Defendants Stealing Identifying Information through Employment

Data was collected regarding the theft of personal identifying information from the defendants' places of employment. Of the 933 total defendants among the 517 cases, 20.3% (189) accessed records at their place of employment in order to perpetrate identity theft. The types of employment were categorized in the same way as the victims:

- Financial Services Industry (banks, credit unions, American Express, Discover, MasterCard, Visa)
- Retail (stores, car dealerships, gas stations, casinos, sports clubs, restaurants, hotels, hospitals, doctors' offices etc.)
- Government agency (includes federal, state, and local)
- Credit Bureau
- Insurance (life, car, property, casualty, health)
- Education (public and private, all levels)
- Unavailable (While it was stated that the defendant accessed information at work, his or her type or place of employment was not specified in the case file.)

As shown in Figure 31, of the 189 defendants who stole personal identifying information through employment, 59.7% (113) were employed in retail, such as stores, restaurants, hotels, gas stations, car dealerships, casinos, hospitals, and doctors' offices. 22.2% (42) worked in the financial services industry – banks, credit unions, and credit card companies. This is consistent with the cases in which the offenses were perpetrated by an insider – most often the retail industry, followed by private corporations. Both are consistent with the most frequent point of compromise – all businesses.

Figure 31. Type of Employment used to Steal Identities

Category	N	Percent
Retail	113	59.7%
Financial Services Industry	42	22.2%
Government Agency	9	4.8%
Education	6	3.2%
Insurance	6	3.2%
Unavailable	13	6.9%
Total	189	100%

Identity Theft through Employment: Hospital
The defendant, whose first and last name were the same as the victim's, used her position as a hospital employee to gain access to patients' personal identifiers. The victim had given birth in the hospital and the defendant accessed her identifiers, which she used to obtain several credit card accounts. The victim became aware of the unauthorized accounts when she was contacted by Discover concerning a credit card for which she had not applied. She then obtained her credit history and found other retail credit card accounts which she had not authorized.

Victimization in Summary

Ninety percent of the victims were financial services businesses, retail businesses, and individuals. The method of victimization for the financial services industry was most frequently the use of fraudulently obtained personal identifying information to open new credit card accounts. They were also often the victims of fraudulent loan applications. The retail industry was also victimized through the opening of new credit card accounts, as well as by the fraudulent purchase of merchandise that was later returned for cash or store credit. In the majority of the cases, the offender did not know his or her victim. The retail industry was found to be most susceptible to identity theft by their employees.

Recommendations

The distillation of this research study's findings provides robust empirical information on which the law enforcement community can base enhanced proactive identity theft control and prevention efforts. It is the first study of its kind to provide to law enforcement agencies and corporate security and fraud investigators empirical data concerning the key factors of identity theft behavior and the conditions under which that behavior occurs. The recommendations presented here are based on the use of the study's findings. While conjecture and conventional wisdom may have led to some of the same conclusions in the past, this study allows law enforcement and corporate security leaders and policy makers to point to the data as a basis for implementing them. These recommendations are an effort to ensure that the findings will be used to improve and increase proactive measures that law enforcement and fraud investigators use to combat identity theft. They fall into five categories:

- Proactive investigation, detection, prevention, and prosecution
- Enhanced law enforcement training
- Enhanced management of cases and resources
- Briefings for law enforcement executives so that they can develop policy, allocate resources, and advocate training based on empirical research
- Future research

Proactive Measures

The findings of this research study should result in proactive measures, including improved investigative methods and enhanced prevention and detection strategies for federal, state, and local law enforcement, as well as corporate security fraud investigators.

Recommendation 1: Local and state law enforcement leaders should encourage more cooperation with federal law enforcement where it has begun and foster it where it is not occurring.

The manner in which the criminal justice system addresses the cases from the beginning underscores the instrumental role of local law enforcement in the referral of cases to the Secret Service. The referrals may result from victim reports of identity theft to local law enforcement, but also may be the product of the alertness of local officials in recognizing telltale signs of identity theft while investigating unrelated crimes. Local police and sheriffs' departments often act as conduits to successful federal investigations and prosecutions of these cases. This trend shows a collaborative approach to investigating identity theft cases and should continue and increase. Most of the cases were prosecuted under federal jurisdiction – a further indication of the cooperative and collaborative approach.

Recommendation 2: Law enforcement at all levels should be aware of the offender characteristics and the role of identity theft in other crimes and apply that knowledge to their investigations. Law enforcement should share the information they find with corporate entities, such as the financial services industry, so that prevention and detection strategies can be enhanced.

The findings show that identity theft offenders are diverse in terms of their age, race, and gender. The women were more likely to be black and were younger than the males who were involved. Most of the offenders did not have prior arrest records, but of those who did, most were for related offenses such as fraud and theft of property. Most offenders used identity theft to facilitate crimes of fraud or theft.

Recommendation 3: The findings of this research study regarding federal and state statutes and disposition should be used as a basis on which to build policy and practice in prosecuting identity theft at all levels.

While most of the cases were prosecuted federally, the reliance on newly enacted identity theft statutes figures prominently in the charging of offenders both on the federal and state jurisdictional levels. At the state level, identity theft statutes were most frequently charged. At the federal level, access device fraud and identity fraud statutes were charged the most. Wire fraud and mail fraud, which at one time were seen as the easiest under which to prosecute identity theft offenders, were used much less frequently. Once an investigation is initiated, it can likely take up to two years for the case to reach disposition. Prosecutors at both the federal and state levels had a slightly better chance of sending a convicted identity thief to prison than not (51%), and could expect to see the imprisoned offender sentenced to three years or less of incarceration. Restitution imposed was, by and large, commensurate with the amount of loss incurred by victims in the identity theft cases.

Law Enforcement Training

The findings of this applied research bring to light several characteristics of identity theft offenders and crimes that may not have been previously known and which can contribute to continued and improved investigation and prosecution. These include the offender demographics, the methods used in the commission of the crimes, the relationships between the offenders and their victims, and organized crime group activity.

Recommendation 4: The findings should be infused into the many fine existing training programs to move beyond assumptions and anecdotes and gain a greater understanding of identity theft.

A CD with figures from this study and notes for instructors will be prepared to move this recommendation forward.

Management of Cases and Resources

The results of this study allow law enforcement to see a spectrum of identity theft cases, rather than dealing with one at a time. Law enforcement managers can use this information to assign resources and prioritize cases.

Recommendation 5: The findings of this study should be reviewed by law enforcement executives to gain a broader picture of where to focus their resources to combat identity theft.

The findings show that the actual dollar loss of the cases ranged from none to $13,000,000. The median loss was $31,356. While previous assumptions tended to point to the existence of dollar loss thresholds under which cases would not be investigated or prosecuted, the findings here show that there is value in pursing identity theft cases even if the dollar loss is minimal or non-existent. The findings regarding geographical distribution and scope, show that the identity theft cases were evenly distributed across the United States and that the scope of the offenses was evenly distributed among local, state, and interstate. In other words, identity theft cases are not more prevalent in one area of the country than another and are not limited by local or state boundaries. This information, along with that about referrals from local and state law enforcement, will help law enforcement managers effectively allocate personnel and funds.

Recommendation 6: So that law enforcement agencies at all levels can share case information, collaborate on investigations, and better prioritize and manage their cases and resources, standardized case classifications should be established. Based on the empirical findings, consideration should be given to including identity theft as a primary classification code.

As was explained earlier, the Secret Service assigns a primary classification code to its cases and one or more secondary classification codes. The most frequent primary case type was “Fraudulent Use of Account Numbers,” while the most prevalent secondary one was “Identity Fraud.” A common system of classification of identity theft cases would help in the management of cases and resources, as it would provide better measurement of the size and scope of identity theft cases and more efficient information sharing among federal, state, and local law enforcement agencies.

Executive Briefings

In addition to the law enforcement training that is recommended here and for which materials are provided, the relevant findings should be disseminated to law

enforcement executives so that they can develop policy, allocate resources, and advocate training based on empirical research.

Recommendation 7: A briefing on the research findings which will aid law enforcement executives in developing and implementing policies and procedures for investigation and prosecution of identity theft crimes should be made available.

This briefing should focus on conclusions drawn from the findings in the areas of offender methods, points of compromise, organized crime activity, insider criminal activity, and the victims.

Recommendation 8: A briefing on the research findings which will provide law enforcement executives with cutting edge information to share with corporations should be made available.

This briefing will focus on the points of compromise and vulnerabilities which provide opportunities for employees and others to steal personal identifying information, as well as the methods they use to perpetrate the theft. Corporations receiving this information will be able to use it in the development of policies and procedures to prevent, detect, and mitigate identity theft and fraud.

Future Research

This research study should be used as a model for a series of studies. The study of closed Secret Service cases from 2000-2006 resulted in a rich data set which will be used to assist law enforcement agencies and corporations in their fight against identity theft and fraud. However, criminals are continually adapting to law enforcement investigative methods by designing new methods for committing such crimes. In order to combat these crimes, law enforcement needs up-to-date information on trends, patterns, and groups, both current and emerging, to move from a reactive posture to a proactive one.

Recommendation 9: This model for research should be applied to cases held by local, state, and other federal law enforcement agencies.

Recommendation 10: Building on the baseline created through this research, further longitudinal study of Secret Service closed cases with an identity theft component should be undertaken to determine trends and patterns of the crime in the near past and to anticipate future trends and areas of vulnerability.

All of the recommendations posited here will be better served and implemented if more applied research studies, such as this one, are completed. The ultimate goal of this and future studies is increased proactive investigation, prevention, and prosecution of these crimes.

Conclusion

The media, public service announcements, and public and private sector literature concerning identity theft and prevention methods have been instrumental in educating the public about the threat and consequences of identity theft. Some characterizations have emphasized identity theft as more of a stranger-to-stranger crime. Others have underscored the importance of not falling into a level of complacency that would open the doors for friends and relatives to take advantage of the unwary victim. Still other descriptions have focused on the methods practiced, ranging from relatively simplistic acts such as “dumpster diving” and mail theft to more sophisticated criminal activities that depend upon the victim’s and offender’s use of the Internet. While provocative, much of this information is based upon surveys and reports that often leave key questions unanswered from an empirical standpoint. Not presuming that the analysis of closed case data on identity theft crimes is definitive, this study of closed Secret Service cases provides empirical evidence about identity theft in the United States from a law enforcement point of view and can be extrapolated to local and state law enforcement.

The analysis of the cases revealed that while identity theft can occur anywhere, it was concentrated in the Northeast and South. The manner in which the criminal justice system addressed the cases from the beginning underscores the instrumental role of local law enforcement in the referral of cases to the Secret Service. Local police and sheriffs’ departments often acted as conduits to successful federal investigations and prosecutions of these cases. The referrals may have resulted from victim reports of identity theft to local law enforcement, but were also the product of the alertness of local officials in recognizing telltale signs of identity theft through the investigation of other crimes entirely unrelated to identity theft. While most of the cases were, ultimately, prosecuted federally, the reliance on newly enacted identity theft statutes figured prominently in the charging of offenders both on the federal and state jurisdictional levels. Prosecutors had a slightly better chance of sending a convicted identity thief to prison than not (51%), and could expect to see the imprisoned offender sentenced to three years or less of incarceration. Restitution imposed was, by and large, commensurate with the amount of loss incurred by victims in the identity theft cases.

While some of the findings about the offenders may not be surprising, others seem to contradict the image that, in some ways, has been formed by default: that identity thieves are usually white males. The results show that identity theft is a crime that minorities are just as apt to commit as whites. The number of younger offenders, female offenders, and female black offenders in these crimes is noteworthy.

The case analysis indicates that the offenders could be separated into two groups: those who engaged in identity theft practices as isolated events as

opportunities presented themselves (i.e., in the form of criminal opportunities such as access to customer/client information through the offender's place of employment) and those who actively pursue identity theft as part of a property theft criminal career (as demonstrated by the types of crimes in the offenders' criminal histories). In these cases, the identity thefts do not happen by accident, but are planned criminal events, usually motivated by a desire for financial gain. The type and extent of planning differs according to how many offenders collaborate to commit these offenses and the degree to which they are seen by the offenders as short or long term ventures. In most cases, identity theft was shown to be the act of solitary criminals or criminals operating in fairly unsophisticated two-person teams. Incidents of organized group activity were fairly rare, but when they did occur, the acts of the offenders were more specialized and the roles assumed by the offenders were often interchangeable. In short, such cases reflected the type of organizational characteristics that mirror the activities of conventional law-abiding ventures. Leaders exercised a span of control designed to optimize the success and profits of the identity theft acts. There appeared to be a connection between the size and organizational sophistication of identity theft operations and the profits reaped.

Analysis of the methods employed by the offenders showed that Internet and/or other technological devices were used in approximately half of the cases. In some cases, the offenders began with a non-technological act, such as mail theft, to obtain the personal identifying information, but then used devices such as digital cameras, computers, scanners, laminators and cell phones to produce and distribute fraudulent documents. While the use of the Internet as a criminal tool had a presence, it did not appear to be a necessity for most offenders to reach their goals

The findings show that the financial services industry was just as likely to be victimized as an individual. The spectrum of methods used was wide, but usually originated in the fraudulent use of personal identifying information. With this information, offenders obtained new credit card accounts, changed credit card accounts opened bank accounts, transferred funds from and between bank accounts, and forged checks. Customers fell prey to identity thieves through simple business transactions conducted in stores, restaurants, hotels, service stations and automobile dealerships, as well as other retail entities. While not in the majority, both financial service and retail industries were found to be vulnerable to the theft of personal information through employee access. According to the case analysis, there was a one in three chance that the victimization was a result of the work of an insider.

The case analysis results refute some presumptions about the relationship between the offender and the victim. While there were instances in which relatives and friends proved to be the perpetrators, they were in the minority. The typical identity theft criminal took advantage of those not personally known to him or her. In terms of loses incurred by identity theft victims, the median loss was

$31,356. In general, the more offenders involved in the case, the higher the victim loss was.

This study is significant because it did not depend on self-reported or survey data. The closed Secret Services cases provided reliable information which was collected objectively and analyzed to reach conclusions. The impact of these findings will be measured by the effective application of the recommendations concerning proactive law enforcement methods, enhanced law enforcement training, management of cases and resources, policy development, and future research.

.

Appendix

Collection Template

CASE TITLE: **CASE #**

DEFENDANT(S):

	RACE	SEX	DOB	Place of Birth
D 1				
D 2				
D 3				
D 4				
D 5				

REGION:

CASE TYPE:

SECONDARY TYPES:

Code	

CROSS REFERENCED CASES:

ACTUAL LOSS:

STATUTES VIOLATED:

DATE OPENED:

DATE CLOSED:

	DISPOSITION
D 1	
D 2	
D 3	
D 4	
D 5	

Criminal Record	Arrests	Convictions
D 1		
D 2		
D 3		
D 4		
D 5		

DETAILS OF INVESTIGATION

Case Origination:

Case Notes:

Jurisdiction:

Evidence:

ROLE	D 1	D 2	D 3	D 4	D 5
Steal/obtain info					
Steal/obtain docs					
Steal/obtain bank cards					
Alter IDs					
Produce counterfeit ids					
Distribute info to others					
Sell IDS					
Use ID for own use					
Use ID to get more ID docs					
Direct others' activities					
Other					

	D 1	D 2	D 3	D 4	D 5
Non-citizen					
If non-citizen, country					
ID theft thru employment?					
Type of employment	------	------	------	------	------
Gov. Agency					
Bank/Credit Union					
Credit Bureau					
Service					
Retail					
Insurance					
Credit Card					
Education					
Private Company					
Unavailable					

Facilitation	ID Theft facilitates	Facilitates ID Theft
Homicide		
Assault		
Sexual Assault		
Burglary		
Robbery		
Larceny/Theft		
Fraud		
Drug Trafficking		
Drug Possession		
Embezzlement		
Forgery /Counterfeiting		
Weapons		
Arson		
Immigration		
Family Offense		
Traffic (not DUI/DWI)		
DUI/DWI		
Credit Card Skimming		
Telephone Scam/Solicitation		
Internet Scam/Solicitation		
Gun Running		
Human Trafficking		
Other:		

Victim-Offender Relationship	D 1	D 2	D 3	D 4	D 5
Immediate Family					
Extended Family					
Friend					
Co-worker/employer					
Acquaintance					
Customer/Client					
Stranger					
Unavailable					

Victim	
Gov. Agency	
Bank/Credit Union	
Credit Bureau	
Service	
Retail	
Insurance	
Credit Card	
Education	
Individual	
Unavailable	

Technology and Devices	
Internet	
E-mail	
Phishing	
Hacking	
419 Scam	
Malware/Viruses	
Database Searching	
Online ID purchase and/or sale	
Other	
Computers (other than Internet)	
Scanning documents	
Producing documents	
Printer	
Copier	
Typewriter	
Digital Camera	
Cell Phones	
Telephone	
Other	

Means	
Mail theft	
Rerouting of mail (change of address cards)	
Dumpster diving residential	
Dumpster diving business	
Public Records	
Geographical Scope	
Local	
Within state	
Interstate	
International	

References

Dadisho, Ed (2005, February). *Identity Theft and Police Response: Prevention*. *The Police Chief.* Retrieved May 23, 2007 from http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=510&issue_id=22005

Federal Trade Commission. *FTC Issues Annual List of Top Consumer Complaints*. Retrieved June 17, 2007 from http://www.ftc.gov/opa/2007/02/topcomplaints.shtm

The President's Identity Theft Task Force (2007, April). *Combating Identity Theft: A Strategic Plan*.

United States Secret Service. *Identity Crimes*. Retrieved May 15, 2007 from www.secretservice.gov/criminal.shtml