email users for virtually no cost (though legislation has recently increased the penalties for spamming).

E*scape*. The crime-inducing aspects of the information system environment of anonymity, deception and stealth combine to make it extremely difficult for law enforcement to link the crime to the individual perpetrator, especially when the crime itself may never be detected, even by its victims (Ahuja 1997).

M*ultiplicity*. A traditional theft, such as a bank robbery, is a relatively finite act. However, if an offender hacks into a bank's files, this one crime can be multiplied exponentially, since it makes available to the offender a huge number of new opportunities to commit crime by exploiting access to the bank's accounts which include personal and financial information. We have also seen how the theft of identity can be used to facilitate the commission of a variety of other crimes.

SCAREM provides highly attractive opportunities to steal information. And the personal information that contributes to one's identity moves constantly through that SCAREM system. Thus, the opportunities available to offenders to commit identity theft are major factors that account for both the commission of the crime and its apparent increase in recent years.

[84] Almost all major break-ins of computing systems - where databases of personal information reside - have resulted from persistent activity by the hacker over long periods of time, from one month to several months. A short list includes: the Internet worm released in 1988; "Hacker in the cuckoo's egg" in which an East German spy penetrated the US department of defense network in 1989; an intruder who stole IDs and passwords from a NYC Internet Service provider in 1993; in 1995 source address spoofing resulted in widespread denial of service; in 1995 $10 million was stolen from Citibank computers by a Russian who deflected fund transfers to his own accounts; in 1996, after a break-in to Harvard's computers, hackers penetrated a US government network (Ahuja 1997).

Exploiting Opportunities: Techniques of Identity Theft

Offenders have developed various techniques to exploit the opportunities of the information age. The techniques used by identity thieves may be divided into roughly two categories: techniques they use to steal the identities, and techniques they use to convert these identities into the rewards they seek.[85]

How offenders steal identities

Some of the notoriety of identity theft rose with media coverage of the dangers of buying and selling on the Internet.[86] However, the ways offenders steal identities are primarily low-tech. Some methods are more popular than others, as is clear from Figures 4 and 5.

- They steal wallets or purses from shopping bags, from cars, or by pick pocketing.
- 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 that is useful to offenders includes pre-approved credit card applications, energy or telephone bills, bank or credit card statements, and convenience checks.[87]
- 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

[85] *Research note*. It should be noted that, except where indicated, the data on which these lists of techniques are derived are taken mostly from Internet sources of varying kinds. These include newspaper and magazine reports, media interviews with fraud investigators and law enforcement personnel, and information provided on various advocacy web sites seeking to either help victims or to sell services designed to prevent victimization by identity theft. There have been no formal studies of identity thieves' practices or techniques that have conducted interviews or observations directly with the thieves. The exceptions to this observation are the studies on check and credit card fraud by Mativat and Tremblay (1997) and Lacoste and Tremblay (2003).

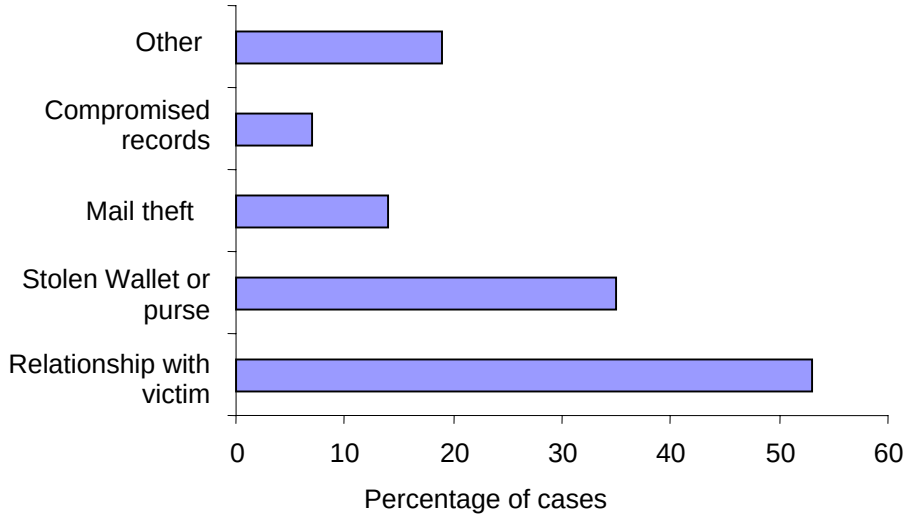
[86] Internet-related identity theft probably constitutes a small proportion of all identity theft, less than 20 percent, though there are limited data to support this impression. Javelin Research & Strategy (BBB 2005) found that less than 5% of identity theft cases (in which the cause was known) occurred during online transactions; only 11.6% could be attributed to other forms of computer crime including the use of spyware, computer viruses and computer hackers. Synovate (2003) notes that 13% of all victims' information was obtained through a transaction (Figure 5), including those via the Internet, but more research is needed to weed out Internet-related identity theft from other forms. 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 may then be used to commit thousands of identity thefts off-line. The high percentage in Figure 5 of victims reporting that they did not know how they lost their personal information suggests that the loss could have occurred via the Internet or other electronic means over which the victim has no control.

[87] In 2002, the USPIS made 5,858 mail theft arrests. The first quarter of fiscal year 2004 saw 1,522 mail theft and identity theft arrests by the USPIS nationally (http://www.identitytheft911.com/).

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 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 (GAO 2002b).
- 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 (Newman and Clarke 2003).
- 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.

Figure 4. How personal information is obtained



Source: GAO-02-363, 27. *Note*: This graph represents only those victims who knew and reported how their information was stolen. This constitutes 20.5 percent of all victims who complained to the FTC during the period covered (1999–2001). One victim may report that multiple methods were used. The Better Business Bureau website (2005) contains a similar, but more detailed graph for a 2004 study conducted by Javelin Strategy & Research.

Figure 5. How accounts are stolen

Source: Synovate (2003)

Source: Synovate (2003).
Theft Note: Nearly a quarter of all victims who knew how their information was obtained reported that their information had been lost or stolen: 14% of all victims reported that their wallet, checkbook or credit card had been lost or stolen; 4% of all victims cited stolen mail as the source of their information.
Transaction Note: 13% of all victims who knew how their information was obtained reported that their information had been taken during a transaction, either through the credit card receipt or through a purchase made via Internet, mail or phone.
"Other" Note: 14% of all victims who knew how their information was obtained reported some "other" type of means, including people who had access to the information such as a relative or co-worker, or individuals who had been given the information and later used it for some other purpose.

How offenders use stolen identities

- They open a new credit card account using the victim's name. All this requires, apart from the applicant's address, is 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 (Willox 2000).
- 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.

Why Do They Do It?

Concealment

Covering up past crimes is a major reason for individuals to steal or assume another's identity. Kathleen Soliah, wanted for various bombings and attempted murder in relation to her activities in the Symbionese Liberation Front in the late 1960s, assumed the identity of Sara Jones Olson (a common Scandinavian surname in Minnesota). She evaded capture for 23 years, and in the meantime became a doctor's wife, mother of three, community volunteer, veteran of charity work in Africa, and practicing Methodist living in an upscale neighborhood in St. Paul, Minn. Terrorism is the most recently cited example of stealing identities to conceal illegal activities, and to make tracking their true identities much more difficult after they have committed crimes. All 19 of the September 11th terrorists were involved in identity theft in some way (Willox and Regan 2002). This resulted in the mistaken arrest of people whose identities had been stolen.

Financial gain and other anticipated rewards

Perusal of cases reported on the Internet suggest two "motives" or anticipated rewards of identity theft: financial gain (Case 13), and revenge (Case14). Of these, financial gain is easily the most often mentioned.

A note on motivation

While there are endless theories in criminology that seek to explain why offenders do what they do, we suggest that the two major factors in causing offenders to make identity theft their crime of choice are the anticipated rewards and the advantage of concealment intrinsic to the crime, both of which are clearly expressed in a number of the techniques used by offenders (as described above) and in our outline of the CRAVED and SCAREM

characteristics of identity and its authentication. We hasten to add that there is little formal academic research in respect to identity theft that supports (or does not support) this assertion. When we consider that it is mainly access to financial information and records that makes the stealing of the identity possible, and then the opening of bank accounts and use of credit cards that leads to financial gain of the offender, it is reasonable to conclude that the primary motive is in fact financial gain. However, it bears repeating that the co-primary reason why identity theft is the crime of choice for many offenders, compared to other means of theft, is because it is easier to commit. By easier, we mean that not only are there many more opportunities available, but also that the crime's intrinsic characteristic of making it possible to conceal one's identity and thus carry out the crime undetected, makes it a most attractive crime. In other words, identity theft is safer and more convenient than other kinds of theft.

7. THE LAW ENFORCEMENT RESPONSE TO IDENTITY THEFT

Reporting and Recording of Identity Theft

As a result of the media coverage and congressional hearings on identity theft that occurred in the years immediately before the Identity theft law of 1998, law enforcement took the brunt of criticism because it had not responded to the individual victims of identity theft, especially those of "classic" identity theft (Cases 24 and 25) in a way that helped solve their problem. Indeed, the police often perceived the problem as not one that they, the police, should be dealing with. It was, after all, the credit card issuing companies and banks who were taking the bulk of the financial loss. Furthermore, it was also well known that retail stores and banks and merchants generally, along with individual cardholders, rarely reported theft or misuse of a credit or bank card to the police.

Even today, the FTC reports that only 26% of victims report the incident to the police (Synovate 2003). And it is further well known that merchants and banks rarely report to the police the crimes that occur on their premises or in their workplace (Clarke 2001). There are a number of reasons for this, but among them the primary one is that businesses prefer to deal with their losses without outside interference, and often businesses will treat some crime that occurs in their workplace – shoplifting or credit card fraud for example – as simply a cost of doing business. The losses are factored into inventory loss (called "shrinkage"). Retailers especially are wary of police presence on their place of doing business for fear it will scare away customers. So the perception by police that identity theft was not primarily their responsibility but that of business factored into the casual way in which individual victims were treated.

Another equally important reason why victims were given the runaround (see Case 10) was that established reporting and recording practices in most if not all police departments were not set up to record these crimes. Identity theft is a crime that in the course of its commission may span several jurisdictions. A victim's credit card may be stolen in Ohio, used in New York or on the Internet to purchase expensive items which

are shipped to an address in California, but the individual victim may live in Texas and the credit card issuing company is headquartered in Delaware. So which jurisdiction should record the criminal event? Thus, the legal and bureaucratic structures of many police departments were not equipped to deal with this complex crime.

With the passing of the 1998 Identity theft federal law, and other laws since then (see Section 8), much more attention has been given to dealing with individual victims by local police. The 1998 law also gave prime responsibility to the FTC to assist consumers both to avoid becoming victims and to reduce the suffering caused them if they are victimized. Recent legislation that requires credit reporting agencies to respond quickly to victims to correct their records[88] will likely increase the number of individuals reporting the crime to police, since they are required by credit reporting agencies to submit an Identity Theft Affidavit, which requires a police report. The IACP (2000) has passed a resolution urging police departments to provide police reports for identity theft victims, and recently has further urged that the rule to be followed is that the police department in the jurisdiction in which the victim lives should take responsibility for issuing the report (GAO 2002a).

Two important issues need to be researched in response to this scenario:

1. The issue of crime incident reporting. As noted, information concerning identity theft lies in many different places, and it may be a prime or facilitating motive in a number of traditional crimes such as robbery, mugging, pick-pocketing, theft from cars, burglary etc. Do the crime incident reporting systems that police departments currently use have sufficient flexibility to collect such information, and if so is the necessity to be on the lookout for such information communicated to line officers by way of a simple form or procedures for recording these events?

2. The issue of flexibility of information systems. Is the crime incident database structure used by the police department set up in such a way that allows for the crime analyst to check across many different crime types or incidents to see if in fact there are any identity theft related issues or patterns? The question of how a database should be structured in order to address problems (as opposed to cases) is an issue that would also be worth consideration.[89] This may in fact be a more basic and fundamental issue that should be addressed by all police departments that have information systems in use, and for all manner of crime incidents and information collection generally.[90]

[88] 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.

[89] *Research note*: The issue boils down to the question of whether law enforcement databases and information systems which are designed specifically for investigation of cases are able also to be used effectively for solving problems. Or does the breadth of information that problem oriented policing requires demand a different database structure and different sets of data? See for example the review of crime analysis in America (O'Shea et al. 2002 and 2003).

[90] *Research Note*: There is an obvious need for the application of GIS techniques to the study of identity theft because the crime typically exploits to its advantage both time and space. For a review of the state of the art in police reporting systems see Skogan et al. (2004).

Finally, there is one additional pressing problem in relation to issuing police reports. Credit reporting agencies have expressed concern that ID theft affidavits and police reports submitted to them by consumers may themselves be false[91]. Clearly there is an opportunity for dishonest consumers who have heavy debts to claim that someone else ran up the charges. Thus, there is an urgent need for (a) research into the actual incidence of false reporting of identity theft both to credit agencies and to police, and (b) procedures and technologies if appropriate that police departments need to take to prevent their police reports from being forged or otherwise corrupted.

Harm Reduction

Awareness of victim needs

No research has been conducted on the effectiveness or lack of effectiveness of police response to victim needs. Evidence available is mostly anecdotal, much of it either collected by various interests that maintain web sites, or from victim testimony to Congressional hearings of various kinds. Some consumer advocacy groups also have collected information, some from interviews (CALPIRG 2000) or surveys of previously identified victims (Foley 2003b). In both studies the samples were limited in size, though they did provide very useful information concerning victim distress. The cases described in Appendix 4 cover the typical kinds of cases described by these groups. Cases of "classic identity theft" (Case 10) are those that accentuate the individual suffering of the victims, and it is these that most likely, as we suggested in the beginning of this paper, contributed to the wide publicity and eventual legislation addressing some of the issues that exacerbated the suffering of identity theft victims. However, the effectiveness of the legislative changes and the efforts by the FTC to educate the public and agencies concerning the harm caused by identity theft are generally assumed simply by their very strong presence in the media. The latter has also been enhanced considerably by the various advertisements of companies on television warning of identity theft.[92] There is no research as to the extent to which this change of attitude toward this crime has seeped down into the rank and file of police departments. Nor has there been any study of compliance of the credit reporting agencies in response to the legislative requirements for swift response to victims.

Effective police response

In the absence of research on police awareness of the problem of identity theft, there is no

[91] Although we could find no statistical evidence to support this claim, this concern is expressed anecdotally and in comments by some businesses in response to the FTC regarding the proposed legislation to require credit reporting agencies to furnish credit reports within a specific time period (http://www.ftc.gov/os/comments/factaidt/EREG-000033.htm) .

[92] An indicator of public awareness of identity theft is shredder sales. Although there are no formal statistics available, news articles report that sales have increased astronomically over recent years. Staples Inc., for example, sold 1.3 million shredders in 2003, up 63 percent from the previous year (Ambrose 2004). Similar increases have been reported in other stores such as Office Max.

shortage of recommendations for police response to alleviate the harm done to the victims of identity theft. The responses listed below are generally prescriptive and based on those outlined by Newman (2003 and 2004a).

- The benefits of quick response. The costs to the victim – both in terms of out-of-pocket expense and in time spent resolving problems – are substantially smaller if the misuse is discovered and dealt with quickly. No out-of-pocket expenses were incurred by 67 percent of those who discovered the misuse of their personal information within 5 months (Synovate 2003). Likewise the more quickly local police can pursue the case and help the victim to report the crime to the various credit agencies the less harm caused.
- Education through community outreach.[93] Many victims may not know what to do once they discover that they have been victimized, or that swift action on their part may minimize the damage done. Local police, as part of their outreach programs may help in educating consumers concerning these matters and steps they can take both to avoid their victimization and to report their victimization should it occur. Many police departments now have information on their web sites and some offer online ways of reporting victimization. Directing victims to Internet resources or providing them written materials that explain how the recovery process works may help in reducing victim's suffering.
- Effective communication. The FTC has reported that the most common complaint they hear is that "The police just don't care." It is important to communicate to the victim that the police do care and for police to be constantly reminded that victims of identity theft often have been repeatedly victimized, that identity theft is an emotionally abusive crime (Foley 2003b). In responding to the victim's request for a report or investigation of the offence, police are urged to adopt the victim as a partner. Anecdotal evidence suggests that victims are a major source of information in regard to investigation, both in terms of the financial records that may need to be accessed by the investigator, and in terms of developing a list of possible suspects (see section on investigation below).
- Crisis response plan. Should it happen that a major theft of an agency's database of customer or employee records occurs, it is important that the business or agency have in place a crisis response plan that will minimize the effects on potential victims. Such a plan would usually include (a) toll free dedicated phone lines for employees to call the three major credit bureaus to warn of the theft and (b) information packets distributed to potential victims on what to do to protect their identities and reduce damage.[94] Is it the responsibility of law enforcement, especially local law enforcement to ensure that businesses and agencies have such a response plan?

[93] Though there are many police outreach programs targeting a variety of problems, few have been evaluated in terms of effectiveness, and when they have, with mixed results. For example, for an evaluation of outreach programs in schools see Gottfredson (1997).

[94] The FTC has published a Business Response Guide on what a business should do if the personally identifying information in its files is compromised. http://www.ftc.gov/bcp/conline/pubs/buspubs/idtbizkit.htm.

Task Forces and Cross Jurisdictional Issues

Aside from providing anonymity, identity theft offers many offenders the advantage of physical distance, which is a serious disadvantage to both victims and authorities attempting to bring offenders to justice. Ensuing jurisdictional issues complicate the reporting, investigation and prosecution of identity theft cases, as well as the creation and effectiveness of related legislation. In particular, "the prevalence of identity theft and the frequently multi- or cross-jurisdictional nature of such crime underscore the importance of having means for promoting cooperation or coordination among federal, state, and local law enforcement agencies" (GAO 2002a:19).

One such method is the FTC's Consumer Sentinel Network, which was created as a tool to coordinate law enforcement investigations. Other tools used to facilitate coordination and cooperation among agencies include task forces, coordinating bodies (such as the Attorney General's Identity Theft Subcommittee), and national training seminars on the problem of identity theft. The most common means used by law enforcement agencies to deal with multiple jurisdiction cases is the task force. Overall, task forces – both formal and informal - simplify all aspects of identity theft cases by increasing the advantages available to authorities through pooled resources, information and expertise. This results in stronger and more thorough investigations, more seamless continuity for cases through the stages of the criminal justice process, and avoidance of duplicative efforts by various agencies.

Given that various federal, state, and local agencies have roles in investigating and prosecuting cases of identity theft, task forces can have participation from all levels of government, and may include private sector entities such as banks or victim advocacy groups. The discussion of "state" and "federal" efforts that follows, therefore, is somewhat misleading since many of the efforts organized by one sector may likely contain the participation of agencies from another.

Cooperative efforts falling somewhat outside the realm of the U.S. government have also been created. For example, the Coalition on Online Identity Theft, which includes companies such as Microsoft Corp., eBay Inc., Amazon.com Inc., the Business Software Alliance, Network Associates Inc.'s McAfee Security division, and Cyveillance Inc., adopted a four-pronged strategy to combat online identity theft:

- Promote technology to deal with the problem;
- expand public education campaigns;
- share information about emerging fraudulent activities to improve detection and response and
- work with government to ensure stronger penalties for cyber-thieves (Vijayan 2003; Fisher 2003).

Nations belonging to the Organization for Economic Cooperation and Development recently announced the first multinational pact, consisting of 29 of the world's wealthiest nations, to fight cross-border fraud. This initiative, spearheaded by the U.S., allows for closer cooperation and information sharing among investigators in participating

countries. However, while the pact does not mandate changes, it does recommend that participating countries pass laws to adopt its guidelines; the European Union is expected to order member countries to codify the recommendations (Davidson 2003).

State efforts to address the cross-jurisdictional issues

Many states have created their own task forces in addition to participating in those led by federal agencies. A complete counting of each state's efforts is beyond the scope of this review. Much of the readily available information is limited to examples of states that have reported to investigative bodies such as the GAO.[95] Two notable examples of states that have coordinated various types of task forces on the problem of identity theft are California and Florida.

California. The California Attorney General's Office established five regional task forces in the mid-1990s to assist the cross-jurisdictional investigation and prosecution of high-technology crimes, including cases of identity theft and fraud. One of these, the Sacramento Valley High-Technology Task Force, was reorganized in 1999 as a separate division within the Sacramento County Sheriffs Department and contains participants from local, state and federal agencies representing 32 different entities from 34 counties within the eastern judicial district of the state. In 2001, this Task Force had investigated 153 cases involving identity theft. One case involved at least 25 victims whose credit card information had been stolen by one of three known suspects from his place of employment (GAO 2002a).

One informal task force was created in Southern California to examine the problem of identity theft and the legislative changes necessary to enable its victims to clear their names. This task force, as of 2000, consisted of the Los Angeles District Attorney's Office; the California Attorney General's Office; the Judicial Council of California; the Department of Motor Vehicles; the Los Angeles Police Department; the Los Angeles Sheriffs Department; Beth Givens, Director of the Privacy Rights Clearinghouse, and one other consumer advocate; and two victims of identity theft. The work of this task force enabled two bills centered on victims' rights to be introduced into the California Legislature (Givens 2000a).

Florida. In 2001, the Florida Attorney General's Office of Statewide Prosecution and the Florida Department of Law enforcement (FDLE) created a statewide task force to target the perpetrators of identity theft. Operation LEGIT (Law Enforcement Getting Identity Thieves) consists of 5 full-time Special Agents (as of 2001), and other regional personnel from both local and federal agencies, who investigate cases of identity theft and conduct

[95] *Research note*. Whereas information is available on the number of states that have adopted identity theft legislation, no such information is available on the number of states that have created inter-agency/cross-jurisdictional task forces, or implemented similar means to address this issue in the investigation or prosecution of identity theft. This information, however, may be available through state websites or other sources of state-disseminated information. Further research is needed to understand the existence and extent of such efforts in order to further promote cooperation and avoid the duplication of efforts. No state task force effort has been evaluated in terms of its effectiveness.

educational seminars on the investigation of identity theft-related cases for law enforcement audiences across the state (Florida 2002). The investigation of one case by the Hernando County (Florida) Sheriffs Office, the Florida Department of Law Enforcement, the Office of Statewide Prosecution, and the SSA/OlG led to the capture of one Florida suspect who had used the identity of a California victim for more than 12 years. Between 1987, when the victim had lost his wallet on vacation in Daytona Beach, and 2001, when the investigation was initiated, this offender had purchased and sold homes, opened bank and utility accounts, obtained credit and had been arrested at least three times using the victim's name. The victim had been wrongly arrested in California (on a Florida warrant), been held in jail for more than one week, and had several civil judgments against him before his thief was captured through the efforts of this task force.

The Florida Highway Patrol (FHP), which has the responsibility to conduct criminal investigations of suspected driver's license fraud, implemented a special task force based in South Florida. In addition to this special task force, there are 12 FHP investigators who perform various duties - including the investigation of suspected driver's license fraud - across the state. One top ranking law enforcement officer is assigned to consult with Division of Driver License administrators and act as a liaison to external law enforcement agencies regarding driver's license fraud and security issues. The Department of Highway Safety and Motor Vehicle and the Division of Driver License have also joined together to create a separate fraud unit consisting of 11 people who perform civil investigations of suspected driver's license fraud (Florida 2002).

Federal efforts to address the cross-jurisdictional issues of identity theft [96]

No single federal agency has jurisdiction over cases of identity theft. As such many federal agencies are involved in efforts to combat this problem. As of 2002, the Secret Service was the lead agency in 38 different national task forces related to financial or electronic crimes, which often contain identity theft-related elements. However, none of the 38 task forces focuses exclusively on the problem of identity theft.[97] One identity theft-related investigation, led by the electronic crimes task force of the Secret Service's New York Field Office in cooperation with the New York Police Department, discovered a group of perpetrators who had obtained (through the use of the internet and cellular telephones) and fraudulently used the credit card account information of some of the wealthiest chief executive officers in the nation, in addition to various other citizens. This group had further attempted to transfer almost $22 million from victims' legitimate brokerage and corporate accounts (GAO 2002a).

The SSA/OIG has increased its efforts to work with federal, state and local law enforcement officials to investigate and prosecute Social Security Number misuse, particularly cases in which it is misused to facilitate terrorist acts, in the wake of

[96] *Research note*: The examples of federal efforts described are not exhaustive and none have been evaluated in terms of their effectiveness.

[97] See GAO (2002a) for more information about these task forces. We are aware that additional task forces have been set up in various states since this GAO report, but have been unable at this point to find any additional information in regard to numbers of cases these task forces have investigated.

September 11th. By 2002, "Operation Safe Travel" had identified 186 individuals working at the Salt Lake City (UT) International Airport who had misused Social Security Numbers for security badge applications and employment eligibility verification (GAO 2002b).

The U.S. Postal Inspection Service (PIS) also has several initiatives designed to address credit card fraud and other identity theft-related crimes perpetrated through the U.S. Mail System. Since 1992, the Credit Card Mail Security Initiative has brought together various federal law enforcement agencies and credit card industry representatives to discuss theft issues and develop solutions. The PIS has also spearheaded task forces in 10 different U.S. cities, which include participation from other law enforcement agencies. Florida's task force, for example, was responsible for the arrests of 32 individuals suspected of running a credit card fraud ring responsible for at least $1.5 million worth of losses (GAO 1998 2002c).

Attorney General's Council on White Collar Crime Subcommittee on Identity Theft

Following the enactment of the 1998 Identity Theft Act, the Attorney General's Council on White Collar Crime established the Subcommittee on Identity Theft, whose membership includes various federal, state and local representatives. Specifically, the Subcommittee was created to encourage cooperation and coordination among investigative and prosecutorial strategies to address identity theft cases involving multiple jurisdictions. The Subcommittee is also involved in promoting consumer education programs and has established a number of multi-agency task forces focused on combating identity theft. However, the Subcommittee is informal and has no specific directives, such as a mission statement, which are seen as counterproductive to promoting member participation (GAO 2002a,c).

The Know Fraud initiative

The Know Fraud initiative, which began in November of 1999, is a partnership of several private and government agencies, including the PIS, aimed at educating consumers about how to protect themselves from mail fraud. A second initiative was also launched in 2001. The initiative, which focuses on identity theft, is "the largest consumer protection effort ever undertaken, with postcards sent to 123 million addresses across America, arming consumers with common sense tips and guidelines" (GAO 2002c:38).

The FTC's Efforts

The FTC has worked closely with a number of public and private entities to manufacture cooperative efforts aimed at preventing and combating the problem of identity theft and assisting its victims.

- Protecting victims. The FTC maintains lead coordination with other government agencies and organizations in the development and dissemination of educational materials consisting of print resources, media mailings, and radio and television interviews. A number of these materials can be found on their Web site. Further,

the ID Theft Affidavit – a standardized victim reporting form that can be used to resolve identity theft debts with all three major credit reporting agencies and many other creditors – was created through coordination with both private industry and consumer advocates.[98]

- Investigations. Consumer Sentinel victim complaint data are made available to federal, state and local law enforcement agencies through a secure, encrypted Web site. Law enforcement agencies, for example, can use Clearinghouse data to coordinate investigations, isolate high-impact cases or identify other patterns of identity theft. The Commission also launched an identity theft case referral program in cooperation with the U.S. Secret Service. A full time special agent and an identity theft team develop case leads by examining patterns in the database and the use of other investigative resources. Significant patterns are then referred to one of the Service's Financial Crimes Task Forces located throughout the country for further investigation and prosecution (Beales 2002b; GAO 2002c).
- Increasing awareness. Whereas the efforts of the referral program have increased the speed of identifying investigative leads, centralized analysis of the database has been limited and few law enforcement agencies have accessed the Clearinghouse database.[99] Nevertheless, this resource is still relatively new and efforts are being made to increase use and awareness of the database. The GAO has specifically recommended that the Identity Theft Subcommittee promote the Consumer Sentinel Network and the Identity Theft Clearinghouse to all levels of the law enforcement community. Further, Clearinghouse staff worked with North Carolina's Attorney General to send letters to every other state Attorney General explaining the FTC's identity theft program and how available resources could be used to assist residents, investigators and prosecutors from every state (GAO 2002a,c; FTC 2003a). Similar outreach efforts include state and local training seminars providing information, technical skills and strategies for investigating and prosecuting both traditional and high-tech forms of identity theft; and a law enforcement "Roll Call" instructional video and CD-ROM resource guide produced by the Secret Service. These materials will be sent to over 40,000 law enforcement departments across the country (FTC 2003a; Beales 2003).
- Police report initiative. This initiative was originally created in conjunction with the Identity Theft Subcommittee and the International Association of Chiefs of Police to encourage police officers to take reports from identity theft victims. The resolution adopted from that collaboration called for all law enforcement agencies

[98] Between August 2001 and May 2003, the FTC distributed more than 264,000 print copies of the Affidavit, and there were nearly 351,000 hits to the Web version (Beales 2003; FTC 2003a).

[99] The Consumer Sentinel Network may be used by law enforcement agencies free of charge; however, each agency must enter into a confidentiality agreement with the FTC. A total of 46 federal agencies and 306 state and local law enforcement agencies had signed the agreement as of May 2002; the list of these agencies can be found in Appendix IV (GAO 2002a). California has the largest number of Sentinel users (45), but police departments in cities with large numbers of reported cases such as Los Angeles, Sacramento and San Jose have not subscribed. Similarly, in Texas, two jurisdictions that incorporate almost 22% of the state's population - the Houston Police Department and the Harris County Sheriffs Office - do not use the system. Houston has also been identified as one of the top cities nationally to report victims of identity theft to the FTC. Overall, the number of state and local law enforcement subscribers seriously under-represent the more than 18,000 law enforcement agencies that exist (GAO 2002a).

to take more positive actions in recording incidents, not only to assist in tracking incidents, but to send a more positive message to the public who generally leave their local departments with the impression that the police do not care (GAO 2002a). As a result of this initiative, all three credit reporting agencies (CRAs) have agreed to block inaccurate identity theft-related information from a victim's credit report if the victim provides the company with a police report of the incident (Beales 2002a).

- Joint fraud alert. The CRAs have recently launched a "joint fraud alert." After receiving a request from a victim for the placement of a fraud alert on his or her credit report, the CRA will now share that request with the other two CRAs, thus eliminating the need for the victim to contact each company separately. Under this initiative, the FTC will also begin a one-year pilot program to refer victim complaints and requests for fraud alerts, received through the Sentinel Network, to the three CRAs (Beales 2002a; FTC 2003).
- Protecting personal information. Finally, the FTC is also working with private institutions to identity ways of keeping personal information safe from identity thieves. During an informal roundtable, the FTC and representatives from financial institutions, credit issuers, universities, and retailers examined possibilities for preventing unauthorized access to personal information in employee and customer records. The FTC will also publish a guide for organizations of all sizes on how to protect personal information and assist them in evaluating their current security protocols. A business kit will also be available detailing the necessary steps to take in the event of an information compromise (FTC 2003a). Despite their efforts, however, most cases of identity theft are best addressed through criminal prosecution and the FTC itself has no direct criminal law enforcement authority (Beales 2002a). This situation may change in some respects if a pending bill in Congress is passed to grant the FTC authority to prosecute cases of cross-border fraud (Davidson 2003).

Investigation and Prosecution[100]

While various federal, and numerous state and local law enforcement agencies have a role in investigating and prosecuting identity theft, most identity theft cases fall within the responsibility of local investigators and prosecutors. Nonetheless, all agencies face shared challenges with regard to multi-jurisdictional issues and the lack of resources, staff and training required to handle the investigational and prosecutorial complexities of identity theft. Further, the time it takes many victims to discover their victimization can hamper investigative efforts, and victims themselves can often provide little assistance to investigators. Private financial institutions may also be unwilling to cooperate with

[100] Due to number of agencies involved in the investigation and prosecution of identity theft, the following discussion focuses on general points directly related to cases of identity theft. For a more complete though not exhaustive discussion of this issue, see the GAO reports, which review the specific efforts of various federal agencies and ten states that have either a high incidence of identity theft or the oldest identity theft statutes (Arizona, California, Florida, Georgia, Illinois, Michigan, New Jersey, Pennsylvania, Texas and Wisconsin). Such cases, however, may not be representative of the processes involved in the investigation or prosecution of all identity theft cases.

investigations. In terms of the aggregate number of cases investigated or prosecuted, however, there are no comprehensive statistics on any enforcement results, under any specific federal or state statute, related to investigations, arrests, prosecutions or convictions (GAO 2002a).

State investigation and prosecution

In many cases, cross-jurisdictional issues lead local enforcement agencies to view the case as "someone else's problem." Thus, local police departments will refer the victim to the department in which the offense occurred, and that police department will subsequently refer the victim back to the jurisdiction in which they live (GAO 2002a). To address this problem, some states have passed statutes that allow multiple counties simultaneous jurisdiction. Arizona's statute, for example, would allow a victim whose credit card is stolen in Phoenix and used in Tempe to report the crime in either jurisdiction. Florida's statute similarly allows cases to be investigated or prosecuted in the county in which the victim lives or the county in which any element of the crime occurred. Wisconsin, is considering the enactment of a similar amendment to its identity theft law (GAO 2002a). Nevertheless, the effects of such statutes are unknown.[101]

Encouraging both victims and police to report incidents is recognized as a crucial first step to any investigation, but the difficulties associated with identity theft do not stop there.[102] Identity theft is often wrapped up in other offenses, which may involve highly technical and intricate components.[103] Even investigations of traditional forms of identity theft can easily become complicated. Further, the mere possession of information may not, in and of itself, be a crime. Rather that information must be used to deceive or commit some other type of offense. Examples of difficulties faced by state investigators are:

- Offenders' identities may be difficult to ascertain depending upon the type of identity theft committed or the methods used to commit the crime. A single offender may also use more than one identity or alias, which may similarly confuse investigations. In one case, a man whose real name was Steven M. Shaw obtained the personal identifying information of other men named Steven or Stephen "X" Shaw through his place of employment. This man used the identities of his counterparts to steal over $100,000 before a fraud analyst at one company caught a discrepancy in the application he had filed (May 2002).[104]

[101] Florida's Grand Jury report notes that not enough agencies are acting upon this recently enacted statute (Florida 2002), but more research is needed in all jurisdictions with such statutes, and the results should be compared to jurisdictions without them.

[102] See Gayer (2003) for the impressions of law enforcement officers on the difficulties posed by identity theft investigation.

[103] Several states investigate identity theft crimes under their economic or high tech crime units, or may have a specialized task force or similarly specialized division in place to deal with investigations.

[104] It should be noted that neither credit bureaus nor providers have a legal duty to inform the authorities or the victim of suspected fraud cases. In this case, the analyst did report the incident leading to the arrest of Steven M. Shaw; many others may simply deny the fraudulent application.

- A single piece of personal information may also be obtained through several different sources, which is time consuming and difficult for investigators to track. Driver's licenses, for example, may be stolen, re-issued by legitimate agencies, either through a mistake or a corrupt employee, or counterfeited. One investigation of driver's license fraud found that persons wanted by the police routinely conducted business with impunity at various license offices in Florida due to the lack of "real-time" electronic information sharing among agencies. This investigation also found that private driving schools were often used to obtain fraudulent licenses, both common and commercial, which were available through the payment of a small fee (Florida 2002).

- One study reported that, "on average, law officers surmised that only 11% of identity theft cases received by their departments are solved" (Gayer 2003:4).[105] Anecdotal evidence from victims similarly suggests that their thieves were arrested on unrelated charges, not as a result of the identity theft investigation. As a result, many offenders are not caught[106] or may be released if they are not linked to their respective identity theft crimes. One inmate who had escaped from a state prison in Alabama stole a man's identity and used it to hide from authorities in Los Angeles. This offender was then arrested for murder in L.A., but later released. After new evidence emerged in that case, authorities sought to re-arrest the offender and a nationwide alert went out for the victim's arrest. The victim was arrested a total of five times and later filed and won a lawsuit against the city of Los Angeles[107] (May 2002).

- Authorities detained one conspirator in the 1993 World Trade Center bombing when he arrived at JFK International airport in 1992 with a suspect Swedish passport. Subsequent inspection of his luggage revealed instructional materials for making bombs. This man was sentenced to six months' imprisonment for passport fraud. Later convicted for his role in the World Trade Center bombing and sentenced to 240 years in prison and a $500,000 fine, this defendant used, and was in possession of, a number of additional false documents (GAO 1998 2002b).[108]

---

[105] The number of active police investigations within a given jurisdiction is unknown, and existing estimates may be somewhat inaccurate. For example, in 2001, the California Deputy Attorney General reported to the GAO that the Los Angeles Police Department had reported 5,000 active identity theft cases; when contacted directly by the GAO the department mentioned over 8,000 cases of identity theft had been reported by residents of Los Angeles in 2001 (GAO 2002a), although all may not be actively under investigation.

[106] One study reported that thieves have a better than one in 700 chance of being caught by federal authorities, but the methods used to obtain this estimate are unclear (Gartner, Inc. 2003). See Appendix 1 for a description of this study.

[107] Rogan v. City of Los Angeles (1987).

[108] One of the new provisions included in the Fair Credit Reporting Act requires banking regulators to identify and maintain a list of "red flag" indicators of identity theft for use in their oversight and regulation of financial institutions (FTC 2003a; Hughes 2003). In light of the example presented here, law enforcement agencies require a similar list of "red flags" to identify potential identity theft, although such a list may already exist.

Aside from the use of the Clearinghouse as an investigative tool, a number of opportunities exist for law enforcement to make greater use of existing data and resources (GAO 2002a); but further understanding of their role and possible triangulation to aid investigations is necessary. There may also be a number of yet unidentified technologies and data that may assist investigations.[109] 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.[110] Law enforcement and other investigative bodies should also begin to strategically and creatively weigh the strengths and weaknesses of identity thieves against their own strengths and weaknesses to formulate the most effective methods of prevention and apprehension (Major Cities Chiefs Association 2004).[111]

Regarding state prosecutions, little is specifically known aside from the information collected by the GAO. One deputy prosecutor in Michigan noted that, in the first eight months since the state's identity theft statute went into effect, only one case had been initiated in Oakland County. Similarly, a chief deputy attorney stated that the Philadelphia District Attorney's Office does not handle identity theft cases, but estimated that between 100 and 200 identity theft cases had been investigated during 2000 – a "small fraction" of the total number of cases reported in Philadelphia (GAO 2002a:18). In 2001, a California Deputy Attorney General reported handling four active cases – a "tiny drop in the bucket" with regards to its prevalence. However, these active cases had one common element: they all involved hundreds or "never ending" amounts of victims (GAO 2002a:13). The high-impact or high-dollar focus of prosecutions is often referred to in anecdotal sources, but more research is required to understand the dimensions of this pattern and the effects of reporting and legislation on its occurrence. Another problem has been the necessity for victims to travel long distances from their homes to the courtroom in order to give testimony.[112]

---

[109] ID Analytics Inc. has examined more than 200 million credit applications from various financial sources to develop a fraud pattern-recognition technology (Hulme 2003). This technology and its resultant insights are available to companies and may be helpful, and subsequently available, to investigative bodies. Other industry-related risk management tools may similarly be useful to investigators if they are not already used. The Netherlands Police also compile a database of documents reported lost or stolen (Gordon et al. 2004), which if not of direct assistance, may be used as a model for a similar U.S. database. The Netherlands database further contains the details of deaths within the country; the SSA currently maintains and distributes a Death Master File, although its quality has been questioned (Joint hearing before the Subcommittee on Oversight and Investigations 2002).

[110] The Republic of Ireland and the United Kingdom have signed a Memorandum of Understanding with regard to increased sharing of documents and information (Gordon et al. 2004); similar agreements with U.S. bordering countries would be undeniably valuable, but physical borders alone do not define jurisdiction. With respect to investigations, further information is required to understand the potential for creating and acting upon such agreements, as well as their potential drawbacks and benefits. Agreements will also be affected by existing or pending legislation, particularly as they relate to information privacy, and the extent of this connection should be examined.

[111] To further assist local law enforcement and federal prosecution efforts, the Office of Community Oriented Policing Services has funded a project to develop a national model anti-identity theft strategy based on best practice within the field. The model will be completed in 2005.

[112] Personal communication between prosecuting attorney and department of Justice, November, 2004.

Finally, while victims clearly have a cause of civil or criminal action against the identity thief, most do not have any remedy against third parties, such as credit bureaus or issuers, who may also be at fault.[113] Currently, there are few legal consequences for companies that fail to protect personal information, although private lawsuits against companies that suffer security lapses may "soon constitute a high-profile 'new breed' of legal case" (Brown and Ploskina 2001).

Federal investigation and prosecution

No one federal agency has primary jurisdiction over identity theft, and several agencies undertake identity theft-related investigations such as the FBI, Secret Service, PIS[114], INS, and SSA.[115] However, the investigations conducted by each agency are generally related to their overall mission. The Secret Service, for example, has primary jurisdiction for investigations of credit card fraud, but have planned to minimize their future involvement in fraud related cases[116]. The SSA investigates cases of Social Security Number misuse and program fraud. What these agency cases have in common, however, is that identity theft is a secondary though frequent element[117] of their primary investigations; and the number of investigations completed by these agencies has

[113] See May (2002) for a discussion of this problem. Also see May (2002) and Welborn (2003c) for a discussion of TRW, Inc. v. Andrews 122 S.Ct. 441, 447 (2001), in which the Supreme Court declined to apply the exclusionary rule to cases of identity theft where victims attempt to sue credit issuers or bureaus. The ruling in this case upheld a two-year statute of limitation on suits filed under the Fair Credit Reporting Act, although some legislative revisions were later passed.

[114] The PIS specifically indicated that it has increased its focus on identity theft-related crime in recent years (GAO 2002c).

[115] Also see Oler (2003) for a discussion of identity theft prosecutions in the Air Force.

[116] The FBI also intends to restructure itself in order to accommodate an anti-terrorism unit. These plans for reorganization have been criticized on the grounds that the agency could potentially lose informants – a valuable source of investigative leads -- and place the responsibility for investigating crimes such as identity theft on state and local agencies, with less assistance from the FBI (Johnson 2002).

[117] The occurrence of identity theft as an element in federal investigations is currently unknown, although it appears to be pervasive: all federal agencies that reported to the GAO commented upon the frequency of identity theft as an element in their respective investigations. For example, an analysis of suspicious activity reports (SARs) conducted by the Financial Crimes Enforcement Network noted that in 1997, the first full year of required SAR reporting by financial institutions, fewer than four cases of identity theft per month were reported; the average monthly reporting rate by 2000 was 56 (GAO 2002c). According to the IRS, many but not all questionable refund schemes involve an element of identity theft or identity fraud (GAO 1998). The Secret Service noted that the vast majority of financial crimes involve the use of some sort of false identification, the use of another's personal or financial information, or the assumption of a false or fictitious identity (GAO 2002c). The use of Social Security Numbers to "breed" other identification documentation, in addition to the value and use of the number itself, is widely acknowledged by federal authorities (see GAO 2004 for a discussion of the ways in which SSNs are obtained and used by private sector entities; and the Office of the Inspector General (1999) for a discussion of SSN misuse trends in the commission of fraud). In 1999 alone, the SSA determined that approximately 82 percent of Social Security number misuse allegations were directly related to identity theft (GAO 2002a). The growing relationship between identity theft and common federal crimes such as terrorism, drug smuggling and organized activities has already been discussed. The potential for identity theft to occur in relation to government documents is also great considering the number of driver's licenses, passports, employment eligibility documents, social security cards and similar identification papers that exist in the U.S., and their importance for obtaining the privileges accorded to each.

generally increased over the past few years.[118] The extent of identity theft within such cases is obscured, therefore, by the fact that none of these agencies is specifically designed to investigate or prosecute identity theft, and none of them specifically records statistics on the identity theft-related elements that may be encountered.

The total number of active identity theft-related investigations by these collective agencies has not been estimated, although some information is known regarding the activities of individual agencies. For example,

- The INS. At U.S. ports of entry, the INS has intercepted over 100,000 fraudulent documents each year between 1999 and 2001. One investigation seized nearly 2 million counterfeit documents in Los Angeles during 1998, which were headed for distribution points around the country[119] (GAO 2002b). Further, the agency believes that its increased enforcement efforts along the southwest border have prompted an increased reliance on alien smugglers, which has in turn caused the alien smuggling industry to become more sophisticated, complex, organized and flexible (GAO 2002b).[120] The incidence of all types of fraud related to alien smuggling is expected to grow in the future.
- The SSA/OIG. Due to limited resources and competing priorities, relatively few allegations of Social Security misuse are investigated by the SSA/OIG. For example, in 1999, the agency investigated 12% of the allegations categorized as program fraud and 3% of the allegations categorized as Social Security number misuse. As a result, many potentially credible allegations of identity theft through Social Security number misuse are not addressed,[121] and those that are may result in successful convictions only because they are tied into white-collar or financial crimes, which may have identity theft-related elements (GAO 2002a).

Information regarding the number of identity theft cases that have resulted in prosecution varies by source and the laws under which they are charged:

- The Secret Service reports that the agency's task forces generate a number of cases that result in prosecution by state, local and federal courts. About 60% of the cases investigated by the Washington Field Office Task Force have been prosecuted by state courts (GAO 2002a).
- One senior Department of Justice official testified in 2001 that 92 cases had been prosecuted in federal courts under the Identity Theft Act.
- The Executive Office for United States Attorneys reported that out of the 568 cases filed in 1999 under 18 U.S.C. § 1028 24 had been charged with at least one

[118] See the series of GAO reports for specific agency data on the numbers of investigations undertaken.

[119] The extent of identity theft as opposed to identity fraud related to these cases is unknown.

[120] Although speculation, this industry may rely more on real as opposed to fraudulent identities, since fake identities may be easier to detect through enhanced enforcement efforts. The qualities of fraudulent and stolen identities and their counterpart identity documents should be compared.

[121] In 2001, SSA/OIG allegations began to be transferred to the Identity Theft Clearinghouse, but this database is under-utilized.

violation of subsection (a)(7)[122]; in 2000, 68 of the 775 cases filed had been charged with at least one violation of subsection (a)(7) (GAO 2002c).

- Senator Jon Kyl, who sponsored the Identity Theft Act reported that 1,350 people had been charged under the new law in 1999; 644 defendants were sentenced, 407 of whom had entered guilty pleas (Bettelheim 2000

Although any number of state and federal statutes may additionally be used to prosecute cases of identity theft,[123] one Justice Department Criminal Division official reported that federal prosecutors consider the Identity Theft Act to be a very useful statute because it provides broad jurisdiction, and may be used as a tool to prosecute other white-collar and financial offenses (GAO 2002a).

Sentencing and Corrections

According to one Assistant U.S. Attorney, "identity theft has become the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society, because offenders are seldom held accountable" (Hoar 2001:2), a fact that many offenders unfortunately realize and capitalize upon. What is generally known about the sentencing and subsequent disposal of identity theft offenders is that they receive fairly light sentences - as measured both by the number of years (if any) that they serve in prison and the location of their confinement.[124] There are no readily available statistics on the number of identity theft offenders sentenced[125], although the ten states surveyed by

[122] The amendment specifically making identity theft a crime under the Identity Theft Act was codified under subsection (a)(7) of 18 U.S.C. § 1028, but a given case may be counted under more than one of the three U.S. Code sections if a defendant was charged with multiple offenses. Whereas the actual number of cases prosecuted under the Identity Theft Act is unknown, the number of cases filed under 18 U.S.C. § 1028 between 1996 and 2000 have increased, while the number of cases filed under 18 U.S.C. § 1029 – one section used to prosecute such cases before the Identity Theft Act – show a general decrease between those years (GAO 2002a,c).

[123] Many cases of identity theft may be prosecuted under existing white-collar, financial fraud, or mail fraud statutes. For example, the GAO (2002c:33) provides a list of all FBI cases that have been prosecuted under statutes 18 U.S.C. § 1028 1029 1014 1344; 42 U.S.C. § 408; and 15 U.S.C. § 1644, which are related to various crimes such as bank fraud, credit card fraud and social security number misuse. This agency is also in the process of developing a system to track the number of identity theft cases it handles; but such a system, developed by any agency, must be able to account for all cases of identity theft - not simply cases that are prosecuted under 18 U.S.C. § 1028(a)(7). Similarly, identity theft offenders may receive a plea bargain or plead guilty to criminal charges unrelated to Section 1028 or subsection (a)(7). Record keeping systems, therefore, should reflect all potential variations to adequately reflect the number of identity theft cases investigated, prosecuted and convicted by each state and the federal government (GAO 2002c).

[124] As mentioned, identity thieves are often treated as white collar or financial crimes offenders who, when convicted, are generally sentenced to minimum-security facilities.

[125] Individual states may publish such statistics, but no comprehensive source exists. Virginia, for example, reported that in fiscal year 2001, 397 offenders had been held in jail pre-or post-trial for an offense committed under the state's Identity Fraud Law. Of these, 73 had been convicted under the statute and nearly all were for the misdemeanor, as opposed to felony, crime (Virginia Attorney General's Identity Theft Task Force 2002).

the GAO had statutes that included imprisonment for convicted offenders, which varied by state[126] up to 30 years.

Sentences under the Identity Theft Act can range as high as 15 years imprisonment and a $250,000 fine for persons who obtain anything of value over $1,000 or more during a 1-year period. A minimum offense level was also established, ensuring that even a person with no prior criminal conviction would receive between 10 and 16 months imprisonment (Rusch 2001). A 20-year statutory maximum is available if the crime facilitates certain types of drug or violent crimes, and a 25-year maximum is available for offenders who use identity theft to facilitate an act of international terrorism. Personal "costs" follow a bright-line rule, and can be handled through either an enhancement or departure to account for non-monetary harm suffered by victims (Economic Crimes Police Team 1999 – see this source for a full discussion of the sentencing guidelines associated with the Identity Theft Act).

The Identity Theft Penalty Enhancement Act, passed by the U.S. House of Representatives on June 23 2004, also created a new crime of "aggravated identity theft," which pertains to offenders who use the identity of another to commit serious federal offenses (or predicate crimes) such as immigration violation, theft of federal funds, or the improper receipt of Supplemental Security Insurance benefits or Social Security Benefits. Conviction for an act of aggravated identity theft would add an additional two years to an offender's sentence without parole, or five years without parole for those who are convicted of its use to commit a terrorist act. The bill also amends the Identity Theft Act to include prohibit the possession of personal identifying information with the requisite criminal intent.[127]

8. LEGISLATION[128]

State legislation

In 1996, Arizona was the first state to pass a law recognizing identity theft as an independent crime. Since that time, many states have followed in its footsteps, and only Colorado and the District of Columbia have yet to pass specific identity theft legislation. Nevertheless, these jurisdictions (and even those with specific legislation) address identity theft under statutes concerning various identity theft-related offenses.[129]

---

[126] In Pennsylvania, for example, an identity theft offender would have to steal approximately $100,000 to receive a one-year sentence. A felony drug case conviction involving more than 2 grams of cocaine or heroin - worth about $200 on the street – has a mandatory minimum sentence of one-year (GAO 2002a).

[127] See: www.house.gov/apps/list/press/ca29_schiff/062304IdTheft2.html; http://feinstein.senate.gov/04Releases/r-idtheft-passes.htm); see also Lormel (2002).

[128] Because identity theft may be prosecuted under a number of relevant state and federal statutes, an exhaustive discussion of this topic falls outside the scope of this review. See Appendix 1 for a list of current state identity theft statutes and examples of federal statutes used to prosecute identity theft-related cases.

[129] See Appendix 3 for more information on state identity theft legislation.

Each state's identity theft statute is also unique in terms of its wording, the types of identity theft criminalized, and its treatment of the crime as either a felony or a misdemeanor.[130] California, for example, originally defined the act of identity theft as a person "who willfully obtains personal information…of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain credit, goods, services, or medical information in the name of the person without the consent of that person." This statute was later amended to remove certain language, such as the words "without the authorization," to include cases where the victims give information willingly, but the information is later used for unlawful purposes (GAO 2002a:12-13). Texas' statute is similar but not identical. Modeled after the federal Identity Theft Act, it defines the act of identity theft as a person who "obtains, possesses, transfers, or uses identifying information of another person without the other person's consent or with intent to harm or defraud another" (GAO 2002a:14).

As a further example, whereas some states have specific provisions criminalizing criminal record identity theft, others contain open-ended language that may simply permit its prosecution.[131] However, almost all of the laws are unclear in terms of the statute of limitations on this crime and fail to address reverse criminal record identity theft, which occurs when a person is unable to obtain employment because an employer background search reveals a criminal record (Perl 2003). State statutes also vary on issues such as whether the victim can report the crime to the local police department if the theft occurred in another jurisdiction, or whether the police are required to make a report.[132]

Nevertheless, in order to understand the ways in which identity theft is prosecuted it is necessary to examine state identity theft laws. Most identity theft prosecutions take place at the state level because federal prosecutors will generally not take a case that involves small amounts of money. Potential punishments for identity thieves may also be stricter under some state laws. Some state judges have more discretion in these cases compared to federal judges who may be bound by the federal sentencing guidelines. Certain forms of identity theft simply fall under state as opposed to federal statutes (Perl 2003). However, state identity theft laws provide multi-jurisdictional benefits to all levels of law enforcement. According to Justice Department Criminal Division officials, "the various state statutes, coupled with the federal statute, provide a broader framework for

[130] Some states include both felony and misdemeanor categories of identity theft and have separate criminal and civil statutes.

[131] Criminal record identity theft occurs when an offender uses an individual's identity to commit a crime or gives another's name to authorities after being caught. California, Maryland, Nevada, New York, North Carolina, Utah, Virginia and Wyoming have statutes that address this form of identity theft directly. See Perl (2003) for a discussion of the similarities and differences among state laws regarding criminal record identity theft, including variations in their punishments and their treatment as a felony or misdemeanor.

[132] Both subtle and obvious stratification exists among state laws. California, for example, has focused a number of laws on the area of victims' rights. One such law grants consumers the ability to "freeze" their consumer report, and several states are considering or have enacted similar legislation (Florida 2002). Some states have also focused on laws controlling Social Security numbers, driver's licenses, or personal information databases where others have remained silent.

addressing identity theft, particularly when a multi-agency task force approach is used" (GAO 2002a:7).[133]

Although the effectiveness of such laws is unclear at this time, some anecdotal evidence suggests that their enactment has impacted awareness of identity theft to some degree. Some companies in California, for example, have conducted training seminars, reviewed data systems that may be subjected to new legislation (S.B. 1386[134]) and have started to consider response scenarios in the event of a security breach (Vijayan 2004). Nevertheless, policymakers and criminal justice administrators have the added responsibility of ensuring that relevant legislation is effectively enforced.[135]

Federal legislation

Aside from the Identity Theft Act, a number of relevant federal statutes and laws address problems associated with identity theft.[136] For example, at least three sections of the U.S. Code address identity fraud:18 U.S.C. § 1028 (fraud in connection with identity documents); 18 U.S.C. § 1029 (fraud in connection with access devices such as credit cards); and 42 U.S.C. § 408(a)(7) (fraud in connection with the misuse of Social Security Numbers].[137] Additional federal agency rules may also indirectly affect the crime of

[133] Also see Algoso, Blackledge and Vasavada (2004) for a discussion of how state laws help to fill federal regulatory gaps in the area of consumer financial privacy; Matejkovic and Lahey (2001) for a discussion on the inadequacies of state and federal criminal laws; and Pastrikos (2004) for a comparison of federal statutes to those in Arizona, California, New York and discussion of the most effective statutes in protecting American citizens.

[134] This law, for example, poses a legal risk to companies that do not protect personal data and requires companies to proactively notify customers of a security breach involving their personal information. However, its wording is somewhat ambiguous, which may make compliance difficult. In reaction to the new law, one company in Ohio decided that it did not make sense to protect the Social Security numbers of California residents because they were intermingled with customers from other states in their databases. Without a national scope, therefore, state laws may fall short of their intentions (Vijayan 2004; Buxbaum 2003).

[135] Although the extent of non-compliance is unclear, some evidence suggests that it exists. Federal agents, for example, used phony birth certificates and out of state licenses to obtain driver's licenses in seven states. The GAO noted failed training and flouted policies as the cause of this nation-wide failure ("Post-9/11, states…," 2003).

[136] See Appendix 3 for examples of federal statutes that have been used to prosecute identity theft cases. A number of additional federal laws also affect certain elements related to identity theft, for example: the USA Patriot Act (2001) has various provisions requiring the development of technology standards to confirm identity; the Enhanced Border Security and Visa Entry Reform Act of 2002 (2002) requires that all travel and entry documents issued by the U.S. to aliens be machine-readable, tamper-resistant and include standard biometric identifiers; the Computer Fraud and Abuse Act (1986) made it illegal to use a computer to commit a crime or cause similar damage; the Electronic Communication Privacy Act (1986) made it illegal to intercept electronic communications; and the Driver's Privacy Protection Act (1994) ended the state's habit of selling driver's license information (GAO 2002b; Slosarik 2002). See also, GAO (2004) for a discussion of federal and state laws affecting the disclosure of personal information; the U.S. Senate Majority Task Force on the Invasion of Privacy (2000) for a discussion of various privacy issues and related U.S. legislation; and Murphy (2004) for a discussion of financial privacy laws affecting the sharing of customer information.

[137] The Economic Crimes Policy Team has actually identified 180 separate federal statutes, comprised of 216 subsections, that proscribe the same conduct under 18 U.S.C. § 1028(a)(7) (a.k.a., the Identity Theft Act).

identity theft. The U.S. Postal Service now requires that anyone who rents a private mailbox at a commercial mail-receiving agency must designate the address as a private mailbox (or PMB). This rule adds an extra level of protection against identity theft since it may prompt companies to verify a "customer's" request that their address be changed to a private mailbox - a common method used by identity thieves to intercept a victim's mail ("Postal rule helps stem…" 1999).[138]

Numerous proposals for legislation also exist at both the state and federal levels.[139] The range of issues targeted by proposed legislation includes: protection of personal information and privacy, victim's rights, cyberspace law, control or elimination of Social Security Number use, and the ways in which credit card companies or private entities can do business. One of the more all encompassing proposals to date, "Total Information Awareness," would employ the most advanced technologies to create a centralized database on all American citizens. This proposed database would maintain individual dossiers with information on every type of electronic transaction from telephone bills to medical prescriptions, credit card purchases and travel plans (Mayle and Knott 2002). Whereas the need for similar centralized databases is recognized, the Big Brother connotations of this bill have caused particular concerns.[140]

Aside from what could be, however, the reality of what is has changed dramatically with the passage of the Identity Theft Law and the more recent Identity Theft Penalty Enhancement Act. These laws, however, may require further amendments as our understanding of identity theft, and the methods used to commit it, evolve.[141] A few additional laws, as they relate to identity theft, also deserve some attention.

The Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACT Act). The Fair Credit Reporting Act (FCRA) was originally passed in 1970 and amended in 1996 to provide new consumer rights regarding, among other things, the use, privacy and accuracy of credit reports. The 1996 amendments also temporarily preempted states from passing stronger consumer protection laws within a few specific areas under the Act. In 2003, the FCRA was significantly altered by new amendments

[138] Businesses, although regulated by particular federal bodies and required to operate within certain state laws, require further legislative attention. See Gerard, Hillison and Pacini (2004) for a discussion of the legal responsibilities of organizations with regard to identity theft. Some, however, may have their own self-imposed regulations or participate in some form of private ad-hoc regulatory body, but the deterrent value of operating guidelines as opposed to law is weak, particularly when following guidelines may substantially affect a company's "bottom line." As mentioned, however, companies are increasingly aware of the potential effects of their behavior and the FTC is working with many industry representatives to improve corporate practices.

[139] See Welborn (2003a,b) for an overview of proposed identity theft legislation; and Katyal (2001) for a discussion of the need for criminal law in cyberspace.

[140] It should also be noted that the passage of many bills relies not only upon partisan support but the attention it receives from interested lobbyists, notably private entities who have a stake in maintaining the status quo of their businesses operations.

[141] Gordon et al. (2004), for example, note that the current statute does not address the need to authenticate identity documents.

under the FACT Act, most significantly by permanently blocking states from passing more stringent financial privacy rules than the federal government.

Sections within Title II of the FACT Act (2003) are specifically designed to combat identity theft. Some sections, for example, protect or empower the consumer in relation to their credit and enhance identity authentication. One section directs the Secretary of the Treasury "to conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs of identity theft by providing convincing evidence of who actually performed a given financial transaction" (Gordon et al. 2004: 27). As this law is implemented (the legislation allows for a gradual roll out over a period of two years), police departments may be flooded with victims requesting that reports be taken to satisfy creditors and credit bureaus that certain charges were the result of identity theft (Major Cities Chiefs Association 2004).[142]

With the passage of the new amendments, however, "[c]onsumers are still the front line of their own defense against both credit-bureau mistakes and identity theft…[b]ut at least now they have a lot more tools to prevent ID theft and clean up after it" (quote from Edward Mierzwinski, program director at the U.S. PIRG in Black 2003). Some view the FACT Act as a victory for financial industries, whose lobbyists have pushed to make the FCRA provisions permanent. Others believe that the states could help to further protect consumers from corporate information-sharing practices (Hughes 2003). Historically, however, the credit reporting industry has used the FCRA as "both a shield and a sword in their dealings with consumers" (Florida 2002:21).

Gramm-Leach-Bliley Act (GLBA). Enacted in 1999, the GLBA directs financial institutions,143 such as banks and investment companies, to have policies, procedures and controls in place to prevent the unauthorized disclosure of customer financial information and to deter fraudulent access to such information. This Act also created an "opt-out" standard for consumers, which requires financial institutions to give consumers notice that the institution can disclose private financial information unless otherwise directed by the individual (GAO 2002c,d). However, while the Act protects citizens from the sale of personal information in the private sector, it does not address the collection or dissemination of personal information by the government; and it does not allow citizens to "opt-out" of government information-sharing or similar disclosures (Florida 2002).144

[142] For additional information, see Holt (2004) and Muris (2003); see also Lucas (2004) for a discussion of the "hidden costs" of the FACT Act to businesses.

[143] In 2002, colleges and universities were also found to fall under the umbrella of the GLBA since they collect personal information on students (notably SSNs), parents and donors. These institutions are now required to develop alternate record systems and further protect existing systems from infiltration ("Legislatures try to shore up…," 2004).

[144] Personal information has both market and practical value within public and private sectors. The effect of laws limiting the use or sale of such information, however, is unknown. The insurance industry, for example, uses personal information obtained through various sources to investigate potentially fraudulent claims; law enforcement agencies similarly use this information to investigate and prosecute financial crimes. Some proposals or existing laws, therefore, may have unintended consequences that should be examined further (GAO 1998).

Overall, "[w]hile the U.S. has several laws and regulations in effect, they tend to deal with the problem in a piecemeal fashion, rather than attacking the big picture" (Gordon et al. 2004: 28). Further, many existing and proposed laws may not resolve the problem of identity theft since they fail to validate, verify or authenticate individual identity (Gordon et al. 2004). Great strides have been made to address the problem of identity theft through federal and state legislation, but more research is clearly needed to inform the effective development of statutes and related methods of enforcement.[145]

9. PREVENTION

Reducing Opportunity

Ever since the recording of births and deaths, ever since individuals and groups lived continuously (more or less) in specific locations that came, with the invention of the postal services of various kinds, to be identified by names and numbers, individuals have acquired identities rooted in these fundamental cornerstones of modern society. The opportunity to steal these identities therefore has always been there. Thus, the question arises why has identity theft suddenly emerged within the past five years as a crime of such magnitude?

We have suggested in this paper that it has been the onset of the information society that has pushed all kinds of information to the fore, that has transformed information from the dusty file cabinets of bureaucracies (both governmental and private) into a major product of the market place. Thus, it has taken on the characteristics of other products of the market place that have traditionally been the targets of thieves. In fact, the British Crime Survey (2004) has shown a clear decline in burglary in recent years, a decline which is reasonably attributed to (1) small household items like electronic goods such as VCRs are too cheap to steal (not Valuable) and (2) those that are valuable such as TVs are too big to steal (not Removable). Instead, the targets of burglaries are credit cards and wallets which are many times more popular targets of burglars even more than the traditional target of jewelry ("The decline of the English burglary," 2004).

We suggest, therefore, that future research should focus on the opportunity structure (described in the above section) that now makes identity theft both possible and desirable to offenders. It follows that some of the major techniques that are used to prevent or reduce theft of traditional products may also apply to identities. As already noted, Newman and Clarke (2003) have demonstrated how this approach may be applied to a range of computer related crime, especially ecommerce crime. What follows is a brief outline of how the techniques of situational crime prevention may be applied to the prevention of identity theft per se. This attempt can only be tentative at this stage, since there is little or no research on the effectiveness of the techniques outlined below in preventing identity theft. However, all the basic techniques listed have been shown to

[145] One proposal for an "ideal" identity theft statute has been developed. See Pastrikos (2004). Research should also focus on the international aspects of identity theft and their related impact on identity theft legislation.

work to some degree in prevention of theft of particular products and in particular environments. These are generally reviewed in Clarke (1997). Many of the techniques are also reviewed and tested in the 17 volumes of *Crime Prevention Studies*.

A further difficulty in applying the techniques is the problem identified at the beginning of this paper: the fact that identity theft occurs in many different settings and is related to many different kinds of crimes, some of them quite specific, and may themselves be composed of specific behaviors, such as, for example, credit card fraud or mugging. Even with seemingly specific crimes such as check or card fraud, close analysis of these crimes reveals a highly complex opportunity structure and many different avenues that thieves take in carrying out those crimes (Newman 2003; Mativat and Tremblay 1997; Lacoste and Tremblay 2003). For the purposes of this literature review, therefore, the following outline of techniques can only be roughly indicative of what is possible. It should be read more as an outline of an entire program of research that is needed to establish effectiveness or refine techniques of intervention.

Techniques to reduce identity theft

Situational prevention divides up the possible techniques into five categories:

1. Increase the effort the offender must make to complete the crime
2. Increase the risks of getting caught
3. Reduce the rewards that result from the crime
4. Reduce provocations that may encourage or otherwise tempt offenders
5. Remove excuses that offenders may use to justify their crime

Table 2 summarizes the techniques as they may be applied to identity theft. While there are aspects of these five categories of techniques that clearly apply specifically to preventing identity theft, some appear much more relevant than others. Certainly the first three broad categories of increasing effort, increasing risks and reducing rewards appear most relevant. In principle, research projects could be developed to assess the effectiveness of any of the techniques outlined in Table 2. Again, however, we must emphasize that there are many different crimes involved in identity theft to which there are a wide range of techniques available. For example, wallets may be stolen from cars. The techniques to prevent such crimes may depend on a whole range of matters to do with where the car is parked, whether it is locked, whether valuables are displayed inside the car and so on, all of which have little to do directly with the identity that is stolen by way of the wallet.

TABLE 2: TECHNIQUES TO REDUCE IDENTITY THEFT

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
Target harden ▪ Tamper proof credit cards ▪ Firewalls ▪ Tamper proof ID documents ▪ Shred utility bills etc. *Control access to facilities* ▪ Lock mail boxes ▪ Card/password access to ID databases ▪ ID for mail forwarding ▪ Disallow remote access to databases ▪ Limit number of persons with access to ID databases *Deflect offenders* ▪ Require several forms of ID to obtain new ID or replacement. *Control tools/ weapons* ▪ Control sale of ID making equipment (card readers, stripers, printers) ▪ Use tracking ID tags to track location of use and who uses machine	*Extend guardianship* ▪ Close scrutiny, background checks of employees with access to ID databases *Assist natural surveillance* ▪ ATMs in well lit areas ▪ Disallow employees to take work home ▪ Support whistleblowers *Reduce anonymity* ▪ Photo, thumb print on ID documents, credit cards ▪ Require additional ID for on-line purchases ▪ Train clerks, police, officials in document authentication procedures *Utilize place managers* ▪ Reward vigilance for supervisors of employee/customer records *Strengthen formal surveillance* ▪ Retain backup files of computer usage ▪ Track keystrokes of computer users ▪ Monitor all utilization of ID databases ▪ Cameras on ATMs, at check-out counters, shipping and mailing services, ID granting agencies ▪ Background checks of employees	*Conceal targets* ▪ No social security numbers on health, school cards ▪ No credit card numbers on receipts ▪ Place ATMs so keystrokes cannot be observed or recorded ▪ Shred utility bills *Remove targets* ▪ Pre-paid cards for pay phones ▪ Smart cards that contain limited personal ID information ▪ Do not leave wallets in cars *Identify property* ▪ Guaranteed ID authentication services (e.g. Microsoft Passport) ▪ Vehicle ID licensing and parts marking *Disrupt markets* ▪ Monitor pawn shops ▪ Monitor retail returns departments ▪ Monitor deliveries to vacant houses ▪ Monitor classified ads. *Deny benefits* ▪ Swift notification of stolen credit card	*Avoid disputes* ▪ Maintain positive management-employee relations *Reduce arousal and temptation* ▪ Avoid public disclosure of security holes and patches in software ▪ Do not boast of security features in software	*Set rules* ▪ Responsible computer use policy *Post instructions in college dorms, workplace* ▪ "Respect Privacy" ▪ "Protect our customers' privacy" *Alert conscience* ▪ "Hacking hurts people" Assist compliance ▪ Provide shredders for employees

Adapted from Clarke and Eck (2004) and Clarke (2004).

The Role of Technology and the "Arms Race"

Table 2 assumes a heavy role of technology in both providing opportunities for offenders but also techniques to thwart them. As we have noted above, offenders take advantage of the opportunities afforded them by the information age. If there are weaknesses in the information systems that make the exchange of information so easy in the market place, offenders will exploit those weaknesses. Since the information systems of today are the outcome of the incessant march of technological innovation, it should come as no surprise that offenders will also take advantage of new technologies. They were very quick, for example, to see that pay-as-you-go cell phones were an excellent opportunity for theft of phones and phone services.[146] Similarly, no sooner had credit card manufacturers started to place holograms on credit cards, than counterfeiters obtained the very same machines and began to apply holograms too (Newman and Clarke 2003).

Researchers have termed this process an "arms race" echoing the language of neo-evolutionary theory (Ekblom 1999; Pease 2001). While we are a long way from linking criminological theories to neo-evolutionary theory, the reference serves to impress on us the force with which technology drives the process of innovation and adaptation in the market place. Thus, emerging technologies and old technologies serve to provide signposts as to where or how identity thieves will strike next. Three facets of the technology environment help us in assessing the promise (both positive and negative) of technologies. These are:

1. The specific technology and its design purpose. In regard to identity theft, such technologies include roughly three kinds:
    - tamper proofed plastic cards such as debit, check, credit, phone, college IDs, visas, driver's license, workplace IDs, various kinds of "smart" cards.
    - tamper proofed documents such as visas, passports, birth and death certificates, letters of credit, documents of ownership, property titles, documents of financial exchange, wills etc.
    - Firewalls and encryption software used for on-line transactions, such as online purchases by credit card; on-line voting, on-line renewal of motor vehicle registration etc.
    - RFID chips (Remote Frequency ID chips) that allow for the tracking of people and objects. These chips, rapidly evolving, make it possible to track cattle, cars, people, and products. They are already quickly being incorporated by businesses to track inventory and sales, and parents may purchase knapsacks for their children that have RFIDs embedded in them for tracking their kids at school. Prescription drugs will now be tracked with RFID chips. The possibility that credit cards, cell phones and other hot products could be embedded with such chips raises the prospect that possession of these "hot products" makes them really hot.
2. The system within which the technology is applied or works, that is the

[146] The design of mobile phones clearly contributed to their theft in the United Kingdom (Harrington and Mayhew 2002) and to their "cloning" and theft of cell phone service in the United States (Clarke, Kemper and Wyckoff 2001).

authentication procedures used to link the physical or electronic object to an individual. Procedures for authentication vary according to the technology and purpose of the ID. Most issuers of drivers' licenses have a system that requires the showing of additional documents of identification, although these vary considerably in stringency.[147] However, the purchase of items whether online or in a retail store using a credit card may receive only perfunctory authentication. As noted above, research has shown clearly that even the addition of elementary authentication requirements at checkout such as a password or photograph substantially reduces credit card fraud. A significant research project therefore might review and develop model guidelines for the authentication procedures to be followed in (a) Issuing all forms of ID and (b) In authenticating IDs at point of contact.[148] This could be followed up by development of training guidelines for all individuals whose jobs require that they check IDs. This would range across many government agencies to almost all retail purchasing.

3. The infrastructure that supports both the above, that is, the assembly of databases that contain the information that is embedded in the technologies and systems (i.e. personal information). All of the technologies and systems above depend on the collection, storage and quick access to the personal information that is linked to the IDs, whether electronic, paper or plastic. While technologies of various kinds can protect these databases, the fact that they must be accessed constantly for verification of individual IDs means that they are open to attack. However, as we have reported above, access to such databases has, with some notable exceptions, been by low tech means, by disgruntled or otherwise motivated employees who have access to the databases. Thus, the system of maintaining, accessing and preserving these data bases depends for its security in the long run on the individuals who maintain them. This is not to say that technology cannot help reduce this risk. The introduction of electronic verification of credit card accounts at point of sale, for example, eliminated one significant security risk: the checkout

[147] *Research Note:* A thorough review of the documentary requirements or other evidence (such as interviews) by document issuing agencies in the United States is urgently required. A good place to start would be with Departments of Motor Vehicles.

[148] *Research Note:* Post 9/11 there was a call for national ID cards, since many of the 9/11 terrorists had easily stolen passports and obtained false driving licenses. It can be seen that if one's ID were encapsulated in just one object, a national ID, this could make the work of the identity thief much easier, since he/she would only have to steal one object, rather than having to breed other forms of identification. However, others have argued that new technologies available for "smart cards" could in fact make a universal ID possible, since such cards may be programmed to contain different levels of security, providing access only to particular personal information depending on the specific task at hand. For example, a retail purchase may not require knowing the cardholder's date of birth, but getting a driving license would. Another argument in favor of smart cards is that they can be constructed in such a way that they can contain all the data necessary for carrying out most transactions, so that massive databases containing all cardholders' personal information are not needed (See Newman and Clarke 2003 for a review of these issues). While the introduction of national ID cards is a highly charged political issue, research nevertheless should be conducted to evaluate smart cards and to work out ways of introducing them into the marketplace along with other technologies. It should be emphasized however, that offenders will quickly overcome the embedded security designed into these cards, that this is a constantly evolving process. Thus, the authentication procedures are just as important as the technology, so research must take account of this.

clerk who previously had the discretion to decide whether or not to check the purchaser's credit card with the list of stolen card numbers. This practice made it impossible for clerks either to be negligent in checking the authenticity of the card account or to collude with purchasers.

One final issue is worth consideration. It is difficult to escape the conclusion that some businesses see the crime of identity theft as a business opportunity. The advertisements that have swamped the major TV networks over the past year have served to scare consumers into purchasing shredders, or purchasing insurance riders to their household insurance to protect them against identity theft. Some card issuers have marketed special check cards or special credit cards bearing the photograph of the cardholder. Card issuers generally do not charge customers for these special cards, but do use them as a marketing tool to break into new markets. Of the businesses involved in these various enterprises, insurance companies are probably the major players who should be engaged in any attempt to introduce improved security for identities. It is the insurance companies, after all, whose ancient business model is premised on the assumption that consumers will pay money to ensure the security of themselves and their possessions. The complex interrelationship between businesses and the opportunities afforded for crime, including identity theft, requires much further investigation.

10. CONCLUSIONS AND RECOMMENDATIONS

General observations

This comprehensive review of the literature on identity theft has revealed an enormous number of research possibilities. To date, it is clear that the research of scientific quality is that done or commissioned by the FTC. However, since it is the charge of the FTC to protect consumers, this research is necessarily directed at collecting information concerning victims and the impact of identity theft on consumers.

The information collected by the FTC also provides an indication of how the criminal justice system may be impacted by identity theft. For example, the FTC has estimated that over 9 million individuals in the U.S. were victimized by identity theft in 2003. We have seen that recent legislation may set in motion the requirement that consumers who are trying to clear their credit reports must obtain a police report to verify the theft of their identity. Does this mean that some 9 million victims will make their ways to their local police departments in the coming year requesting a police report? If they do not, police departments will be relieved of a heavy burden. But another research question will remain: if there were so many victims, why did they not report their victimization to the police?

The issue of reporting and recording identity theft by local police departments therefore emerges as a major issue in need of research. We have seen that the focus on police lack of appreciation of individual victims' suffering originated from the publicity given to some notorious cases and these cases were given credibility by the subsequent

congressional hearings and legislation that followed them. Much has been achieved in educating police about victim suffering, but it must be said that the push to focus on police response is based on anecdotal evidence and on a handful of studies that suffer from small samples and other methodological difficulties. More research therefore is needed to identify the proportion of victims who in fact really do suffer from theft of their identity in contrast to those who may simply experience a little inconvenience. While the FTC data sheds some light on this, it is based essentially on reports from consumers and victims, not on the observation of actual police behavior. The imbalance, therefore, of research that has focused on victims as against research on the actual criminal justice response to identity theft should be corrected.

But suppose the 9 million victims do inundate police departments with requests for a police response to their victimization. How would police departments cope? One doubts that they could, and certainly our report on the investigative and prosecutorial response to identity theft to date suggests that there is simply no way that 9 million cases of identity theft could be managed in a year. Indeed, with the Secret Service, multi-agency task forces, and FBI financial crimes task force combined, the numbers of cases managed per year are likely in the hundreds, not thousands. Of course, we do not know how many cases are managed by state and local investigators and prosecutors. At this level, especially those cases that fall below the thresholds of the major task forces, there is a vast "dark figure" of identity theft cases that are never recorded by police because there is no way that they can be prosecuted given the current difficulties in defining and recording the crime, as well as various cross jurisdictional issues. This is, however, speculation. Research is needed to assess whether this "dark figure" exists, and if so, its extent.

Even if such research were conducted, it would be of limited use, except to point out the many victims whose cases do not reach settlement, and leave victims frustrated and bitter. For what police or prosecution departments could cope with a massive increase in case loads from the potential 9 million victims?

The answer to this speculative question is, of course, to take steps to ensure that identity theft does not occur in the first place. A problem that is seemingly as enormous as identity theft and that is the result of the increased opportunities provided offenders by the information society as outlined in this report, suggests that police would benefit by focusing their resources more on preventive measures rather than trying to solve large numbers of small or even large cases. It is, however, unrealistic to think that police alone could tackle many of the issues needed to reduce opportunities for offenders. They need help from the many organizations that are part of the problem: credit reporting agencies, retail stores, banks, in short all organizations that issue identity documentation or that must authenticate identities in the course of their operations. Research, perhaps based on case studies, on how identity theft prevention partnerships might be forged and the role that government can play in fostering such partnerships may well be the key to reducing identity theft to manageable levels.

Specific research recommendations

Breaking down identity theft into its component parts.

As a first step we recommend that researchers should recognize the three basic stages of identity theft and design research accordingly. These stages are:

- Time 1 (T1): Time of initial offense (acquiring personal information). Personal information may or may not be acquired through an illegal act; and may or may not be obtained with the intent to commit a subsequent act of identity theft. The acquisition of personal information at T1 is the first step in a sequence leading to the commission of identity theft.
- Time 2 (T2): Identity theft. Personal information obtained at T1 may or may not be directly acquired by the offender who uses it at T2 to commit an act of identity theft. Additional crimes may or may not be committed at T2 in relation to the commission of identity theft; for example, breeding or counterfeiting of documents using the victim's personal information. Although these acts are crimes in and of themselves, the rewards of such crimes are later used at T2 to facilitate the ultimate act of "identity theft."
- Time 3 (T3): Outcomes of identity theft. This is the time of discovery and potential criminal justice involvement regarding the act of identity theft, as well as the realization of losses by the victim. For offenders, these losses can be understood as gains - both financial and non-financial depending upon the type of identity theft victimization. The processes at T2, however, may have already been repeated several times before the identity theft victimization is detected at T3. Thus, the process of "classic" identity theft, or repeated victimization, can be represented as: $(T2 – T3)x$. The processes involved with seasoned offenders, who may steal and use multiple identities, can be represented as: $(T1 – T2 – T3)x$.

Specific research suggestions

In order to identify specific research possibilities, we have found it useful to divide identity theft into a number of categories according to classic opportunity/rational choice theory. These are targets, offenders, situations, guardians, and outcomes. We also urge that to the extent possible, research should focus on specific acts of identity theft when searching for effective interventions, and to avoid lumping together the varieties of behaviors that are commonly bundled together and characterized as "identity theft." For example, separate studies should be conducted on credit card fraud, account takeover, "phishing", database theft, document breeding, etc. and each of these examined from the point of view of the three stages of ID theft described above. The following recommendations are an attempt to summarize the main areas of research we think emerge from the literature review. For even more specific suggestions we refer the reader to the research notes listed in footnotes throughout the paper.

Research focus	Research need	Benefit
Targets (individuals)	• Routine activities leading to victimization at T1. • Decisions by victims between T1 and T2 leading to further victimization • Identification of vulnerable victim populations	• Identification of behavior patterns and circumstances that may point to effective interventions
Targets (agencies and organizations)	• Extent to which agencies suffer ID theft at T1 • Extent to which individual identities in care of agencies are targeted at T1 and T2 • Routine activities of agencies that increase risk and provide opportunities to offenders at T1 and T2 • Extent to which agencies or corporations perceive themselves as victims • The extent to which agencies are victimized at T3 (e.g. unknowingly issuing breeder documents).	• Most at risk agencies identified so that preventive efforts may be focused on them. • Businesses learn that their business practices may contribute to the problem
Target (information as a "hot product")	• Assess the types of information that may be "hotter products" than others at T1 and those most useful to offenders at T2 and T3 • Identify the information systems that provide opportunities for offenders (e.g. internet) at T1, T2 and T3.	• Vulnerable points in information systems such as purchase transactions, credit card use, are identified and effective interventions devised (see Table 2 of techniques)
Offenders (individuals)	• Number and types of offences committed at T1 and T2, and extent to which T2 connects to T3. • Scripting of methods used by offenders to carry out their crimes through all three stages. • Extent to which offenders use relationship with victim (whether personal or agency) to obtain or use identities at T1 or T2. • Extent to which ID theft is "spur of the moment" (opportunistic) or planned • Extent to which identity theft is committed in conjunction with other crimes (e.g. burglary)	• Almost nothing is known about offender behavior. Current knowledge depends entirely on reports by victims and occasional investigators. This knowledge, especially detailed accounts or scripting of the steps taken to complete an offence are needed in order to devise effective interventions. • Educate police concerning occurrence of identity theft in relation to traditional crimes
Offenders (Groups)	• Evidence of organized groups at T1 and T2 is based on scant reports from a few major cases successfully prosecuted. • Interviews of offenders needed to verify these accounts of organized crime involvement. • Identify types of identity theft most often committed by organized groups	• Information will assist in preventive measures, and develop early warning signs of organized activity • Research may indicate ways to disrupt group activity and overcome any

Research focus	Research need	Benefit
	• Interviews of offenders to identify how special skills are attained and transmitted.	special techniques they use.
Situations (locations-times-guardians)	• Proximity of targets and offenders. When information is the target, it may be distant both in time and space from individual victim. Table 2 identifies many possible points of intervention requiring evaluative research. • Investigate extent to which distance between target and offender may be related to: amount of loss, time taken to discovery, successful investigation or prosecution. There is an obvious need for application of GIS techniques to identity theft because of the significant roles played by time and space. • At T1 and T2 many guardians may be identified as employees, family members, check-out clerks, software programs that protect computers. To what extent do these guardians help or hinder identity theft? • Research is needed to identify standards of authentication used by document issuing agencies, e.g. Departments of Motor Vehicles.	• Develop ways to hasten time to discovery. • Can guardians be targeted as sources of intervention and prevention? • GIS may reveal ways to improve detection of identity theft and solve the cross jurisdictional problems both for victim and criminal justice processing. • Raising standards of authentication will make it harder for offenders at T! T2 and T3.
Outcomes (costs or losses)	• The relationship between the losses or the costs of identity theft need to be understood in relation to the period of misuse (time between T2 and T3, and the number of subsequent offenses before discovery). • The time until discovery may be important for understanding the ultimate impact of losses • Losses may be suffered differently by different types of victims (i.e., financial or personal; individuals or entities; total amount of losses). • Losses by all victims (although accumulated at various stages) are technically not felt or realized until the time of discovery which makes this type of crime different from common burglaries or thefts. • The reciprocal nature of costs to individuals and businesses needs to be understood.	• Development of more reliable and valid ways for estimating the cost of identity theft to individual victims, organizations and society • Ways to reduce harm to individuals and to society may be identified.
Outcomes (discovery and reporting)	• The specific situations leading to discovery or non-discovery at either T1 or T2 are not clear, but appear be related to the specific offenders and victims involved, the types of information obtained and the types of crime committed. Initial discovery may also occur at either T1 or	• Construction of consistent guidelines and practices for defining, recording and reporting identity theft will provide more reliable and valid information from an

Research focus	Research need	Benefit
	T2. • More information is needed to understand who first discovers specific types of identity theft, the methods of discovery, the time until discovery (or time of misuse), and the potential relationships between these elements. • Patterns of reporting and/or non-reporting in relation to discovery may also be present, and may be affected by the type of victimization experienced. • The extent of false reporting by individuals and entities also requires further investigation. • Criminal justice involvement and subsequent processing are related to the ultimate time until discovery of the crime, which may be further related to the type of information obtained and any other offenses committed. For example, investigations may not be initiated or subsequently hampered due to delay in discovery; the statute of limitations related to specific crimes may have expired, which affects the ability to prosecute cases. The relationship of discovery to ultimate criminal justice involvement and processing must be better understood. • The number and types of cases and/or offenders involved in the system (and corresponding rates of attrition or retention within the system); the movement of cases throughout the system; and the costs, resources and related training or procedures necessary to process identity theft cases at various stages are unclear - the relationships among these variables also require further investigation.	offender and police reporting perspective to balance the currently lopsided data that are primarily victim driven. • Research on multiple reporting patterns may reduce victims' burden of having to visit many agencies, and reduce duplicative data collection efforts. • Crime reporting databases that are currently case oriented may be restructured to be more problem oriented, providing more flexibility in recording complex crimes such as identity theft..

REFERENCES

Abernathy, W.B. (2003). *The many ugly faces of identity theft.* Presentation at the 2003Banking Institute of the University of North Carolina School of Law's Center for Banking and Finance. http://www.treas.gov/offices/domestic-finance/financial-institution/cip/pdf/the-many-ugly-faces-of-identity-theft.pdf

Ahuja, V. (1997). *Secure commerce on the Internet*. NY: Academic Press.

Algoso, D., S. Blackledge and J. Vasavada. (2004). *Financial privacy in the States:How consumers benefit from personal information safeguards*. Sacramento, CA: CALPIRG Education Fund. http://calpirg.org/reports/financialprivacy04.pdf

Ambrose, E. (2004, April 18). "ID thefts put shredder sales on a tear." *Chicago Tribune*. http://www.chicagotribune.com/business/yourmoney/sns-yourmoney-0418shred,0,1001919.story.

Ashman, J., J.P. Franzis, C. Harris, D. Langdon, W. Simoncelli, C. Smith and S. Swol.(2002). Identity theft: Possible implications for property and casualty insurance. *CPCU Journal*, 55(10): 1-14.

Barrett, D. (2002, October 3). "Busboy admits stealing identities of America's rich and famous." Associated Press Newswires.

Beales, H. (2003, April 3). *Prepared statement of the Federal Trade Commission on identity theft, before the House Financial Services Committee*. http://www.ftc.gov/os/2003/04/bealesidthefttest.pdf

Beales, H. (2002a, March 20). *Prepared statement of the Federal Trade Commission on Identity theft: The FTC's response, before the Subcommittee on Technology, Terrorism and Government Information of the Senate Judiciary Committee*. http://www.ftc.gov/os/2002/03/idthefttest.htm

Beales, Howard. (2002b, July 18). *Prepared statement of the Federal TradeCommission on Identity theft: The impact on seniors before the Senate Special Committee on Aging*. http://www.ftc.gov/os/2002/07/020718identitytheft.htm

Benner,J., E. Mierzwinski and B. Givens. (2000, May). *Nowhere to turn: Victims speak out on identity theft*. California Public Interest Research Group and the Privacy Rights Clearinghouse. http://www.calpirg.org/consumer/privacy/idtheft2000/idtheft2000.pdf

Bettelheim, A. (2000, March 11). "Congress urged to do more to combat identity theft and ensure victims' rights." *CQ Weekly*, 58(11): 543.

Better Business Bureau. (2005, January 26). "New research shows that identity theft is more prevalent offline with paper than online." http://www.bbbonline.org/idtheft/safetyQuiz.asp

Black, J. (2003, December 11). "Your new weapon vs. ID theft." *Business Week Online*. http://yahoo.businessweek.com/technology/content/dec2003/tc20031211_2562_tc073.htm

Block, S. (2003, May 6). "More uneasy consumers purchase identity theft insurance." *USA Today*: 03b.

Borrus, A. (2003, March 31). "To catch an identity thief." *Business Week*, 3826: 91.

Boularad, G. (2004). "Foiling I.D. thieves." *State Legislatures*, 30(9): 12-15.

Brown, D. and B. Ploskina. (2001, August 13). "E-theft: Who's liable?" *Interactive Week*: 11-12.

Bury, L. (1999). "Chips Can be Good for You." *Accountancy* 123(1269): 48; Staff (1994, July 12). "Beating the Counterfeiters." *Cards International*.

Buxbaum, P.A. (2003, October 13). "Nine-digit dilemma." *Computerworld*, 37(41): 41- 42.

California Office of the Attorney General. *ID Theft Registry*. http://caag.state.ca.us/idtheft/general.htm

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

Catalano, S.M. (2004). *Criminal victimization 2003*. Washington, D.C.: Bureau of Justice Statistics.

Cheney, J.S. (2003). *Identity theft: A pernicious and costly fraud*. Discussion Paper, Payment Cards Center. Philadelphia, PA: Federal Reserve Bank of Philadelphia.

CIFAS. (n.d.). *How serious is the problem?/Deceased fraud*. http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp; http://www.cifas.org.uk/identity_fraud_deceased_fraud.asp

Clarke, R and G. Newman (Eds.). (2005b). Modifying Criminogenic Products: What Role for Government? In R. Clarke and G. Newman (Eds) *Designing out Crime from Products and Systems*, Crime Prevention Studies Vol. 18.

Clarke, R and G. Newman (Eds.). (2005c). Secured by Design: A Plan for Security Coding of Electronic Products. In R. Clarke and G. Newman (Eds) *Designing out Crime from Products and* Systems, Crime Prevention Studies Vol. 18.

Clarke, R.V., R. Kemper and L. Wyckoff. (2001). Controlling Cell Phone Fraud in the US: Lessons for the UK '*Foresight*' Prevention Initiative. *Security Journal* 14: 7-22.

Clarke, Ronald V. (1997). *Situational Crime Prevention: Successful case studies.* 2nd. Edition. NY: Harrow and Heston.

Clarke, Ronald V. (1999). *Hot Products. Understanding, Anticipating and Reducing the Demand for Stolen Goods*. Police Research Series. Paper 98. London: Home Office.

Clarke, Ronald V. (2001). *Shoplifting*. Problem Oriented Guides for Police No. 11. Washington. DC.: Department of Justice, COPS, and Center for Problem Oriented Policing. http://www.popcenter.org/Problems/problem-shoplifting.htm.

Clarke, Ronald.V. and Graeme Newman (2005a). *Designing out Crime from Products and Systems*, Crime Prevention Studies. Vol. 18. In Press.

Clough, B. and P. Mungo (1992). *Approaching Zero: Data Crime and the computer underworld.* London: Faber and Faber.

"Companies vulnerable to identity theft." (2003). *AFP Exchange* 23(4): 55.

Cornish, D. B and Ronald V. Clarke (Eds.). (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* NY: Springer-Verlag.

Davidson, P. (2003, June 17). "29 nations target cross-border Internet scams: Group sees stronger law enforcement, cooperation." *USA Today*: 01b.

Davis, K. (2004, January). Targeting kids for identity theft. *Kiplinger's Personal Finance*, 58(1): 20,22.

"The decline of the English burglary." (2004, May 27). *The Economist.*

Denning, Dorothy E. and William E. Baugh Jr. (2000). Hiding crimes in cyberspace. In Douglas Thomas and Brian Loader (Eds.), *Cybercrime.* London: Routledge.

Dugas, C. (2003, April 22). "Visa acts to calm fears of ID theft: Eligible card holders could get $15,000 in reimbursement." *USA Today*: 01b.

Economic Crimes Policy Team. (1999, December 15). Identity theft: Final report. United States Sentencing Commission. http://www.ussc.gov/identity/identity.htm

"ED debuts web site on student identity theft." (2004). *Inside School Safety*, 8(12): 8-9.

"Education department takes steps to curb identity theft among students." (2004). *Black Issues in Higher Education* 20(23): 8.

Ekblom, P. (1999). Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on Crime and Crime Prevention*, 6: 27-51.

"Equifax first to market with identity theft prevention products." (2003). *Electronic Information Report* 24(24): 5.

Federal Trade Commission. (2005). *National and state trends in fraud and identity theft, January-December 2004*. http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf

Federal Trade Commission. (2004). *National and state trends in fraud and identity theft, January-December 2003*. http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

Federal Trade Commission. (2003a). *Overview of the Identity Theft Program, October 1998-September 2003*. http://www.ftc.gov/os/2003/09/timelinereport.pdf

Federal Trade Commission. (2003b). *National and state trends in fraud and identity theft, January-December 2002*. http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf

Federal Trade Commission. (2003c). *Identity theft victim complaint data: Figures and trends, January 1-December 31 2002*. http://www.consumer.gov/idtheft/charts/CY2002OverallCharts.pdf

Federal Trade Commission. (2003d). *Identity theft: When bad things happen to your good name*. http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf

Federal Trade Commission. (2002a). *Identity theft victim complaint data: Figures and trends, January 1-December 31 2001*. http://www.consumer.gov/sentinel/images/charts/idtheft01.pdf

Federal Trade Commission. (2002b). *Identity theft complaint data: Figures and trends on identity theft – January 2001 through December 2001*. http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2001.pdf

Federal Trade Commission. (2001a). *Identity theft victim complaint data: Figures and trends on identity theft - January 2000 through December 2000*. http://www.ftc.gov/bcp/workshops/idtheft/charts-update.pdf

Federal Trade Commission. (2001b). *Identity theft complaint data: Figures and trends on identity theft, January 2000 through December 2000*. http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf

Felson, M. (1998). *Crime and Everyday Life* (Second Edition). Thousand Oaks, CA: Pine Forge Press.

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

Felson, M. and R.V. Clarke (Eds.) (1997) *Business and Crime Prevention.* Monsey, NY: Criminal Justice Press.

Fisher, D. (2003, September 8). "Group fights online ID theft." *eWeek*:22.

Foley, L. (2003a). *Fact Sheet 117: Identity theft and the deceased: Prevention and victim tips.* Identity Theft Resource Center. http://www.idtheftcenter.org/vg117.shtml

Foley, L. (2003b). *Identity theft: The aftermath 2003*. Identity Theft Resource Center. http://www.idtheftcenter.org/idaftermath.pdf

Foley, L, and C. Nelson (2003). *Fact Sheet 120: Identity theft and children.* Identity Theft Resource Center. http://www.idtheftcenter.org/vg120.shtml.

Florida, Sixteenth Statewide Grand Jury. (2002, January 10). *Statewide Grand Jury report: Identity theft in Florida.* First Interim Report of the Sixteenth Statewide Grand Jury. http://www.idtheftcenter.org/attach/FL_idtheft_gj.pdf

Gartner Inc. (2003, July 21). "Gartner says identity theft is up nearly 80 percent." *Press release.* http://www3.gartner.com/5_about/press_releases/pr21july2003a.jsp

Gayer, J. (2003). *Policing privacy: Law enforcement's response to identity theft.* California: CALPIRG Education Fund. http://www.calpirg.org/reports/policingprivacy2003.pdf

Gerard, G.J., W. Hillison and C. Pacini. (2004). Identity theft: The US legal environment and organizations' related responsibilities. *Journal of Financial Crime* 12(1): 33-43.

Givens, B. (2000a, June 1). *Identity theft: The growing problem of wrongful criminal convictions*. Presented at the SEARCH National Conference on Privacy, Technology and Criminal Justice Information, Washington D.C. http://www.privacyrights.org/ar/wcr.htm

Givens, B. (2000b, July 12). *Written testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*. http://www.privacyrights.org/ar/id_theft.htm

Gordon, G.R. and G.E. Curtis. (2000). *The growing global threat of economic cyber crime*. National Fraud Center, Inc. http://www.lexisnexis.com/rissolutions/conference/docs/cyber.pdf

Gordon, G.R., N.A. Willox, Jr., D.J. Rebovich, T.M. Regan, and J.B. Gordon. (2004). Identity fraud: A critical national and global threat. *Journal of Economic Crime* Management 2(1): 1-48.

Gottfredson, Denise (1997) "School-based Crime Prevention" in Lawrence W. Sherman, Denise Gottfredson, Doris MacKenzie, John Eck, Peter Reuter, and Shawn Bushway (Eds.), *Preventing Crime: What Works, What Doesn't, What's Promising*. A Report to the United States Congress. National Institute of Justice. http://www.ncjrs.org/works/

Graham, John (1989). *Auto Safety: Assessing America's Performance*. Dover, Mass.: Auburn House Publishing Company.

Green Sheet, The. (n.d.). "Many concerned about identity fraud." http://www.greensheet.com/PriorIssues-010201-/6.htm

Hardie, J., and B. Hobbs. (2005). Partners against Crime – the role of the corporate sector in tackling crime. In R. Clarke and G. Newman (Eds) *Designing out Crime from Products and Systems*, Crime Prevention Studies Vol. 18. In press.

Harrington, V., and P. Mayhew. (2002). *Mobile Phone Theft*. Home Office Research Study, No. 235. London: Home Office.

Harris Interactive. (2003, August). *Identity theft: New survey and trend report*. Conducted for Privacy and American Business. www.bbbonline.org/idtheft/IDTheftSrvyAug03.pdf

Higgins, M. (1998). Identity thieves. *ABA Journal* (October): 42-47.

Hoar, S.B. (2001, March). Identity theft: The crime of the new millennium. *USA Bulletin*, 49(2): 1-10. http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm

Holt, T.J. (2004). The Fair and Accurate Credit Transaction Act: New tool to fight identity theft. *Business Horizons*, 47(5): 3-6.

Home Office (2004). *The British Crime Survey*. *Patterns of crime*. http://www.homeoffice.gov.uk/rds/patterns1.html.

House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. (2004, September 22). *Identity theft: The causes, costs, consequences and potential solutions*. Hearing held by U.S. Representative Adam Putnam (R-FL).

Hughes, K. (2004). *Final report of cognitive research on the new identity theft questions for the 2004 National Crime Victimization Survey*. Studies Series (Survey Methodology #2004-02). Washington, D.C.: Statistical Research Division, U.S. Bureau of the Census. http://www.census.gov/srd/papers/pdf/ssm2004-02.pdf

Hughes, S. (2003, July 19). "Amendments expected to help financial information bill sail through house committee." *CQ Weekly*, 61(29): 1840.

Hulme, G.V. (2003, May 19). "Outfoxing I.D. thieves: Startup aims to stop fraud before it starts." *InformationWeek*, 940: 24.

IACP (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.

Johnson, W.J. (2002, May 30). "FBI plan strips protection." *USA Today*: 12a.

Joint hearing before the Subcommittee on Immigration, Border Security, and Claims and the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary House of Representatives. (2002). 107th congress, second session, June 25 2002. *Risk to homeland security from identity fraud and identity theft.* Washington, D.C.: Government Printing Office. http://www.house.gov/judiciary/80452.PDF

Joint hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services and the Subcommittee on Social Security of the Committee on Ways and Means of the U.S. House of Representatives. (2002). *Preventing identity theft by terrorists and criminals.* 107th Congress, first session, November 8 2001. U.S. Washington, D.C.: Government Printing Office. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_house_hearings&docid=f:76259.pdf

Jones, R.W. (2002). Taming the beast: An assessment of the fraud risk implications of the electronification of the U.S. payment system. *Journal of Economic Crime Management* 1(1): 1-18.

Jones, Gareth and Mike Levi (2000). The Value of Identity and the need for Authenticity. Research Paper, *Turning the Corner*: *Crime 2020*. Foresight Panel. DTI CD Annex.

Katyal, N.K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review* 149(4): 1003-1114.

Kingman, K. (2004, May). "ID theft: Volunteers help stem crime and help victims recover." *Community Links*: 11-13.

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

"Legislators try to shore up campus data security holes." (2004). *Recruitment and Retention in Higher Education*, September:5-6.

Levi, M. and Handley, J (1998a). *Prevention of Plastic Card Fraud*. Crime Prevention Unit Paper 71. London: Home Office.

Levi, M. and Handley, J (1998b). *The Prevention of Plastic and Cheque Fraud Revisited*. Home Office Research and Statistics Directorate. Home Office Research Study 182.

Levi, M.; Bissell, P. and Richardson, T (1991). *The Prevention of Cheque and Credit Card Fraud*. Crime Prevention Unit Paper No. 26.

Levy, Steven (1984). *Hackers: Heroes of the Computer Revolution.* New York: Bantam/Doubleday.

Lormel, D.M. (2002, July 9). *The identity theft penalty enhancement act.* Statement for The record before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information. http://www.fbi.gov/congress/congress02/idtheft.htm.

Lucas, P. (2004, October 1). "The FACT Act's hidden costs." *Credit Card Management* 17(7):52.

Major Cities Chiefs Association. (2004, November 4). *Draft literature review – identity theft.* Presented at focus group meeting Baltimore: Johns Hopkins Univerity.

Marx, G.T. (2001). Identity and Anonymity: Some Conceptual Distinctions and Issues for Research. In J. Caplan and J. Torpey, *Documenting Individual Identity*. Princeton University Press.

Mashaw, J.L. and D.L. Harfst (1990). *The Struggle for Auto Safety*. Cambridge, MA: Harvard University Press.

Matejkovic, J.W. and K.W. Lahey. (2001). *Financial Services Review* 10(1-4): 221-235.

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.) (2004). *Understanding and Preventing Auto Theft*. Crime Prevention Studies, Vol. 17. Monsey, N.Y.: Criminal Justice Press.

May, G. (2002). "Stop thief!" *Journal of Texas Consumer Law*, 5(3): 72-80.

Mayle, A., and A. Knott. (2002, December 17). "*Outsourcing Big Brother: Office of Total Information Awareness relies on private sector to track Americans*." The Center for Public Integrity. http://www.public-i.org/dtaweb/report.asp?ReportID=484

"Meth use linked to identity theft." (2004). *Alcoholism and Drug Abuse Weekly* 16(26):7.

Morris, R.G., II. (n.d.). *The development of an identity theft offender typology: A theoretical approach*. http://www.shsu.edu/~edu_elc/journal/research%20online/re2004/Robert.pdf

Murphy, M.M. (2004). Financial privacy laws affecting sharing of customer information among affiliated institutions. In Claudia L. Hayward (Ed.), Identity theft. N.Y.: Novinka Books.

Muris, T.J. (2003, July 10). *Prepared statement of the Federal Trade Commission on the Fair Credit Reporting Act before the Senate Committee on Banking, Housing, and Urban Affairs.* http://www.ftc.gov/os/2003/07/fcrasenatetest.htm

National White Collar Crime Center and the Federal Bureau of Investigation. (2003). *IFCC 2002 internet fraud report, January 1 2002-December 31 2002*. http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf

National White Collar Crime Center and the Federal Bureau of Investigation. (2002). *IFCC 2002 internet fraud report, January 1 2001-December 31 2001*. http://www.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf

National White Collar Crime Center and the Federal Bureau of Investigation. (n.d.). *Internet Fraud Complaint Center (IFCC): Six-month data trends report, May- November 2000*. http://www.ifccfbi.gov/strategy/6monthreport.PDF

Newman, G. (2003). *Check and Card Fraud.* Problem Oriented Guides for Police No. 21. Washington D.C.: Dept. of Justice, COPS and Center for Problem Oriented Policing. http://www.popcenter.org/Problems/problem-check-card-fraud.htm.

Newman, G. (2004a). *Identity Theft*. Problem Oriented Guides for Police No. 25. Dep. of Justice, COPS and Center for Problem Oriented Policing. http://www.popcenter.org/Problems/problem-identity_theft.htm.

Newman, G. (2004b). Car Safety and Car Security: An Historical Comparison. In Michael G. Maxfield and Ronald V. Clarke (Eds.) *Understanding and Preventing Car Theft.* Crime Prevention Studies, Volume 17. Monsey , New York: Criminal Justice Press.

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

Newton, John, Det. Chief Insp. (1994). *Organised 'Plastic' Counterfeiting*. London: Home Office.

O'Brien, T.L. (2004, October 24). "Identity theft is epidemic. Can it be stopped?" *New York Times*, Section 3: 1,4.

Office of the Inspector General. (1999, May). *Using social security numbers to commit fraud*. Management Advisory Report [A-08-99-42002]. http://www.ssa.gov/oig/ADOBEPDF/auditpdf/ad99-4~1.pdf

Oler, K. (2003). Catch me if you can: Identity theft litigation in the Air Force. *The Reporter*, 30(1): 3-7.

O'Shea, Timothy C., Keith Nicholls, Jonathan Archer, Elton Hughes and Jana Tatum (2003). *Crime Analysis In America: Findings And Recommendations.* Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services. http://www.cops.usdoj.gov/

O'Shea, Timothy C., Keith Nicholls, Jonathan Archer, Elton Hughes and Jana Tatum (2002). *Crime Analysis In America.* Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services. http://www.cops.usdoj.gov/

Pastrikos, C. (2004). Identity theft statutes: Which will protect Americans the most? *Albany Law Review*, 67(4):1137-1157.

Pease, K. (2001). *Cracking Crime through Design*. London: Design Council.

Perl, M.W. (2003). It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft. *Journal of Criminal Law and Criminology*, 94(1): 169-208.

"Post-9/11, states fail to do enough to end ID fraud." (2003, September 17). *USA Today*: 10a.

"Postal rule helps stem identity theft." (1999). *ABA Banking Journal*, 91(6): 64.

Privacy and American Business. (2003, June/July). Special double issue on identity theft. *Privacy and American Business* 10(5): 1-32. http://www.bbbonline.org/idtheft/PABIDTheft.pdf

Rinehart, T.A., A.T. Laszlo and G.O. Briscoe (2001). *The COPS Collaboration Toolkit: How to Build, Fix, and Sustain Productive Partnerships*. http://www.cops.usdoj.gov/Default.asp?Item=344

Rusch, J.J. (2001, July). *Making a federal case of identity theft: The Department of Justice's role in identity theft enforcement and prevention*. http://www.usdoj.gov/criminal/fruad/fedcase_idtheft.html

Saltzman, M. (n.d.). "Identity theft is on the rise, tough to solve." Reprinted from the *Miami Herald*. http://newid.com/story.htm

Seabright, P. (2004) *The Company of Strangers*. NJ: Princeton University Press.

Skogan, W.G., S.M. Hartnett, J. DuBois, J. Bennis, S. Kim, D. Rosenbaum, L. Graziano and C. Stephens (2004). *Policing Smarter Through IT: Learning from Chicago's Citizen and Law Enforcement Analysis and Reporting (CLEAR) System*. Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services. http://www.cops.usdoj.gov/

Slosarik, K. (2002). Identity theft: An overview of the problem. *Justice Professional* 15(4): 329-343.

Star Systems. (2002, November). *Identity theft and security concerns: 2002 consumer survey*. Conducted by Tele-Nation. http://www.star.com/pdf/STARIDTheft.pdf

Steel, J. (1995). "Combating Counterfeit Credit Cards: The Technological Challenge." *Credit World*, 83(5): 16-18.

Sullivan, B. (2005, January 26). "Study: 9.3 million ID theft victims last year, Consumers who eye accounts online are safer, authors say." http://www.msnbc.msn.com/id/6866768/

Sullivan, B. (2004, October 7). "Elaborate con wrings cash out of stolen credit cards". MSNBC. http://www.msnbc.msn.com/id/6175738

Sutton, M. (1995). Supply by theft: Does the market for stolen goods play a role in keeping crime figures high? *British Journal of Criminology*. 35(3): 400-416.

Swartz, N. (2003). "Want the CIA Director's address? Get it for $26 online." *Information Management Journal*, 37(6): 16.

Synovate. (2003). *Federal Trade Commission – Identity Theft Survey Report*. McLean, VA. http://www.ftc.gov/os/2003/09/synovatereport.pdf

Teague, D. (Jan. 7 2004). "*Authorities: Scam took Ids of deceased*." MSNBC. www.msnbc.msn.com/id/3899283

Titus, R.M. and A.R. Gover. (2001). Personal fraud: The victims and the scams. In Graham Farrell and Ken Pease (Eds.), Repeat victimization, *Crime Prevention Studies*, Vol. 12. Monsey, N.Y.: Criminal Justice Press.

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. (2004, January). *Social Security Numbers: Private sector entities routinely obtain and use SSNs, and laws limit the disclosure of this information*. Report to the Chairman, Subcommittee on Social Security, Committee on Ways and Means, House of Representatives. Washington, D.C. [GAO-04-11] http://www.gao.gov/new.items/d0411.pdf

U.S. General Accounting Office. (2002a, June). *Identity theft: Greater awareness and use of existing data are needed*. Report to the Honorable Sam Johnson, House of Representatives. Washington, D.C. [GAO-02-766] http://www.consumer.gov/idtheft/reports/gao-d02766.pdf

U.S. General Accounting Office. (2002b, June 25). *Identity fraud: Prevalence and links to alien illegal activities*. Before the Subcommittee on Crime, Terrorism and Homeland Security and the Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives. [GAO-02-830T] http://www.consumer.gov/idtheft/reports/gao-d02830t.pdf

U.S. General Accounting Office. (2002c, March). *Identity theft: Prevalence and cost appear to be growing*. Report to Congressional requesters. Washington, D.C. [GAO-02- 363] http://www.gao.gov/new.items/d02363.pdf

U.S. General Accounting Office (2002d, February 14). *Identity theft: Available data indicate growth in prevalence and cost*. Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate. [GAO-02-424T] http://www.gao.gov/new.items/d02424t.pdf

U.S. General Accounting Office. (1998a). "Identity Fraud." Report No. GGD-98-100BR. http://www.gao.gov

U.S. General Accounting Office. (1998b, May). *Identity fraud: Information on prevalence, cost, and internet impact is limited*. Briefing report to Congressional requesters. [GAO/GGD-98-100BR] http://www.gao.gov/archive/1998/gg98100b.pdf

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

U.S. Senate Majority Task Force on the Invasion of Privacy. (2000, March). *Report and recommendations*. http://www.senate.state.ny.us/Docs/nyspriv00.pdf

Vijayan, J. (2004, June 7). "One year later, California identity theft law remains low-key." *Computerworld*, 38(23): 7.

Vijayan, J. (2003, September 8). "Firms unite to fight online ID theft." *Computerworld*, 37(36): 51.

Virginia, Attorney General's Identity Theft Task Force. (2002, October 29). *The report of the Attorney General's Identity Theft Task Force*. Richmond, VA: Office of the Attorney General. http://www.oag.state.va.us/Protecting/Consumer%20Fraud/ID%20TASK%20Force/IDTHEFTFINALRPT.pdf

Welborn, A.A. (2003a). *Remedies available to victims of identity theft*. CRS Report for Congress [RL31919]. Congressional Research Service. http://www.bna.com/webwatch/identitytheft2.pdf

Welborn, A.A. (2003b). *Identity theft: An overview of proposed legislation*. CRS Report for Congress [RL31752]. Congressional Research Service.

Welborn, A.A. (2003c). *Identity theft and the Fair Credit Reporting Act: An analysis of TRW v. Andrews and current legislation*. CRS Report for Congress [RS21083]. Congressional Research Service. http://www.bna.com/webwatch/identitytheft.pdf

Weisburd, D., E. Waring and E.F. Chayet. (2001). *White-collar crime and criminal careers*. Cambridge, U.K.: Cambridge University Press.

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

Willox, N.A., Jr. and T.M. Regan. (2002). Identity fraud: Providing a solution. *Journal of Economic Crime Management* 1(1): 1-15. http://www.jecm.org/archives/02_vol1_issue1_art1.pdf

Wortley, Richard (1997). Reconsidering the role of opportunity in situational crime prevention. In Graeme Newman, Ronald V. Clarke and S. Giora Shoham (eds.). *Rational Choice and Situational Crime Prevention.* Aldershot, UK: Ashgate, pages 65-81.

APPENDIX 1
DESCRIPTIONS OF IDENTITY THEFT DATA SOURCES

COMPLAINT DATA

Federal Trade Commission, Consumer Sentinel Network.
The Consumer Sentinel Network is a centralized depository of fraud and identity theft complaints from over 100 different organizations across the U.S.[1] Both the Sentinel and the Identity Theft Clearinghouse have been discussed in depth throughout this report. However, this is the most comprehensive victim reporting database in existence, and it should be recognized that various types of reports have been published by the FTC using this data in addition to the ones used to inform the current discussion:

- Three-year trend for Sentinel complaints.
- Fraud complaint trends.
- Internet-related fraud complaint trends.
- Three-year trend for identity theft records.
- Identity theft victim age data and law enforcement contact.
- Major metropolitan areas ranking for fraud complaints.
- Major metropolitan areas ranking for identity theft complaints.
- Fraud complaint and identity theft victims by state.
- Detailed state trends.
- Sentinel top complaint categories.
- Sentinel top complaint categories - Three-year trends.
- How identity theft victims' information is misused. How IDT victims' information is misused - Three-year trends.
- How IDT victims' information is misused - Three-year trends, Part 2.
- Cross-border fraud trends: January - December 2003.
- 2003 fraud trends in top 26 major metropolitan areas.
- 2003 IDT trends in top 26 major metropolitan areas.
- 2003 national and state trends in fraud and identity theft.
- 2002 national and state trends in fraud and identity theft.
- 2001 national and state trends in fraud and identity theft.
- Identity theft complaint data: Figures and trends on identity theft, January 2000 through December 2000.
- Identity theft complaint data: Figures and trends on identity theft, January 2001 through December 2001.
- Identity theft complaint data: Figures and trends on identity theft, January 2002 through December 2002.

Internet Fraud Complaint Center (IFCC) – Recently renamed the ***Internet Crime Complaint Center (IC3)***
The IC3 is a joint effort of the National White Collar Crime Center (NWC3) and the Federal Bureau of Investigation (FBI). Although this complaint center has focused on Internet fraud, despite its recent shift to focus more broadly on Internet crime, this database contains identity theft data. It is unclear, however, whether these data are received by the FTC through the FBI.[2] Nevertheless, the IC3 receives complaints not only regarding what it has defined "identity theft," but complaints regarding credit/debit card fraud; check fraud; communications fraud, which includes thefts of wireless, satellite or landline services; utility/public service fraud; insurance fraud; and

[1] Some Canadian complaint information is contained in the database. See FTC 2004 for more information regarding Sentinel contributors.

[2] Whereas the FBI is listed as a contributor to the Consumer Sentinel, neither the IC3 nor NWC3 are.

government fraud – all of which are recognized and related categories of identity theft.[3] The data is not publicly available, but published reports contain trends for topics such as monetary losses; victim and perpetrator information by state; demographic characteristics including as gender and age; and law enforcement contact. To date, there are only three IFCC reports:

(2003). IFCC 2002 Internet Fraud Report.
(2002). IFCC 2001 Internet Fraud Report.
(2000). IFCC Six-month data trends report. May-November 2000.

SURVEY/STUDY DATA

California Public Interest Research Group (CALPIRG)

CALPIRG is a statewide, non-profit public interest advocacy group – one of many state groups under the guidance of the U.S. PIRG – that conducted the first known studies of identity theft. In addition to its earliest reports co-authored with the U.S. PIRG ("Theft of Identity: The Consumer X-Files," 1996; and "Theft of Identity II: Return to the Consumer X-Files," 1997), CALPIRG partnered with Privacy Rights Clearinghouse (PRC; a non-profit advocacy, research and consumer education program located in San Diego, California) to conduct the first survey of known identity theft victims ("Nowhere to Turn: Victims Speak Out on Identity Theft"; Benner, Mierzwinski and Givens 2000). Although its sample was small (N=66) and its methodology is unknown[4], this study was the first to examine the personal costs of identity theft victimization, and its insights have not been proven false by subsequent research – at least not yet. Similarly, CALPIRG is the only source of data on law enforcement perspectives related to identity theft, but it's sample was even smaller: only 28 officers were interviewed from various jurisdictions across the country (Gayer 2003). Although the findings must be treated with caution, these studies have their own intrinsic value.

Federal Trade Commission

The FTC study recently conducted by Synovate (2003) is truly the precursor to the upcoming version of the NCVS. It is the largest randomized telephone survey of identity theft victimization to date (N=4,057), although its response rates are unknown.[5] The research, however, was conducted over 12 days spanning between March and April of 2003. Aside from the strengths and weaknesses of this survey that have already been discussed, some screening data were obtained for non-identity theft victims – currently the only known or public source of such information. Given the recent testing of identity theft questions to be included on the NCVS (Hughes 2004), it is unclear whether the FTC will conduct similar studies. Nevertheless, the full realization of the NCVS is still a few years away. In the meantime, this database holds a lot of potential and is currently under-analyzed.

Javelin Strategy & Research

This independent research company has conducted at least two studies of identity theft/identity fraud since 2003. Its most recent study, conducted in 2004, used an almost identical methodology to the FTC's 2003 study in order to update the FTC's results and examine identity theft patterns longitudinally. The reports published by Javelin, however, are copyrighted material and prohibitively expensive for individual use. Some of the Javelin findings can be viewed on the Better Business Bureau website: http://www.bbbonline.org/idtheft/safetyQuiz.asp; and a complimentary report is available for personal use from the Javelin website: http://www.javelinstrategy.com/reports/.

Gartner, Inc.

Gartner is a private technology research group, which has conducted at least two studies of identity theft in 2002 and 2003. Information regarding these studies is not freely available, although several reports can be purchased directly from the company. Some of their findings have been widely cited in the popular press, but almost nothing is known

[3] During 2002, for example, the IFCC (2003) reported that 1% of its referred complaints were related to "identity theft." An additional 11.6% were for credit/debit card fraud alone, although all of these cases may not contain identity theft-related elements.

[4] This research was admittedly preliminary; however, aside from the fact that those individuals surveyed were victims who had reported to either CALPIRG or PRC, no methodological information is reported.

[5] The population estimate used by Synovate was based on the U.S. population aged 18 and older as of July 1 2002, and was obtained from the U.S. Census (215.47 million).

about their methodologies. Everything that is known, in fact, is about the more recent 2003 study; but what is known or rather what is not known is cause for concern. The May 2003 survey was conducted by mail with a sample of 2,445 households. Based on its finding that 7 million U.S. adults were the victims of identity theft, it was estimated (though not reported) that their calculations were based on a population of 205.8 million U.S. adults. The population estimate used by Synovate contained almost 10 million additional adults. Further, the exact definition of "identity theft" used by the survey is unclear. Given that it is one of the largest victimization studies to date, however, further examination of their data or their findings may prove fruitful in some respects.

Harris Interactive (for Privacy and American Business [P&AB]).
To date, Harris Interactive has conducted two studies on behalf of P&AB, which is a project of the Center for Social and Legal Research, a non-profit, non-partisan public policy think tank. It's 2003 study is the second largest victimization survey conducted to date. Nevertheless, the information that is known about it raises some concerns. In particular, the 2003 survey was conducted online and uses a total U.S. population estimate (not just an online population estimate) which is still about 5 million individuals short of the one used by Synovate for roughly the same time frame. However, the actual population estimate used was not reported. Aside from its findings, the only other information that is known is that it was conducted with a sample of 3,462 adults aged 18 and older, representing about 140 million online users. An additional study conducted in 2002 with 2,244 adults raises similar methodological concerns. Three additional studies were also conducted for P&AB by Opinion Research Corporation in 1998 1999 and 2001. [6] However, because all five surveys used differing definitions of "identity theft," their results are not comparable.

Identity Theft Resource Center (ITRC)
The ITRC is a nonprofit organization dedicated completely to the issue of identity theft. Aside from being one of the best sources for identity theft information, ITRC has recently completed a survey of known victims similar to that of CALPIRG/PRC . Its online study (Identity theft: The aftermath 2003; Foley 2003b) was conducted with 169 victims who had contacted ITRC between September of 2001 and July of 2003. Although its sample is certainly larger than "Nowhere to Turn," its response rate was about 12%. Nevertheless, this study, like its counterpart, has intrinsic value.

Identity Theft University-Business Partnership at Michigan State University
(http://www.cj.msu.edu/~outreach/identity/research.html) There are no known published reports, although several projects are currently underway and some may have already been completed:

- Identity theft: People, process and property risk assessments
- The psychology of identity theft: A predication model
- Identity theft: Legislation and criminal justice controls
- The evolution of identity theft: A review of biological, environmental, and technological determinants
- The sociology of identity theft: A "network" analysis
- **Victimization: The effects of ID theft (survey; N=70 victims)*
- Social policy and identity theft: The SS# dilemma

Given the importance of examining such topics, the Partnership may yet become a valuable source of information and data.

Star Systems
Star Systems is a private company, which markets various types of electronic payment services and technologies. Their survey, which was conducted by Tele-Nation in November of 2002, was completed by 2,000 respondents. A second phase of this survey, also completed in November of 2002, asked an additional 1,000 respondents about their perceptions regarding both their personal and private financial safety before and after September 11th. Overall, that study concluded that the heightened awareness of physical and privacy concerns caused by these events had not subsided. While its results are limited, the population estimate used was based on the 2000 Census (214.5 million estimated, not reported by Star Systems), which is much closer to that used by Synovate.

[6] The 2001 study was conducted as part of a larger survey for SEARCH and the U.S. Bureau of Statistics, although no further information is available.

APPENDIX 2
SUMMARY OF FTC CONSUMER SENTINEL/IDENTITY THEFT CLEARINGHOUSE DATA [a*]

	2000 [b, i]	**2001** [c, g]	**2002** [d, g]	**2003** [e, g]	**2004** [f, g]
Total # of requests for identity theft information	13,677[d**]	31,042 31,011[d] 30,992[e]	56,895 56,838[e] 56,779[f]	108,706 108,538[f]	76,926
Total # of complaints	31,103 31,117[d]	86,168 86,198[d] 86,212[e]	161,819 161,836[e] 161,896[f]	214,905 215,093[f]	246,570
% of all complaints related to identity theft received by Consumer Sentinel that year	22%[d]	39%[d, e]	43%; 40%[e]	42%	39%
% of victims reporting more than one type of identity theft		20%	22%	19%	19%
% of complaints for credit card fraud:		42% (36,190)	42% (67,963); 41%[f]	33% (70,918); 32%[f]	28% (69,039)
% new accounts		26% (22,403)	24.4% (39,483); 24.4%[f]	19.2% (41,216); 19.3%[f]	16.5% (40,684)
% existing accounts		10.2% (8,789)	12.1% (19,580); 12.2%[f]	12% (25,788); 12%[f]	11.9% (29,341)
% unspecified		5.6% (4,825)	5.4% (8,738); 5.4%[f]	1.4% (3,008); 1.4%[f]	0.1% (246)
% of complaints for phone or utilities fraud:		20% (17,233)	22% (35,600); 20%[f]	21% (45,130); 19%[f]	19% (46,848)
% new wireless		9.7% (8,358)	10.5% (16,990); 10.6%[f]	10.4% (22,350); 10.4%[f]	10% (24,657)
% new telephone		5.3% (4,566)	5.2% (8,414); 5.2%[f]	5.6% (12,034); 5.6%[f]	5.9% (14,547)
% new utilities		2.4% (2,068)	3% (4,854); 3%[f]	3.8% (8,166); 3.8%[f]	4.2% (10,355)
% unauthorized charges/existing acct.		0.5% (430)	0.7% (1,132); 0.7%[f]	0.6% (1,289); 0.6%[f]	0.7% (325)
% unspecified		2.3% (1,981)	2.2% (3,560); 2.2%[f]	0.8% (1,719); 0.8%[f]	0.3% (739)
% of complaints for bank fraud [j]		13% (11,201)	17% (27,509); 16%[f]	17% (36,533); 17%[f]	18% (44,382)
% existing accounts		6.2% (5,342)	8.1% (13,107); 8.1%[f]	8.2% (17,622); 8.3%f	8.5% (20,958)
% electronic fund transfer		1.9% (1,637)	3.1% (5,016); 3.1%[f]	4.8% (10,315); 4.8%[f]	6.6% (16,273)
% new accounts		2.7% (2,326)	3.7% (5,987); 3.7%[f]	3.8% (8,166); 3.8%[f]	3.6% (8,876)
% unspecified		2.3% (1,981)	2% (3,236); 2%[f]	0.5% (1,074); 0.5%[f]	0.1% (246)
% of complaints for employment-related fraud		9% (7,755)	9.3% (15,049); 9%[f]	11.1% (23,854); 11%[f]	13% (32,054)
% of complaints for government documents or benefits fraud:		6% (5,170)	8% (12,945); 7%[f]	8% (17,192); 8%[f]	8% (19,725)
% fraudulent tax return		1.9% (1,637)	1.9% (3,074); 1.9%[f]	3.7% (7,951); 3.7%[f]	3.8% (9,369)
% driver's license issued/forged		2.7% (2,326)	3% (4,854); 3%[f]	2.3% (4,942); 2.3%[f]	2.2% (5,424)
% govt. benefits applied/received		0.4% (344)	0.8% (1,294); 0.8%[f]	1.3% (2,793); 1.3%[f]	1.4% (3,451)
% Social Security Card issued/forged		0.7% (603)	1.7% (2,750); 1.7%[f]	0.4% (859); 0.4%[f]	0.5% (1,232)
% other documents issued/forged		0.3% (258)	0.3% (485); 0.3%[f]	0.4% (859); 0.4%[f]	0.7% (1,725)

% unspecified		0.2%	(172)	0.1%	(161);	0.1%[f]	<0.1%	(<214);	<0.1[f]	<0.1%	(246)
% of complaints for loan fraud:		7%	(6,031)	6%	(9,709);	6%[f]	6%	(12,894);	5%[f]	5%	(12,328)
% business/personal/student loan		3.4%[h]	(2,929)	2.6%[h]	(4,207);	2.7%[f]	2.3%	(4,942);	2.3%[f]	2.6%	(6,410)
% auto loan/lease		1.8%	(1,551)	2.1%	(3,398);	2.1%[f]	2%	(4,298);	2%[f]	1.9%	(4,684)
% real estate loan		0.7%	(603)	0.9%	(1,456);	0.9%[f]	1%	(2,149);	1%[f]	1.2%	(2,958)
% unspecified		0.6%	(517)	0.5%	(809);	0.5%[f]	0.3%	(644);	0.3%[f]	0.2%	(493)
% other identity theft fraud:		19%	(16,371)	16%	(25,891);	15%[f]	19%	(40,831);	19%[f]	22%	(54,245)
% other		12.9%	(11,115)	9.1%	(14,725);	9.1%[f]	11.6%	(24,928);	11.6%[f]	14.3%	(35,259)
% illegal/criminal		1.7%	(1,464)	2%	(3,626);	2%[f]	2.1%	(4,513);	2.1%[f]	2.4%	(5,917)
% medical		1.6%	(1,378)	1.7%	(2,750);	1.7%[f]	1.8%	(3,868);	1.8%[f]	1.8%	(4,438)
% Internet/e-mail		1%	(861)	1.4%	(2,265);	1.4%[f]	1.7%	(3,653);	1.6%[f]	1.8%	(4,438)
% apartment/house rented		0.9%	(775)	1%	(1,618);	1%[f]	0.9%	(1,934);	0.9%[f]	0.9%	(2,219)
% bankruptcy		0.4%	(344)	0.4%	(647);	0.4%[f]	0.3%	(644);	0.3%[f]	0.3%	(739)
% insurance		not reported***		not reported***			0.3%	(644);	0.3%[f]	0.4%	(986)
% property rental fraud		not reported***		not reported***			0.2%	(429);	0.2%[f]	0.3%	(739)
% child support		not reported***		not reported***			0.2%	(429);	0.2%[f]	0.3%	(739)
% securities/other investments		0.2%	(172)	0.2%	(323);	0.2%[f]	0.2%	(429);	0.2%[f]	0.1%	(246)
% magazines		not reported***		not reported***			0.1%	(214);	0.1%[f]	0.2%	(493)
% attempted identity theft		10%	(8,616)	8.3%	(13,430);	8%[f]	8%	(17,192);	8%[f]	6%	(14,794)

a. The Consumer Sentinel Network regularly receives new data, which can include information from previous time periods. Thus, new FTC reports often present figures that are different from those reported during previous years. All figures in the columns represent reported rates for the given year, since subsequent reports do not include disaggregated totals. Updated estimates are also noted.
b. Source: FTC (2001a,b). Data for 2000 were obtained from the FTC (2001a,b), unless otherwise noted.
c. Source: FTC (2002a,b). Data for 2001 were obtained from the FTC (2002a,b), unless otherwise noted.
d. Source: FTC (2003b). Data for 2002 were obtained from the FTC (2003b), unless otherwise noted.
e. Source: FTC (2004). Data for 2003 were obtained from the FTC (2004), unless otherwise noted.
f. Source: FTC (2005). Updated figures from previous years were calculated by the FTC using the following calendar year (CY) totals: CY 2002 = 161,896; CY 2003 = 215,093; CY 2004 = 246,570.
g. Whole numbers in this column were not reported by the FTC, but tallied for this table. These figures were calculated only for the given column year - that is, they were not recalculated based on subsequent reporting - and these figures were not rounded. Percentages also add to more than 100 because a number of victims reported experiencing more than one type of identity theft.
h. This figure, as it was reported, does not specify student loans.
i. Data for 2000 were not reported in percentages by category and subcategory as they were in later years. These data were presented in a graph (FTC 2001a), but the actual percentages or whole numbers of victims reporting were not tallied for this table based on a lack of information. The graph, however, depicts rates of reporting by category and subcategory that are roughly comparable to those reported for later years.
j. FTC (2005) notes that the overall category of "Bank Fraud" includes fraud involving checking and savings accounts and electronic fund transfers.

* A similar summary table appears in Appendix E of FTC (2004) for the years 2001-2004.
** The FTC, in its earliest reports, did not present the actual number of complaints received in 2000. One report does note that 31% of its identity theft contacts in 2000 were requests for information (FTC 2001b), but the total number of calls was not provided. The number that was reported in 2003(b) may reflect higher totals than were originally recorded in 2000.
*** Not reported by the FTC. These subcategories were added by the FTC in Calendar Year 2003, which may indicate that no complaints were received for these categories in 2001 or 2002, or that complaints for these categories were tallied under different categories during these years.

APPENDIX 3
SUMMARY OF FEDERAL IDENTITY THEFT-RELATED STATUTES AND STATE IDENTITY THEFT LAWS

FEDERAL IDENTITY THEFT-RELATED STATUTES

Statute	Description
18 U.S.C. § 1028	Identification fraud; Under section 1028, title 18 of the U.S. Code, it is a criminal offense (punishable by up to 15 years in prison, or a fine, or both) to, among other things, knowingly possess with intent to use unlawfully or transfer unlawfully five or more identification documents or false identification documents.
18 U.S.C. § 1029	Credit card fraud; Under section 1029, title 18 of the U.S. Code, it is a criminal offense (punishable by up to 15 years in prison, or a fine, or both) to, among other things, knowingly and with intent to defraud, traffic in or use one or more unauthorized access devices (such as credit cards) during any 1-year period and by such conduct obtain anything of value aggregating $1,000 or more during that period.
26 U.S.C. § 7206	Tax fraud
18 U.S.C. § 1030	Computer fraud
18 U.S.C. § 1344	Financial institution fraud
18 U.S.C. § 1343	Fraud by wire, mail or television
18 U.S.C. § 1342	Fictitious name or address
18 U.S.C. § 1341	Mail fraud and swindles
18 U.S.C. § 1708	Mail theft
18 U.S.C. §§ 1001,1030,1015,1035	False statements
18 U.S.C. § 287	False, fictitious or fraudulent claims
8 U.S.C. §§ 1160,1325; 18 U.S.C. §§ 911,1542 1546	Immigration/nationality
21 U.S.C. § 843; 26 U.S.C. § 5603; 18 U.S.C. § 922(a)(6)	Drug, alcohol, and gun control statutes
42 U.S.C. § 408	Use and control of Social Security data; Under section 408(a)(7), title 42 of the U.S. Code, a penalty for up to 5 years in prison, or a fine, or both, can result from, among other things, falsely representing-with intent to deceive-a number as the Social Security account number assigned by the Commissioner of Social Security to him or to another person.

Sources: U.S. GAO 1998; Economic Crimes Policy Team 1999; Hoar 2001.

Note: This table lists only a few examples of relevant federal statutes that can be used to prosecute identity theft cases, aside from revisions made to 18 U.S.C. § 1028 under the Identity Theft Act. In its review, the Economic Crimes Policy Team identified 180 separate federal statutes, comprised of 216 subsections, that proscribe the same conduct under 18 U.S.C. § 1028(a)(7). See Appendix C in their report for a full list of these statutes. The GAO (2002c:33) also provides a table of the FBI's accomplishments between 1996-2001 under various federal statutes.

STATE IDENTITY THEFT STATUTES

State	Statute	Notes
Alabama	Alabama Code § 13A-8-190 through 201	Enacted in 2001.
Alaska	Alaska Stat. § 11.46.565	Enacted in 2001.
Arizona	Ariz. Rev. Stat. § 13-2008	First state to enact identity theft legislation in 1996. Under this revised section, a person commits identity fraud by knowingly taking another person's name, birth date, or SSN without the

State	Statute	Notes
		consent of that person, with the intent of obtaining or using the person's identity for any unlawful purpose or for causing financial loss to the person. Further, under Arizona's statute, taking the identity of another person is a class 5 felony, punishable with imprisonment of 1-1/2 years, plus a fine of not more than $150,000.
Arkansas	Ark. Code Ann. § 5-37-227	Enacted in 1999.
California	Cal. Penal Code § 530.5-530.8	Enacted in 1997. This statute, which became effective January 1 1998, makes it a public offense to (1) willfully obtain the personal identifying information of another person without the authorization of that person and (2) use that information to obtain, or attempt to obtain, credit, goods, or services in the name of another person without consent of that person. Under this law, "personal identifying information" is defined as the name, address, telephone number, driver's license number, SSN, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit-card number of an individual. Conviction under section 530.5 is punishable by imprisonment in a county jail not to exceed 1 year, or a fine not to exceed $1,000, or both.
Colorado	No specific identity theft law.	An identity theft law was proposed (H.B. 1122), but died in the Colorado House Appropriations Committee in April of 2004. However, H.B. 1134 signed by governor on 6/4/04: created the Motor Vehicle Investigations Unit in the Department of Revenue to investigate and prevent the fraudulent issuance and use of driver's licenses, identification cards and other motor vehicle documents, and to assist victims of identity theft. This bill also authorizes a criminal who wrongly uses another's identity to be charged in the jurisdiction where a government agency issued identity documents and sets standards and procedures for a court to determine that a victim's identity has been mistakenly association with a crime.
Connecticut	Conn. Stat. § 53a-129a (criminal) Conn. Stat. § 52-571h (civil)	Enacted in 1999.
Delaware	11 Del Code, § 854	Enacted in 2000.
District of Columbia	No specific identity theft law.	
Florida	Fla. Stat. Ann. § 817.568	Enacted in 1999. Florida Statute § 817.568(8) allows law enforcement to investigate and prosecute identity theft cases where the only contact with their jurisdiction is the residence of the victim.
Georgia	Ga. Code Ann. § 16-9-120 through 128	Enacted in 1998.
Hawaii	HI Rev. Stat. § 708-839.6-8	
Idaho	Idaho Code § 18-3126 (criminal) Idaho Code § 28-51-102 (civil)	Enacted in 1999.
Illinois	720 Ill. Comp. Stat. 5/16G	Enacted in 1999.
Indiana	Ind. Code § 35-43-5-3.5	Enacted in 2001.
Iowa	Iowa Code § 715A.8 (criminal) Iowa Code § 714.16.B (civil)	Enacted in 1999.

State	Statute	Notes
Kansas	Kan. Stat. Ann. § 21-4018	Enacted in 1998.
Kentucky	Ky. Rev. Stat. Ann. § 514.160	Enacted in 2000.
Louisiana	La. Rev. Stat. Ann. § 14:67.16	Enacted in 1999.
Maine	ME Rev. Stat. Ann. tit. 17-A § 905-A	Enacted in 2002.
Maryland	Md. Code Ann. art. 27, § 231	Enacted in 1999.
Massachusetts	Mass. Gen. Laws ch. 266, § 37E	Enacted in 1998.
Michigan	Mich. Comp. Laws § 750.219e	Enacted in 2000.
Minnesota	Minn. Stat. § 609.527	Enacted in 1999.
Mississippi	Miss. Code Ann. § 97-19-85	Enacted in 1998. Mississippi possibly enacted the nation's first identity theft statute (Miss. Code Ann. § 97-19-85), although it was titled as a "false pretenses" statute rather than specifically labeled as an "identity theft statute." Originally enacted in 1993, the statute was amended in 1998 to include additional identifiers and increase punishment from a misdemeanor to a felony.
Missouri	Mo. Rev. Stat. § 570.223	Enacted in 1999.
Montana	Mon. Code Ann. § 45-6-332	Enacted in 2001.
Nebraska	NE Rev. Stat. § 28-609 & 620	
Nevada	Nev. Rev. State. § 205.463-465	Enacted in 1999.
New Hampshire	N.H. Rev. Stat. Ann. § 638:26	Enacted in 1999.
New Jersey	N.J. Stat. Ann. § 2C:21-17	Enacted in 1999.
New Mexico	N.M. Stat. Ann. § 30-16-24.1	Enacted in 2001.
New York	S. 694-A; NY CLS Penal § 190.77-190.84	S. 694-A was passed by the New York State Senate in 2001.
North Carolina	N.C. Gen. Stat. § 14-113.20-23	Enacted in 1999.
North Dakota	N.D. Cent. Codes § 12.1-23-11	Enacted in 1999.
Ohio	Ohio Rev. Code Ann. § 2913.49	Enacted in 1999.
Oklahoma	Okla. Stat. tit. 21, § 1533.1	Enacted in 1999.
Oregon	Or. Rev. Stat. § 165.800	Enacted in 1999.
Pennsylvania	18 Pa. Cons. Stat. § 4120	Enacted in 2000. The first offense under this statute is a misdemeanor, although identity theft may be a lesser-included offense with felony charges involving forgery and theft, given that the fact patterns of these crimes may overlap.
Rhode Island	R.I. Gen. Laws Sect. 11-49-1.1	Enacted in 2000.
South Carolina	S.C. Code Ann. § 16-13-510	Enacted in 2000.
South Dakota	S.D. Codified Laws § 22-30A-3.1	Enacted in 2000.
Tennessee	TCA §39-14-150 (criminal) TCA § 47-18-2101 (civil)	Enacted in 1999.
Texas	Tex. Penal Code § 32.51	Enacted in 1999.
Utah	Utah Code Ann. § 76-6-1101-1104	Enacted in 2000.
Virginia	Va. Code Ann. § 18.2-186.3	Enacted in 2000.

State	Statute	Notes
Vermont	Identity theft legislation recently enacted.	H.B. 327 signed by governor on 6/8/04: allows a consumer to request that a credit reporting agency place a security alert on the consumer's credit report if he consumer's identity might have been used to fraudulently obtain goods or services and to place a security freeze on the credit report if the consumer has a sworn complaint about the unlawful use of personal information. The consumer credit reporting agency would have to provide a written summary of the rights of the consumer. Establishes the crime of identity theft and penalties for violations.
Washington	Wash. Rev. Code § 9.35.020	Enacted in 1999.
West Virginia	W. Va. Code § 61-3-54	Enacted in 1998.
Wisconsin	Wis. Stat. § 943.201	Enacted in 1997.
Wyoming	Wyo. Stat. Ann. § 6-3-901	Enacted in 1999.

Sources: FTC 2003a,d; GAO 2002a 1998; Florida 2002; http://www.ncsl.org/programs/lis/privacy/idt-01legis.htm; http://www.consumer.gov/idtheft_old/statlaw.htm; http://www.senate.state.ny.us/Docs/press/press026.html; http://101-identitytheft.com; and http://www.identitytheft911.com.

Note: This table largely builds upon the FTC's efforts to maintain a current list of state identity theft statutes (http://www.consumer.gov/idtheft_old/statelaw.htm). Some additional research was completed to update missing information, and some readily available descriptions are provided for illustrative purposes, but this list is far from comprehensive. Additional information about state identity theft legislation and identity theft-related legislation can be found through the sources listed above, or through various state-sponsored websites, such as the Attorney General's.

APPENDIX 4
CASES OF IDENTITY THEFT

The Internet is a rich source of information concerning identity theft. A simple search on Google using "identity theft" is the search term returns on average 1.5 million pages (see Appendix 5 for a more detailed analysis of the web presence of identity theft). Sifting through this enormous amount of information is a major enterprise. A significant contribution to research methodology could be the development of a protocol or set of procedures for retrieving information from the Internet, and developing criteria for assessing its validity and value. The cases that follow have been taken from a Google search in which the term ""identity theft" case" was entered.

1. Exploiting weakness in technologies and information systems.

CASE 1

Philip A. Cummings, 35, of Cartersville, Georgia, who provided vast amounts of personal data to his accomplices in the identity theft scheme, told a nonplussed U.S. District Judge George B. Daniels that he "didn't know the magnification" of the crime. Prosecutors say the enormous fraud scheme victimized tens of thousands of people, with losses somewhere between $50 million and $100 million.

From the middle of 1999 through August of 2000, Cummings worked as a help-desk worker at Teledata Communications, Inc., a Long Island computer software company that gives banks computerized access to databases containing credit information. Prosecutors say Cummings sold the passwords and codes for downloading consumer credit reports to an unidentified co-conspirator.

Tens of thousands of credit reports were stolen as a result. Cummings received about $30 for each stolen report. The pilfered data was distributed to approximately 20 accomplices, who then sold it to a nationwide network of criminals.

Under the terms of a plea bargaining agreement, Cummings could be sentenced to a minimum of 14 years in federal prison on charges of conspiracy, wire fraud, and fraud in connection with identification documents, say federal prosecutors. Cummings has also agreed to forfeit any property he might have obtained as a result of his crimes.

Source: idtheft911.com: http://www.identitytheft911.com/education/articles/art20040915guilty.htm

CASE 2: Specific technology

Thieves use handheld magnetic card readers that can be bought on the Internet or improvised to glean personal information off the magnetic strip on credit and debit cards. Sometimes the data are transferred to other magnetic strips to make counterfeit credit cards. The culprits have included waiters, gas station attendants, and store clerks paid by organized-crime rings. Some private automatic-teller machines also have been rigged to skim account numbers and PINs.

Source: Consumerreports.org.
http://www.consumerreports.org/main/content/display_report.jsp?FOLDER%3C%3Efolder_id=348199

2. Financial scams

CASE 3

Knueppel also offered the theory that retired people are more vulnerable to the schemes because they're at home during the day to take the calls. He said he had recently retired from the state health department when he took a call from a telemarketer promising a low-interest credit card with a $5,000 limit.

All Knueppel had to do to get the card was give the telemarketer his bank account information so that a $189 entry fee could be deducted. Knueppel said he'd never really had credit cards, but he let his guard down with the offer because he perceived that retirement would mean money problems. And with family members in the Midwest, he wanted a credit card in case he needed to fly to see them in an emergency, he said.

"I allowed myself to listen to the spiel," he said. "I more or less dropped my defenses."

The promised credit card never came, Knueppel said, and he "just kind of wrote it off as a bad experience" until postal inspectors contacted him after finding his name on the list of a fraudulent company they'd just busted.

Schemes like the one Knueppel encountered are called "advance-fee" schemes and involve a telemarketer asking for bank account information to obtain an entry fee before a credit card is sent out.

One of the largest fraudulent telemarketing operations to be dismantled was the First Capital Consumers Group, which operated out of Toronto until charges were brought against it two years ago, said the Postal Inspection Service, which investigated First Capital along with the Federal Trade Commission.

That company targeted American consumers with poor credit histories, defrauding them of more than $8 million, Brady said.

First Capital and other fraudulent telemarketing companies often follow up their phony offers by sending customers what Brady said amounted to junk mail - not the credit cards they were promised.

Paul Schroeder, whose office was in Bel Air, was accused in a civil complaint of mailing items on behalf of First Capital and other fraudulent telemarketing companies. In August, Schroeder agreed in U.S. District Court to turn over $1.8 million in assets that will be used to make restitution to his victims, according to the Federal Trade Commission.

Source: Baltimore Sun: http://www.baltimoresun.com/news/local/bal-bz.md.fraud06oct06,1,3551697.story?coll=bal-local-headlines

CASE 4

Fake FDIC Email Phishes for Financial Info
22 September 2004

A current phishing email bearing the FDIC logo attempts to fool recipients into giving up personal identity and account information.

The email, which has the spelling-challenged subject line "Your Checking Account Alerdl" and gives the fake sender address "FDIC-Notification-Urgean@fdic.gov," includes the logo of the Federal Deposit Insurance Corporation (FDIC). The FDIC, an independent agency created by Congress in 1933, supervises banks, insures deposits up to $100,000, and has the overall objective of helping to maintain the stablity and soundness of the U.S. banking system. The FDIC does not maintain account records for holders of individual checking accounts.

Like many phishing scams, the email claims that the recipient's account information must be updated urgently "due to inactive accounts, frauds, and spoof reports." The email adds that "failure to update your records will result in Bank account deletation [SIC]." The recipient is directed to a web address, which is displayed as:

http://www.fdic.gov/fdic_intsafe/update_bankaccount.jsp

but actually takes the user to:

http://24.222.25.12/fdic/index.html

a site which, unsurprisingly, has nothing whatsoever to do with the FDIC.

If you receive this phishing email, you should not under any circumstances click on any link, go to any web address linked to, or provide any information about yourself or your accounts.

The full text of this scam email appears below:

From: FDIC-Notification-Urgean@fdic.gov
Subject: Your Checking Account Alerdl
Dear Bank Account Holders,
Federal Deposit Insurance Corporation
Due to concerns, for the safety and integrity of the FDIC community we have issued this warning message.
It has come to our attention that your account information needs to be updated due to inactive accounts, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in Bank account deletation. This notification expires on September 18th 2004.
Once you have updated your account records your Bank Account will not be interrupted and will continue as normal.
Please follow the link below and renew your account information.
http://www.fdic.gov/fdic_intsafe/update_bankaccount.jsp

Sincerely,
www.fdic.gov
Security Department.

Source: idtheft911.com: http://www.identitytheft911.com/education/alerts/alert20040922fdic.htm)

3. As Motive for other crimes

CASE 5: Theft of wallet

On Xxxx xx,2000 – my birthday – my wallet was taken at the checkout counter at Tom Thumb. Security cameras showed the checker taking my wallet, and charging nearly $500 of groceries after I left the store. Despite my calling the police, no charges were filed against the individual because he did not "steal" the wallet from my person. The wallet –containing my recently renewed Drivers License, MasterCard, ATM Card, parking card, business cards (with cellular and home numbers), and college ID card (with social security number on it) - was never recovered. The head of store security and the police detective told me that the wallet was probably thrown away.
(Source: Privacy Rights Clearninghouse)

CASE 6: Burglary:

ADAM CLYMER reports; Thousands of military personnel facing deployment for a possible war with Iraq are also confronting a threat on the home front — the risk of identity theft after burglars stole computerized records from a health care company in Phoenix last month.

The names, addresses, telephone numbers, birth dates and Social Security numbers of about 562,000 troops, dependents and retirees were on laptops and computer hard drives stolen from a nondescript building in an industrial park on Dec. 14, company officials said. Some medical claim records for people on active duty were also stolen from the company, TriWest Healthcare Alliance.

Even without the medical records, the information stolen is enough for criminals to use in creating false identities. TriWest, a Pentagon contractor handling medical claims for military personnel and dependents, warned the 562,000 customers in 16 Mountain and Western states that their identities might be stolen. It also posted a $100,000 reward.
Source: Castlecops.com, Washington, Jan. 11 2004: http://computercops.biz/article2020.html)

4. Facilitating other crimes

CASE 7

TRENTON, New Jersey: A US terrorism task force is investigating three Pakistani nationals who allegedly tried to fraudulently obtain a state identification card from a Motor Vehicle Commission agency, a newspaper reported on Tuesday.

Undercover state police officers arrested the three on Monday at a Motor Vehicle Commission office in Edison Township after observing what officials said appeared to be a “suspicious” transaction, the Home News Tribune of East Brunswick reported. The men, Mohade Aftab Khan 29, and Muhammed Ivrizwan, 42, and another whose name was not released, were each charged with forgery, tampering with public records and conspiracy.

The Joint Terrorism Task Force, consisting of both state and federal agents, stepped in after Mr Khan told investigators that he planned to travel to Pakistan and then Iraq. “We’re still trying to find out why Mr Khan wanted the card and why he would travel with it,” Lt Matthew Hartigan, a member of the state police document fraud squad, told the newspaper. “All that’s being followed up by the Joint Terrorism Task Force.”

Mr Khan, who officials said was an illegal immigrant and the person trying to obtain the New Jersey identification card, was being held on $100,000 bail at a local jail, but immigration officials have filed a request that would bar his release even if he could post bail. Mr Ivrizwan, who is in the United States legally, was also being held on $25,000 bail at the jail, but it was not known where the third man was being held. —AP
Source: Daily Times, http://www.dailytimes.com.pk/

CASE 8

The California Department of Motor Vehicles issues more than 100,000 fraudulent driver's licenses annually to criminals who use them to steal the identities of unsuspecting victims, according to internal DMV documents and interviews with agency fraud investigators. As a result, hundreds of Californians are wrongly arrested each year. Thousands more become victims of financial fraud that ruins their good credit when thieves use the driver's license to secure loans for purchases they make - but will never pay for. Sometimes, people are victimized several times. In one case 18 different individuals obtained a fraudulent duplicate license using the same victim's identity. In another case, a man secured a license using a woman's identity. And there are repeated examples of the victim and the thief having vastly different appearances - including a recent case of an African-American couple with brown hair and brown eyes impersonating a white couple with fair hair and blue eyes. An Orange County Register investigation has found that this fraud is flourishing - with the investigative caseload doubling in the past fiscal year - even as the DMV brass has actively fought to kill legislative reforms and repeatedly ignored solutions posed by their own fraud investigators.
Source: By Kimberly Kindy in The Orange County Register September 24 2000

5. Avoiding arrest

CASE:9

Tom was laid off from a high paying job in the medical industry. He had great recommendations and felt sure he would be rehired. For two years he was denied position after position after each company had done a background check. Finally Tom hired a private investigator who showed him that his criminal background included 2 DUI's and an arrest for murder. None of which belonged to him. He learned that an on-line information broker continued selling this erroneous information even after he corrected it with the Sheriff.
Source: Written testimony for the United States house of representatives committee on government reform to M. Davis, chairman (Virginia) Henry Waxman, ranking minority member (California). Investigative hearing on privacy and security with regard to peer to peer file sharing. Hearing date: May 15 2003 10:00 a.m. Room 2154 Rayburn House office building. Testimony provided by Mari J. Frank, esq.
http://www.identitytheft.org/writtentestimony.htm)

6. "Classic" Identity theft: repeat victimization.

CASE 10

On September 19, I first became aware that my identity had been stolen. I received a bill from Sears – for $675.55 of electronic purchases I did not make. I notified Sears, and put fraud alerts at the three credit reporting agencies, and ordered copies of my credit reports.

I was dumbfounded by what I discovered: over $7,000 of charges on seven credit cards, with attempts to open 6 more. Starting on September 9th, most accounts had been opened on the Internet. Despite the fraud alert, accounts are still being opened. An account was opened at Wicke's furniture store on September 22d. The suspect presented my driver's license - and, despite the fraud alert, the miswriting of my social security number, and obvious differences in the signature – was granted instant credit. Subsequently, nearly $3000 in charges were made, in 6 separate instances, over a four-day period.

I have contacted the credit card companies and stores, as soon as I become aware of them – to report the fraud and theft, to get more details of how they received credit accounts, and to request fraud affidavits and copies of the approved applications and sales receipts. All but two companies have refused to give me copies of the applications and sales receipts; most insist a police detective must call and request; one said I needed a court order or subpoena. In addition, I have gotten a new drivers license number, met with the manager at my bank, spoken with my local post office, and alerted my landlord, apartment manager, and neighbors to make note of suspicious people or cars.

Meanwhile, the crime spree using my identification continues.

Every day I wait with anxiety and dread for more phone calls and the mail to arrive. The mail brings more bills from fraudulent accounts, fraud affidavits to fill out, rejection letters from failed attempts to open credit accounts with my information, or updated credit reports with additional inquiries and accounts opened. Yet what I fear more

is what I don't receive: the suspects have used other addresses on credit applications, and there are sure to be additional accounts that I will not be aware for some time.

Each appearance on my credit reports requires a lot of time, expense, and energy to take care of.

I must get frequent copies of my credit reports from the three Credit Reporting Agencies, as new instances of theft appear on it every day.

I call the CRA to get the phone numbers of the companies, alerting the CRA of fraud.

I call the companies, where I am transferred several times and/or put on hold for extended periods of time. I give them the details of the situation (always prefaced by, "Hi, my name is R.E., and I am a victim of Identity Theft…"), request the account be closed, a fraud alert put on, and be sent a fraud affidavit to fill out. Oftentimes, I am told that it will be 3 weeks to a month before I receive it. On several occasions, I have called back a few days or a couple weeks later, to find the internal investigators have not received the information, and the request must be resubmitted.

The thieves have also written checks using my drivers license and name. I found this out recently when a check of mine was denied. I am awaiting a fraud affidavit from the check verification company. Changing my drivers license number should protect me from further check fraud, but how can I be sure they won't get away with it somewhere else? Perhaps get cellular or home phone service, take out a loan, or get a car? The detective told me to carry my police report with me at all times, in the event that I could be arrested for crimes the thieves have committed using my identification. And he still says I'm not the victim?

* * *

Not only do I have a difficult time for convincing law enforcement to admit that I'm the victim, much time is spent proving I'm not the perpetrator to the defrauding credit companies.

While Identity Theft is not a violent crime, the toll it has taken on me emotionally, financially and physiologically is beyond description, and could only be misconstrued as hyperbole. When you're repeatedly victimized, with your personal identity violated with each offense, the effect is profound.

Source: Privacy Rights Clearinghouse

7. Organized Identity theft

CASE 11

Five men — including a Navy petty officer based in Virginia — have been charged with involvement in a fraud ring that used the stolen identities of Navy officers to buy thousands of dollars worth of merchandise from stores in the Baltimore area.

U.S. Navy authorities say 27-year-old Petty Officer 3rd Class Curtis L. Phillips has been charged with violating the Uniform Code of Military Justice. Phillips is stationed on the USS George Washington, an aircraft carrier based in Norfolk, Virginia. Last July, the carrier returned to the United States after a six-month deployment to the Persian Gulf.

Between June and November of last year, authorities say, five Baltimore area men used the identities of some 20 Navy officers stationed aboard the George Washington to fraudulently obtain credit accounts at such stores as Home Depot and Target.

They have also been charged with making fraudulent use of the identities of at least five patients who had used lab testing services at Quest Diagnostics. A Quest employee was charged in April with stealing those patients' identities.

Source: http://www.identitytheft911.com/education/articles/art20040916navy.htm. 16 September 2004.

CASE 12 Organized identity theft for financial gain

Jan 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 it without delay. The only trouble was that this was not Jane Sprayberry. The driver's license had her name on it, but the photograph was not her. The imposter in no time ran up a big bill on high priced jewelry, clothing and appliances. Jane's husband, just one week before, also had his bank account emptied and credit card cloned. A coincidence? Not at all. A ring of fraudsters in Detroit had inserted themselves into employment of large business and corporations and began collecting reams of personal information: personnel records, credit records, old car rental agreements. Offenders who were eventually caught had bags and books full of such records – which they used over a period of years. They ran up an average of $18,000 in credit card charges per each victim. And they sold identities on the street for around

$25 each. It took Sprayberry and her husband more than six months to clean up the mess, and they were out $80,000 in credit card charges and bank account loss.
Source: Davis, K. (2002). "Clean up your trash: a home shredder is insurance against identity theft. Kiplinger Personal Finance Magazine. June, v.56, i6, p.102.

Primary motives of Identity theft: Financial Gain

CASE 13

Sidney, a wealthy retired executive learned that his identity was stolen many months after he and his wife purchased a new home. His loan application, with his 3 in one credit report attached, revealed his credit score, his checking, savings, and investment accounts, social security number, and all necessary information for an impostor to become Sidney. He believes his masquerader had gotten a copy of Sidney's loan application through his broker's laptop computer (which also had his downloaded credit report) and opened new credit card accounts, purchased computers, electronic equipment, furniture, rented an apartment, obtained utilities, etc, stealing almost $100,000.

Source : Written testimony for the United States house of representatives committee on government reform to M. Davis, chairman (Virginia) Henry Waxman, ranking minority member (California). Investigative hearing on privacy and security with regard to peer to peer file sharing. Hearing date: May 15 2003 10:00 a.m. Room 2154 Rayburn House office building. Testimony provided by Mari J. Frank, esq.
http://www.identitytheft.org/writtentestimony.htm)

Primary motives of Identity theft: Revenge

CASE 14

The first cyber stalking case prosecuted in Orange County, California turned out to be identity theft. A computer expert was angry when a woman he liked shunned his advances. He proceeded to go online to a chat room and pretend to be her- stating that she has fantasies of being raped. He gave out her telephone number and home address. The woman didn't even own a computer. When several men appeared at her door to share her fantasies, she was terrified and called the police.

Source: Written testimony for the United States house of representatives committee on government reform to M. Davis, chairman (Virginia) Henry Waxman, ranking minority member (California). Investigative hearing on privacy and security with regard to peer to peer file sharing. Hearing date: May 15 2003 10:00 a.m. Room 2154 Rayburn House office building. Testimony provided by Mari J. Frank, esq.
http://www.identitytheft.org/writtentestimony.htm)

APPENDIX 5
Web pages returned by Google Search on 10/8/04

Identity theft type or technique	Number of Pages	Search terms
Identity theft or fraud	1,530,000	"identity theft" OR "identity fraud".
Identity theft by hacking, electronic means	644,000	"identity theft" OR "identity fraud" AND hacker OR computer OR electronic
Check fraud	533,000	"identity theft" OR identity fraud" check
Identity theft with computer	485,000	"identity theft" OR "identity fraud" AND computer
Plastic card fraud	401,000	"credit card fraud" OR "card fraud".
Identity theft cases	353,000	“identity theft" OR "identity fraud" case OR cases
Identity theft using various scams	72,700	"identity theft" OR "identity fraud" AND "skimming OR pfishing OR scam".
Dumpster diving	46,900	"dumpster diving"
Card skimming	44,400	skimming card”
Identity theft via burglary	15,300	"identity theft" OR "identity fraud" AND burglary
Identity theft for revenge	13,000	"identity theft" OR "identity fraud" AND revenge OR "getting even".
Mail fraud	8,110	"identity theft" OR "identity fraud" "mail fraud
Identity theft via mail theft	3,090	"identity theft" OR "identity fraud" "mail theft”
Document fraud or theft	873	"identity theft" OR "identity fraud" AND "document theft" OR "document fraud".
Identity theft via pick pocketing	239	"identity theft" OR "identity fraud" AND "pickpocketing
Identity theft via theft from cars	71	"identity theft" OR "identity fraud" +"theft from cars”
Controls		
	16,100,000	“dinner”
	938,000	“burglary"