

Identity Fraud Trends and Patterns:

Building a Data-Based Foundation for Proactive Enforcement

October 2007

**Gary R. Gordon, Ed.D.
Donald J. Rebovich, Ph.D.
Kyung-Seok Choo, Ph.D.
Judith B. Gordon, MLS**

**Center for Identity Management and Information Protection
Utica College**



*U.S. Department of
Homeland Security*
**United States
Secret Service**

This project was supported by Grant No. 2006-DD-BX-K086 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United State Department of Justice.

© 2007 Center for Identity Management and Information Protection

Acknowledgements

Several organizations and individuals were instrumental in this project. The authors extend their thanks to the Bureau of Justice Assistance for providing funding, guidance, and direction. The United States Secret Service allowed the authors access to data and space in which to work. Their cooperation, guidance, and support were crucial to the success of this endeavor; the authors owe them a debt of gratitude. Special thanks go to the Criminal Investigative Division staff, as they graciously escorted the authors in and out of the building countless times. The administration of Utica College provided support and grant management. Several Utica College undergraduates worked tirelessly to input the data into the statistical analysis software.

About CIMIP

The Center for Identity Management and Information Protection at Utica College is a research collaborative dedicated to furthering a national research agenda on identity management, information sharing, and data protection. Founded in June 2006, its ultimate goal is to impact policy, regulation, and legislation, working toward a more secure homeland. CIMIP's partners, LexisNexis, IBM, TransUnion, United States Secret Service, United States Marshal Service, Federal Bureau of Investigation, Utica College, Carnegie Mellon University, Indiana University, and Syracuse University, are committed to working together to provide resources, gather subject matter experts, provide access to sensitive data, and produce results that will be put into action in the form of best practices, new policies, regulations, and legislation, training opportunities, and proactive initiatives for solving the growing problems of identity fraud and theft, secure sharing of information, and information protection. To learn more about CIMIP, visit www.cimip.org.

About the Authors

Gary R. Gordon, Ed.D., principal investigator, is a professor of Economic Crime Programs at Utica College. In 1988, Professor Gordon developed the first major in Economic Crime Investigation in the United States. He also developed a Master's Degree in Economic Crime Management that commenced in January 1999, using a distance learning format. In 1988, Dr. Gordon founded the Economic Crime Institute (ECI) of Utica College and is its Executive Director. He has coordinated seventeen national conferences focusing on economic crime issues. In June 2006, he founded the Center for Identity Management and Information Protection and serves as its Executive Director.

Donald J. Rebovich, Ph.D. is associate professor and chair of the Economic Crime Investigation Program at Utica College. He is the assistant editor of the Journal of Economic Crime Management. His background includes research in identity theft, economic crime victimization, white collar crime prosecution, and multi-jurisdictional task force development. Before coming to Utica College, Professor Rebovich served as research director for the National White Collar Crime Center (NW3C) and for the American Prosecutors Research Institute.

Kyung-Seok Choo, Ph.D. is assistant professor and chair of the Criminal Justice Program, at Utica College. His background includes research on Korean gangs and delinquent groups in Korean American communities. He is a recipient of the Morton and Roberta Clayman fellowship, through which he researched gangs and immigrant youth. He is also actively involved in research on sex trafficking of Korean women to the United States.

Judith B. Gordon, MLS is the program administrator for CIMIP. In addition to being a researcher, she manages CIMIP's research projects, and coordinates the researchers' activities. She is a contributing author of the LexisNexis/Economic Crime Institute (ECI) white paper: *Identity Fraud: A Critical National and Global Threat* and has been involved in researching the three additional white papers supported by LexisNexis and ECI.

Table of Contents

Executive Summary	1
Introduction	6
Goals and Value of the Study	9
The Empirical Approach	10
Identity Theft Definition	10
Source of Data	10
Elements Collected	10
Data Analysis	11
Excluded Cases	11
Data Limitations	12
Findings	13
The Case	14
Secret Service Case Classification	14
Secret Service Regions	16
Case Referral	17
Jurisdiction	20
Federal Statutes Violated	21
State Statutes Violated	22
Disposition	23
Actual Loss	26
Timing of Cases	27
Geographical Scope	29
The Case in Summary	30
The Offenders	31
Gender, Race, Age, Place of Birth	31
Arrest History	36
Motivating Factors	38
An Identity Theft Offender in Summary	40
The Commission of the Crime	41
Offenses Facilitated by Identity Theft	41

Insider Identity Theft	42
Individual Activity vs. Organized Group Activity: Roles.....	43
Offender Methods	47
Utilization of Methods by Offenders	51
Patterns of Offender Methods	52
Points of Compromise	53
The Commission of the Offense in Summary	54
Victimization	55
The Victims	55
Methods of Victimization (other than individuals)	56
Offender Relationship to Individual Victims	57
Defendants Stealing Identifying Information through Employment.....	59
Victimization in Summary	60
Recommendations	61
Proactive Measures	61
Law Enforcement Training	62
Management of Cases and Resources	63
Executive Briefings	63
Future Research	64
Conclusion	65
Appendix: Collection Template	68
References	74

List of Figures

Figure 1: Most Frequent Primary Case Type	14
Figure 2: Most Frequent Secondary Case Type	15
Figure 3: Secret Service Regions	16
Figure 4: Referral to Secret Service	18
Figure 5: Case Jurisdiction	20
Figure 6: Most Frequently Violated Federal Statutes	21
Figure 7: Most Frequently Violated State Statutes	22
Figure 8: Months of Incarceration	23
Figure 9: Months of Probation	24
Figure 10: Restitution	25
Figure 11: Number of Defendants and Actual Loss	26
Figure 12: Case Duration	28
Figure 13: Year the Case Opened	28
Figure 14: Geographical Scope	29
Figure 15: Characteristics of Offenders	32
Figure 16: Race by Gender	33
Figure 17: Age by Gender	34
Figure 18: Age by Race	35
Figure 19: Race by Arrest	36
Figure 20: Arrest Type	37
Figure 21: Motivating Factors	38
Figure 22: Offenses Facilitated by Identity Theft	41
Figure 23: Identity Theft at Types of Employment	42
Figure 24: Number of Defendants	44
Figure 25: Offender Methods	49
Figure 26: Interrelationships among Methods	50
Figure 27: Points of Compromise for Identity Theft	53
Figure 28: Victims by Category	55
Figure 29: Methods of Financial Services Industry Victimization	56
Figure 30: Offender and Victim Relationships	58

Figure 31: Type of Employment Used to Steal Identities	59
--	----

Executive Summary

The purpose of this study was to provide empirical evidence on which law enforcement can base enhanced proactive identity theft control and prevention efforts. It focuses on identity theft offenders, which sets it apart from previous surveys and other research which have centered on identity theft victims. As a result of the study of closed United States Secret Service cases with an identity theft component (2000-2006), empirical data concerning the key factors relevant to the criminal behavior of identity thieves and the conditions under which that behavior occurs are available to law enforcement agencies and corporate security and fraud investigators for the first time. The results fill a gap identified in the President's Identity Theft Task Force report. The report states, "Unlike some groups of criminals, identity thieves cannot be readily classified. No surveys provide comprehensive data on their primary personal or demographic characteristics" (April 2007, p, 12). This study has gathered and analyzed comprehensive data on identity theft offenders in order to provide both the public and private sectors with information they need to combat these crimes.

For the purposes of this study, the definition of identity theft is aligned with that presented in the President's Identity Theft Task Force report, *Combating Identity Theft: A Strategic Plan*. "Although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud" (April 2007, p. 2). Personal information includes name, address, Social Security number, and date of birth, but excludes credit cards, debit cards, and other bank cards. The data for the study was collected at the Secret Service headquarters by the four authors of this report. Seven hundred and thirty four cases with an identity theft component, which were opened and closed between 2000 and 2006, were reviewed; data was collected on 517, as the other 217 were excluded.

Findings

After the data collection and analysis were completed, the findings were separated into four categories: the case, the offenders, the commission of the crime, and victimization. Highlights of these areas follow.

The Case:

Case characteristics include Secret Service classification, Secret Service region, referral to Secret Service, jurisdiction, statutes violated, disposition, actual dollar loss, timing and duration, and geographical scope.

- Many of the cases were classified as "Fraudulent Use of Account Number" and "Identity Theft."
- The highest percentage of cases was from Region 1 – Northeastern United States and were referred to the Secret Service by local or state law enforcement.

- The cases were referred to the Secret Service from various sources.
 - Approximately 47% of the cases were referred to the Secret Service by local and state law enforcement agencies.
 - Corporate security and/or fraud investigators referred 20.4% of the cases.
- Most cases fell under federal jurisdiction, with 18 USC 1028, Identity Fraud, and 18 USC 1029, Access Device Fraud, most frequently violated.
- Approximately half of the defendants in the cases were sentenced to incarceration, often in combination with probation, and restitution.
- The median actual dollar loss was \$31,356.

The Offenders:

The data analysis showed more diversity among the age, race, gender, and criminal backgrounds of offenders than the picture held by conventional wisdom.

- Most of the offenders – 42.5% -- were between 25 and 34 years of age at the time that the case was opened.
 - The 35 – 49 age group made up 33% of the offenders.
 - 18.5% were between 18 and 24 years old.
 - The remaining 6% were 50 years old or older.
- 53.8% of the offenders were black; 38.3% were white.
- One third of the offenders were female.
 - Of the females, almost two thirds were black.
- 24.1% of the offenders were born outside of the United States.
- 71% of the offenders had no arrest history.
 - Of those who did, a third were for fraud, forgery, or identity theft or fraud.
- The most prevalent motive of the offenders was personal gain. It took several forms including using fraudulently obtained personal identifying information to:
 - Obtain and use credit
 - Procure cash
 - Conceal actual identity
 - Apply for loans to purchase motor vehicles

The Commission of the Crime:

The data was examined to determine the modus operandi of the offenders, the organized nature of the crimes and offenders, and identity theft through employment.

- In most of the cases, the identity theft facilitated other offenses.
 - The most frequent offense that was facilitated by identity theft was fraud.
 - The next most frequent was larceny.
- Organized group activity was discerned in 42.4% of the cases – involving from 2- 45 offenders.

- o The roles that the defendants took varied, but most frequently involved stealing or obtaining personal identifying information and using it for personal gain.
 - o In cases with three or more offenders, there is definite coordination and organization, allowing the group to take advantage of criminal opportunities, to create opportunities for crime, and to avoid detection.
- In approximately half of the cases, the Internet and/or other technological devices were used in the commission of the crime.
 - o Within the half with no use of the Internet or technology, non-technological methods, such as change of address and dumpster diving, were used in 20% of the cases.
 - o The limited number of cases opened in 2005 and 2006 prevented any trending analysis of Internet and technological use.
- The point of compromise for stealing personal identifying information or documents was determined in 274 of the cases.
 - o In 50% of those cases a business (service, retail, financial industry, corporation) provided the point of compromise or vulnerability.
 - o A family member or friend was the point of compromise in approximately 16% of the 274 cases.
- Approximately a third of the cases involved identity theft through employment.
 - o The most frequent type of employment from which personal identifying information or documents were stolen was retail (stores, car dealerships, gas stations, casinos, restaurants, hotels, hospitals, doctors offices) – 43.8%
 - o Private corporations were vulnerable to insider identity theft in about 20% of those cases.

Victimization:

Although most of the media attention surrounding identity theft and fraud has focused on individuals, they did not make up the largest percentage of victims in this study.

- Over a third (37.1%) of the victims were financial industry organizations: banks, credit unions, and credit card companies.
- Individuals accounted for 34.3% of the victims.
- 21.3% of the victims were retail businesses (stores, car dealerships, gas stations, casinos, restaurants, hotels, hospitals, doctors' offices).
- Victimization of organizations took several forms:
 - o The financial services industry was most frequently victimized by offenders using fraudulently obtained personal identifying information to obtain new credit card accounts, to apply for and obtain fraudulent loans, to utter checks, and to transfer funds.

- o The retail industry was victimized by the use of stolen identity information to open store accounts and by purchasing merchandise with fraudulent credit cards.
- The data show that most individuals were victimized by individuals they did not know.
 - o 59% of the victims did not know the offenders.
 - o 10.5% of the victims were customers or clients of the offender.
 - o 5% of the victims were related to the offender
- 20.3% of the 939 offenders in the cases committed identity theft at their place of employment.
 - o Of those offenders, 59.7% were employed by a retail business.
 - o 22.2% were employed by a financial services industry organization.

The findings presented here must be used to improve and increase proactive measures that law enforcement and fraud investigators use to combat identity theft, including investigation, prevention, detection, and prosecution. The information concerning offender characteristics and modus operandi should be used in law enforcement training. The picture that this study paints of identity theft offenses and offenders should be used in prioritizing and managing cases and resources. Law enforcement executives will be able to use this information to develop policy, allocate resources, and advocate training.

Recommendations

The recommendations presented here are based on the use of the study's empirical evidence. 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.

The data should be used to foster proactive investigation, detection, prevention, and prosecution.

- 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.
- 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 continue to share the information they find with corporate entities, such as the financial services industry, so that prevention and detection strategies can be enhanced.
- 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.

Law enforcement training programs will benefit from the knowledge gained from the empirical findings.

- 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.

These findings provide the information law enforcement managers need 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.
- 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.

Executive briefings will allow law enforcement executives to 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.
- 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 study should be used as a model for a series of research studies.

- 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.

The authors anticipate that this groundbreaking study will make a difference in the prevention, detection, investigation, and mitigation of identity theft and fraud crimes. The empirical results regarding identity theft offenders and offenses will provide the basis for proactive procedures, policies, training, and management of resources. The continuation of this study to Secret Service cases that have closed since 2006 will allow the authors to complete trending analysis, so that predictions can be made and actions taken.

Introduction

The purpose of this BJA funded project is to identify patterns and trends of identity theft, so that public law enforcement and private sector security departments will have added knowledge to apply to a proactive means of thwarting this insidious crime. While statistics and anecdotes abound regarding identity theft victims, there has been little research into the trends and patterns of the crime, characteristics of the offenders, and methods used by individual criminals, as well as organized crime activity. Societal perceptions about identity crimes are based on a combination of notorious case incidents, broadcast vignettes depicting the unfortunate experiences of the victims, media announcements cautioning against behavior that may precipitate victimization, and, quite often, word-of-mouth. This information can have a powerful impact on the manner in which the general public synthesizes the information and draws conclusions about the actual level of danger the crime poses to them. In other words, assumptions become reality.

While no less than a decade ago “identity theft” was apt to be met with curiosity and some bewilderment, it has become one of the most recognizable crime terms of the 21st century. Even so, questions remain regarding what it really represents, what type of person is most likely to commit this crime, what criminal methods are most commonly (and successfully) employed, and who is in most jeopardy of being victimized. In order to contain and prevent identity theft, these questions must be answered through an “empirical” approach, anchored in a thorough analysis of criminal justice system data.

Law Enforcement and the Challenges Identity Theft Presents

The United States Secret Service is actively involved in the investigation and prosecution of identity theft and fraud crimes. According to its website (www.secretservice.gov/criminal.shtml):

Identity crimes are defined as the misuse of personal or financial identifiers in order to gain something of value and/or facilitate other criminal activity. The Secret Service is the primary federal agency tasked with investigating identity theft/fraud and its related activities under Title 18, United States Code, Section 1028. Identity crimes are some of the fastest growing and most serious economic crimes in the United States for both financial institutions and persons whose identifying information has been illegally used. The Secret Service records criminal complaints, assists victims in contacting other relevant investigative and consumer protection agencies and works with other federal, state and local law enforcement and reporting agencies to identify perpetrators.

Similar information can be found on the websites of the United States Postal Inspection Service, the Federal Bureau of Investigation, the Federal Trade Commission, the Social Security Administration, the Department of Justice, many state police departments, several local police departments, and the numerous not-for-profit organizations devoted to combating identity theft and helping citizens to recover from it. Identity crimes are far reaching, as the attention given to it by government entities, the businesses that have emerged in an effort to thwart it, and the many stories from the media indicate.

Statistics from Consumer Sentinel, the database of complaints maintained by the Federal Trade Commission, indicate that the highest percentage of complaints received in 2006 (36%) were concerning identity theft (<http://www.ftc.gov/opa/2007/02/topcomplaints.shtm>). Since 2001, the same has been true; the highest percentage of complaints received during each year concerned identity theft. President George Bush established the President's Task Force on Identity Theft in May 2006 by Executive Order 13402. The Task Force report (April 2007, p. 1) states, "The problem of identity theft has become more complex and challenging to the general public, the government, and the private sector." While the Internet, with its chat rooms, electronic banking and payments, phishing and pharming, malware and Spyware, and pretexting, has certainly added a dimension to the crime, the basics are also still employed by identity thieves: common theft, mail theft and change of address, dumpster diving, database and network hacking, and insider theft. The purposes for which identity thieves can use the stolen personal identifier information has been exacerbated by the Internet, as online credit applications, purchases, bank transfers, and the like eliminate the need for face to face contact.

Law enforcement is, of course, faced with the challenges that the growing complexity of the crime presents. Those challenges are compounded by the lack of empirical data showing trends and patterns. According to the FTC, in 2006 62% of the identity theft victims who made reports on the FTC website did not notify a law enforcement agency. In a February 2005 article from *The Police Chief*, "Identity Theft and Police Response: Prevention," the author, Ed Dadisho of the Los Angeles Police Department, states, "Statistics on identity theft are useful for law enforcement agencies in many ways and can determine trends in suspect methodology, victim thought processes, and consolidation of resources to combat identity theft." He goes on to say, "One of the most important ways to prevent identity theft is to educate police officers on the latest techniques to recognize during traffic stops and other detentions."

Such proactive strategies and training require knowledge gathered from research studies such as this one, in which closed United States Secret Service cases involving identity theft were studied and analyzed. For example, it is essential for law enforcement to understand the nature of identity thieves. The President's Identity Task Force Report states, "Unlike some groups of criminals, identity thieves cannot be readily classified. No surveys provide comprehensive data on

their primary personal or demographic characteristics. For the most part, victims are not in a good position to know who stole their information or misused it" (April 2007 p. 12).

Goals and Value of the Study

The mission of this project is to use the compilation of study results as a compass by which law enforcers can navigate through the fog of past conjecture to proactively facilitate effective identity theft enforcement efforts. The analysis of the data will lead to a fuller realization of trends, patterns, and groups perpetrating identity theft. It is the first step toward what is meant to be a successive series of like endeavors gauging the evolution of identity theft as a distinct crime type. They will assist law enforcement administrators, at all government levels, in creating and implementing policies for effective investigation and prosecution of identity theft.

The project was guided by four goals which were intended to provide the law enforcement community with the robust empirical information necessary to enhance identity theft control and prevention efforts.

Goal: To explore and identify, from a national perspective, key identity theft offense, offender, and case characteristics.

Goal: To collect and analyze criminal case data for the purpose of establishing an empirically-based profile of identity theft offense, offender, and case characteristics.

Goal: To isolate those empirically obtained offense, offender and case factors that accurately represent the challenges to effective identity theft control and prevention.

Goal: To convert the aggregation and analysis of identity theft crime case data into a substantive and formative guide to aid the successful control and prevention of identity theft.

The findings of this study will provide reliable information that can be used to improve law enforcement methods. This project stands as an example of applied research in its truest sense, in that it is the planned collection and analysis of criminal justice data regarding identity theft in order to assist the law enforcement community in making informed decisions. The findings on offender characteristics, modus operandi, and the varied reactions of the criminal justice system to these offenses can sensitize law enforcement to early warning signs of the complexities of identity theft cases, preparing them for the investigative road ahead. This study supplies something to the law enforcement community that, heretofore, has not been available: a scientific presentation of the key factors relevant to the criminal behavior of identity theft and the conditions under which that behavior occurs. In the final analysis, the true worth of the study will be measured by the extent to which the consumers of the information maximize the findings to affect control of the commission of identity theft.

The Empirical Approach

The primary aim of this project was to perform an exploratory quantitative and qualitative analysis of United States Secret Service closed cases to detect and synthesize identity theft patterns and trends. The researchers had no preconceived notions at the onset of the research, and did not test hypotheses. The process consisted of three steps: initial exploratory analysis of cases; iterative collection and analysis of the cases; and intensive data analysis to determine patterns.

Identity Theft Definition

In the report of the President's Task Force on Identity Theft, identity theft is defined in this way, "Although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud" (April 2007, p. 2). Although there is ongoing debate concerning the definition of identity theft, for the purposes of this study, the researchers agree with the Task Force definition, but consider personal information to be personal identifying information -- name, address, Social Security number, date of birth, which may be included on documents such as driver's licenses and birth certificates. Access devices -- credit cards, debit cards, ATM cards -- are excluded. While the theft of a credit card may result in fraudulent charges, it does not result in the theft of an identity. The Task Force report agrees: "For example, a stolen credit card may lead to thousands of dollars in fraudulent charges, but the card generally would not provide the thief with enough information to establish a false identity" (p. 3).

Source of Data

The data for this study was collected from United States Secret Service closed cases with an identity theft component which were opened and closed between 2000 and 2006. The staff at Secret Service headquarters selected the cases for the research team, based on the primary and secondary case codes that Secret Service uses to classify its cases. Seven hundred and thirty four cases were made available. The cases consisted of compilations of e-mail communications from the field office to headquarters, generally from one agent, throughout the duration of the case. The research team, working at Secret Service Headquarters in Washington, D.C., collected data on 517 of these, as the other 217 were excluded (see below).

Elements Collected

The researchers independently reviewed several of the same cases to determine which elements were of importance. They then came to consensus on the elements, based on the goals of the study and the available data. The elements

were categorized and arranged in a template to assure uniformity in data collection. (See Appendix A.)

As the cases focused on the offenders and the offense, the team chose several demographic and characteristic elements, including sex, race, date of birth, place of birth, and criminal history. The characteristics of the offense included the Secret Service classification and region, the actual loss, jurisdiction, statutes violated, disposition, the way in which the case was referred to the United States Secret Service, and details of the case including a summary of the file's case notes, the defendants' roles and relationships to the victim, the methods used, the number of defendants (including organized group activity), the geographical scope, and the victim, i.e. individual, government agency, etc.

Data Analysis

Upon completion of the collection phase, the data was inputted into statistical analysis software. The initial univariant analysis was studied and discussed by the research team to discern significant findings and determine further detailed analysis. The process was repeated so that patterns and trends could be discerned and useful information could be provided for law enforcement and corporate security organizations. The summaries of the agent's case notes were studied using content analysis tools. As initial content analysis was completed, it was discussed to determine further analysis.

Excluded Cases

29.6% per cent of the 734 cases available to the team were determined to be outside the definitional scope of this study. The factors used to exclude a case were:

- *Existing account fraud:* The team determined before beginning data collection that cases which dealt solely with existing account fraud where personal identifying information was not used would be eliminated. The President's Task Force Report defines existing account fraud as follows, "This occurs when thieves obtain account information involving credit, brokerage, banking, or utility accounts which are already open" (April 2007, p. 3).
- *No discernible connection to identity theft.*
- *Cases that were opened before 2000.*

Data Limitations

The data used in this study was collected from Secret Service cases related to identity theft that were opened and closed between January 2000 and March 2007 and made available to the research team. These cases were referred to and accepted by the Secret Service during that time period. This data does not represent all of the identity theft cases that were investigated and prosecuted during this time period by the Secret Service and other law enforcement agencies. The characteristics of cases that were not referred to and/or accepted by the Secret Service, but investigated by local or state law enforcement or another federal entity (e.g. USPIIS, FBI), may differ, as may conclusions drawn from them concerning trends and patterns. However, the differences may not be great and the findings of this study should be applied to state and local law enforcement efforts. The researchers recognize that there is an unknown figure of identity theft crimes.

Findings

The data collected has been separated into four categories: the case, the offenders, the commission of the crime, and victimization. The variables within each are reported and explained in this section.

The following characteristics of the case were examined:

- The way in which the Secret Service classified the case
- The distribution of the cases among the Secret Service regions
- The way in which the case was referred to the Secret Service
- The jurisdiction under which the cases fell
- The federal and state statutes that were violated
- The disposition of the case: incarceration, probation, restitution
- The actual dollar loss
- The timing and duration of the cases
- The geographical scope: local, state, interstate, international

The offender characteristics analyzed were:

- Demographics
 - o Gender
 - o Age
 - o Race
- Arrest History
 - o Types of offenses
- Motivating Factors

In analyzing the commission of the crime, the following characteristics were studied:

- Offenses facilitated by identity thefts
- Individual activity versus group activity and the roles the offenders took
- Offender Methods: Internet, technological, and non-technological
 - o Utilization of methods by offenders
 - o Patterns
- Point of Compromise

Victimization characteristics included:

- The victims: organizations and individuals
- Methods of victimization (other than individuals)
- Offender relationship to individual victims
- Identity theft through employment

The Case

Secret Service Case Classification

The Secret Service classifies its cases by primary and secondary code types. Each case is assigned one primary code when it is opened, based on the initial facts of the case. As the case evolves, secondary case codes are added. The agent in charge of the case and the office manager determine what codes to assign. When the case is sent to Secret Service headquarters, the classifications are reviewed and adjusted if necessary.

Figure 1 displays the most frequent primary case types represented by the 517 cases. Fifty per cent of the cases were classified as Fraudulent Use of Account Numbers, Fraudulent Access Device Applications, Stolen Bank Issued Cards, Financial Institution Fraud (FIF) Involving Check Fraud, Counterfeit Bank Issued Credit Cards, Counterfeit Commercial Checks, and Counterfeit State Driver's licenses. A quarter of the cases (listed as other) were of primary code types ranging from altered documents to other counterfeit documents to various types of financial institution fraud.

Figure 1. Most Frequent Primary Case Type

Primary Case Type Description	Frequency	Percent
Fraudulent use of account number	78	15.1
Fraudulent access device	58	11.2
Stolen Bank issued cards	36	7.0
All other cases involving FIF* investigation	35	6.8
FIF* involving check fraud	34	6.6
Counterfeit Bank issued card	27	5.2
Counterfeit commercial checks	23	4.4
Counterfeit State Driver Licence	22	4.3
Fraudulently obtained Genuine ID/Social Security Card	19	3.7
Manufacturing commercial/counterfeit check	15	2.9
Account takeover access/bank card	14	2.7
Stolen/Forged commercial/personal check	12	2.3
Fraudulent retail business card application	11	2.1
All Others	133	25.7
Total	517	100.0

*FIF=Financial Institution Fraud

Figure 2 shows the most frequent secondary case types. The numbers exceed the total number of cases because more than one secondary case type can be assigned to a case. Identity Fraud, which the Secret Service defines as the misuse of personal or financial identifiers for personal gain or to facilitate other criminal activity, was listed as a secondary case type in 87.2% (451) of the 517 cases. Significant Community Impact, which was a secondary code in 51.5% of the cases, is based on the number of people and/or accounts that are involved and the potential impact of the crime.

Figure 2. Most Frequent Secondary Case Type

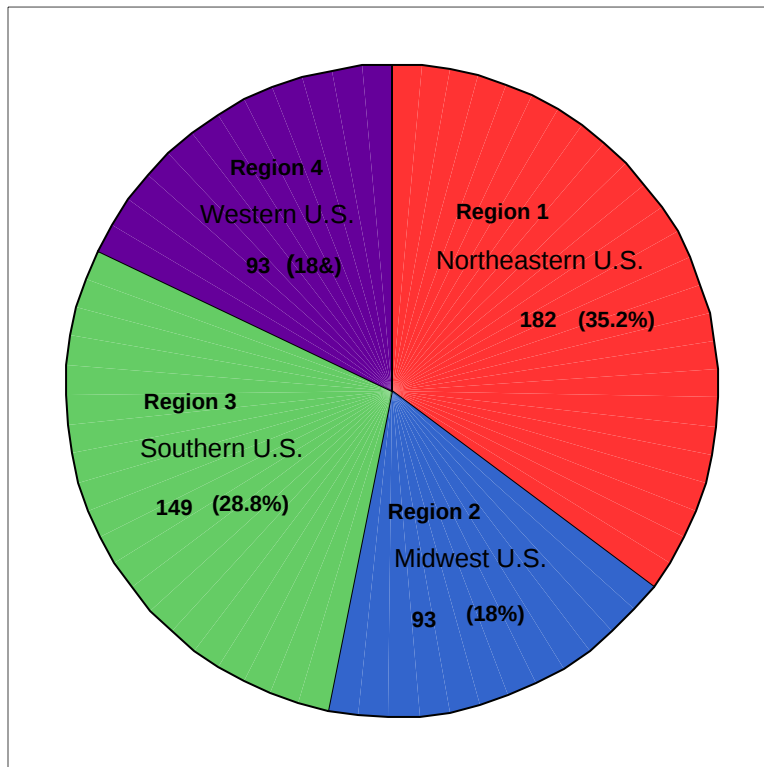
Secondary Case Type Description	Frequency	Percent
Identity Fraud	451	87.2
Significant Community Impact	264	51.5
Crimes Involving Use of Evolving Technology	163	31.5
Domestic Multi-District	100	19.3
Counterfeit State Drivers Licenses	70	13.5
All Other Non-Prioritization Investigations	67	12.9
Organized Crime Groups	60	11.6
All Other Task Forces	49	9.5
Fraudulent Use of Account Numbers	46	8.9
Fraudulent Access Device Applications	40	7.7
Electronic Crimes Task Force	37	7.2
Financial Crimes Task Force	37	7.2
Fraudulent Retail Business Card Applications	30	5.8
Transnational Criminal Activity	24	4.6
Fraudulently Obtained Genuine ID	24	4.6
Counterfeit Social Security Cards	20	3.9
Stolen Bank Issued Cards	18	3.5
Counterfeit Bank Issued Credit Cards	8	1.5
Drug Related (Non-Task Force)	8	1.5

Secret Service Regions

Each of the cases was housed in a regional or field office. These offices are in one of four regions designated by the Secret Service. Region 1 encompasses the Northeastern United States, Europe, Russia, and South Africa. Region 2 is comprised of the Midwest United States and Canada. The Southern United States, South America, and Central America make up Region 3. The 4th region includes the Western United States and Far East. Figure 3 shows that of the 517 cases, 35.2% (182) were from Secret Service field offices in Region 1, the Northeastern United States (180) and Europe (2). 28.8% (149) came from Secret Service field offices in the Southern United States. Eighty eight of the cases were from Secret Service field offices in the Midwestern United States and five were from Canada, for a total of 18% from Region 2. The cases from the Western United States (93), Region 4, made up 18% of the total. None of those was from the Far East.

Figure 3: Secret Service Regions

N=517



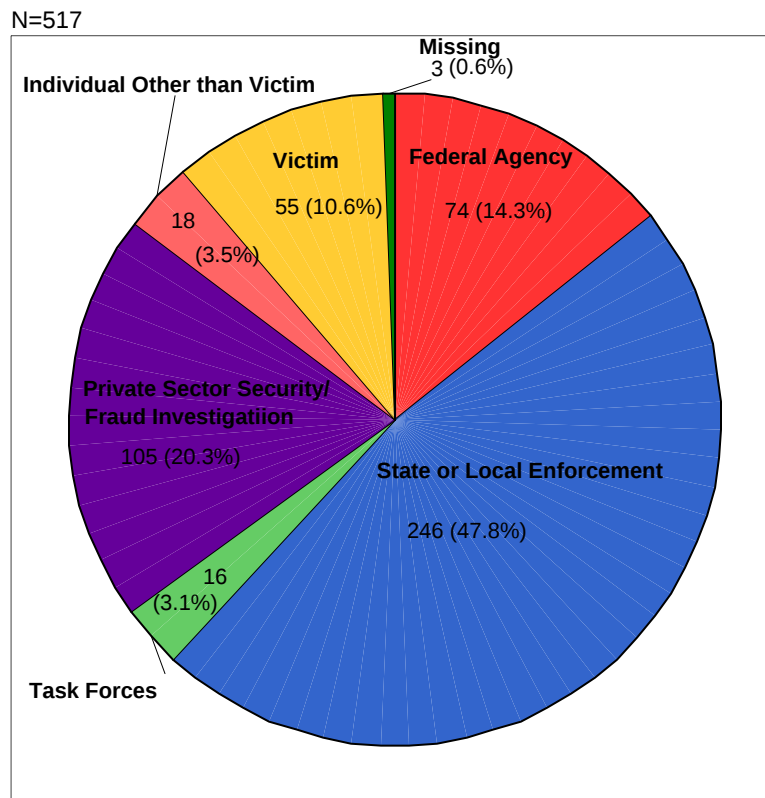
Case Referral

In each case file, the way in which the case was referred to the Secret Service was identified. The Secret Service was brought in through several channels, categorized as follows:

- Victim
- Individual other than the victim
 - o Includes anonymous tip, attorney, defendant turning himself in, confidential informant, private investigator, witness
- Local or state law enforcement agencies
 - o Includes local and county police departments, local and county sheriff's offices, state police, district or state attorney
- Federal agencies
 - o Includes Secret Service headquarters, field or regional offices, FBI, DEA, ATF, etc.
- Task forces
 - o Counterfeit Crimes
 - o Economic and Identity Crimes
 - o Electronic Crimes
 - o Financial Crimes
 - o Identity Theft
 - o Organized Crime
- Private sector security/fraud investigation
 - o Includes card processors, corporations, credit card companies, financial institutions, nursing homes, retail establishments, small business, higher education

Figure 4 shows that the largest percentage of the cases was referred to the Secret Service by local or state law enforcement: 246 cases or 47.6%. The identity theft or fraud was discovered during a routine traffic stop in 20 of those cases. (This may also have been the case in many of the others; the case files did not always indicate how law enforcement became involved.) The next most frequent referral is from private sector security and/or fraud investigations: 20.3% (105). 14.3% (74) of the cases were referred from other federal agencies. Within that category, 29 of the cases were brought to the Secret Service by the United States Postal Inspection Service. In 10.6% of the cases (55), the victim contacted the Secret Service directly.

Figure 4. Referral to Secret Service

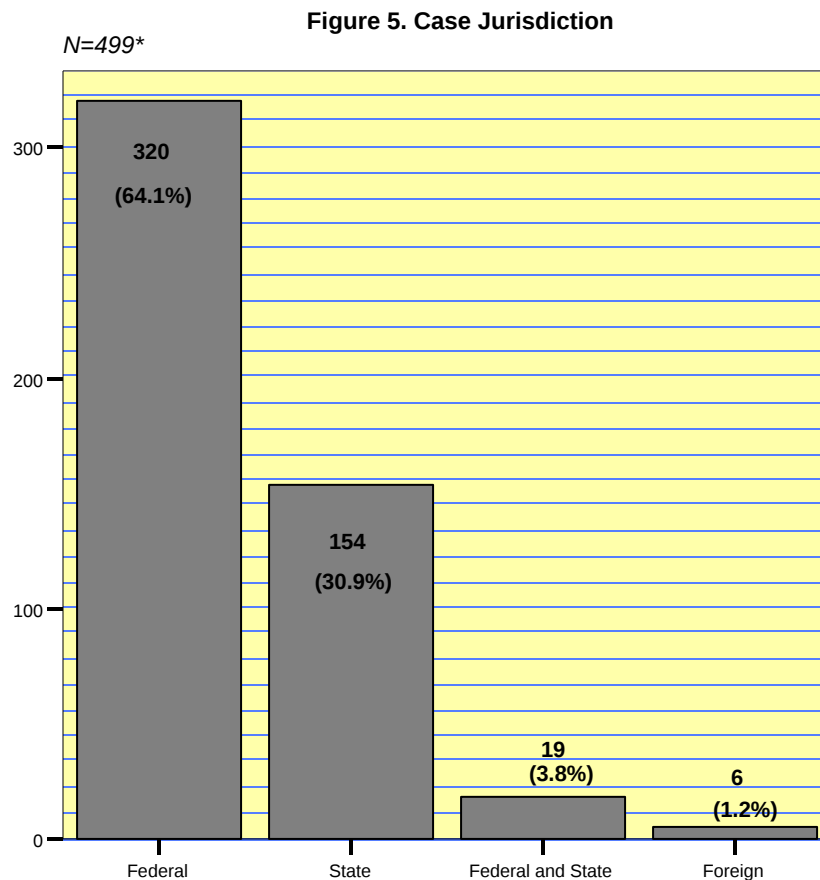


Case Referral: Local Law Enforcement

In this case from Region 2 (Midwest U.S.) the defendant was involved in a car accident. During the accident investigation, counterfeit personal checks, counterfeit identification, and a computer disk containing templates for U.S. Treasury checks, IRS refund checks, Social Security cards, and state drivers licenses were found. The detective from the local police department notified the Secret Service Financial Crimes Task Force. When interviewed, the defendant admitted that he had used the computer to commit several crimes. He obtained a LexisNexis account number from an attorney friend and used it to obtain Social Security numbers. He said he “hacked” into a military site where he accessed over 100 Social Security numbers. He made counterfeit Social Security cards and sold them to illegal immigrants. He used counterfeit bank checks and false identification to purchase a vehicle. The case was tried under state jurisdiction using a statute related to the interstate transportation of stolen property. The defendant, who had no arrest history, was sentenced to two years of incarceration and three years of probation.

Jurisdiction

The jurisdiction of each case was dependent on the U.S. Attorney's Office in the area. Each office has guidelines for cases it will prosecute. Secret Service cases often start as state cases, but as the investigation evolves, they meet the thresholds for a federal case and the state charges are dropped. As shown in Figure 5, the jurisdiction for the majority of the cases was federal: 320 out of 499 (64.1%). Individual states had jurisdiction in 30.9% (154) of the cases; 3.8% (19) were a combination of state and federal; and the jurisdiction of 6 cases (1.2%) was outside the United States. In 18 cases, the jurisdiction was not made available. Of the 320 cases with federal jurisdiction, 41.8% (134) were referred to the Secret Service from local or state law enforcement. Ninety two (59.7%) of the state jurisdiction cases were referred from local or state law enforcement. In many of these cases, victims were in one state and offenders in another.



**18 cases are excluded.*

Federal Statutes Violated

While in the past, identity theft cases were more apt to be prosecuted using mail and wire fraud statutes, Figure 6 shows that within the cases under federal and federal and state jurisdiction (339), federal statute 18 USC 1029 -- Fraud and related activity in connection with access devices -- was violated 161 times. Federal statute 18 USC 1028 -- Fraud and related activity in connection with identification documents, authentication features, and information -- was violated 133 times. This may indicate that prosecutors have become more willing to use these relatively new statutes. It should be noted that in most cases, more than one statute was violated, though not all were charged, and that more than one statute under the larger designation, such as 18 USC 1029, may have been violated. Seventy eight of the violations were of 18 USC 1344 – Bank Fraud. Misuse of Social Security Number, 42 USC 408(a)(7)(B), was noted in 49 of the cases.

Figure 6. Most Frequently Violated Federal Statutes

		N
18 USC 1029	Access Device Fraud	161
18 USC 1028	ID Fraud	133
18 USC 1344	Bank Fraud	78
42 USC 408 (a) (7) (B)	Misuse of SSN	49
18 USC 371	Conspiracy to Commit Access Device Fraud	44
18 USC 1341	Mail Fraud	28
18 USC 1343	Wire Fraud	28

State Statutes Violated

In the 173 cases that came under state jurisdiction or federal and state jurisdiction, several statutes in each state were violated. These statutes were placed into 15 categories, as shown in Figure 7. As with the federal statutes, in many cases more than one statute was violated and more than one statute within each category could be charged. The most frequent type of state statute violated was identity theft/fraud, followed by theft/larceny/stolen property and forgery. Credit card fraud statutes were violated 55 times. Statutes in these four categories were violated a total of 267 times.

Figure 7. Most Frequently Violated State Statutes

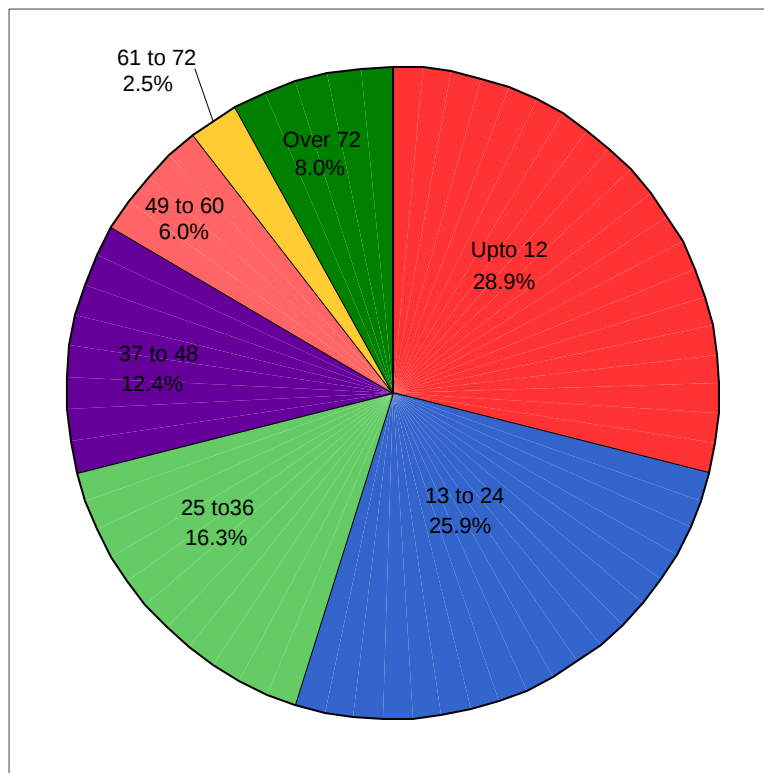
	N
Identity Theft/Fraud	82
Theft/Larceny/Stolen Property	69
Forgery	61
Credit Card Fraud	55
Bank/Check Fraud	17
Unspecified Fraud	13
Conspiracy/RICO	11
Criminal Impersonation	10
Drugs	10
Counterfeiting	7
Computer Crime	6
Miscellaneous	6
Tampering	6
Weapons	4
Assault, Violent Crimes	2

Disposition

Dispositions included incarceration, probation, restitution, and fines. There were 933 defendants in the 517 cases in this study. Four hundred and seventy nine (51.3%) of the defendants received a sentence of incarceration; however, the term of incarceration was not collected for 43 individuals. The majority of defendants whose sentences were known (54.8%) received a sentence of 24 months or less, as shown in Figure 8. Of the 479 defendants sentenced to incarceration, 67.4% (323) were federally prosecuted; 26.7% (128) were prosecuted under state jurisdiction. Five percent (24) were prosecuted using both federal and state statutes; .8% (4) received incarceration in a foreign jurisdiction. These percentages align with the percentage of cases that fell under each jurisdiction.

Figure 8. Months of Incarceration

N=436*



* 43 unspecified cases are excluded

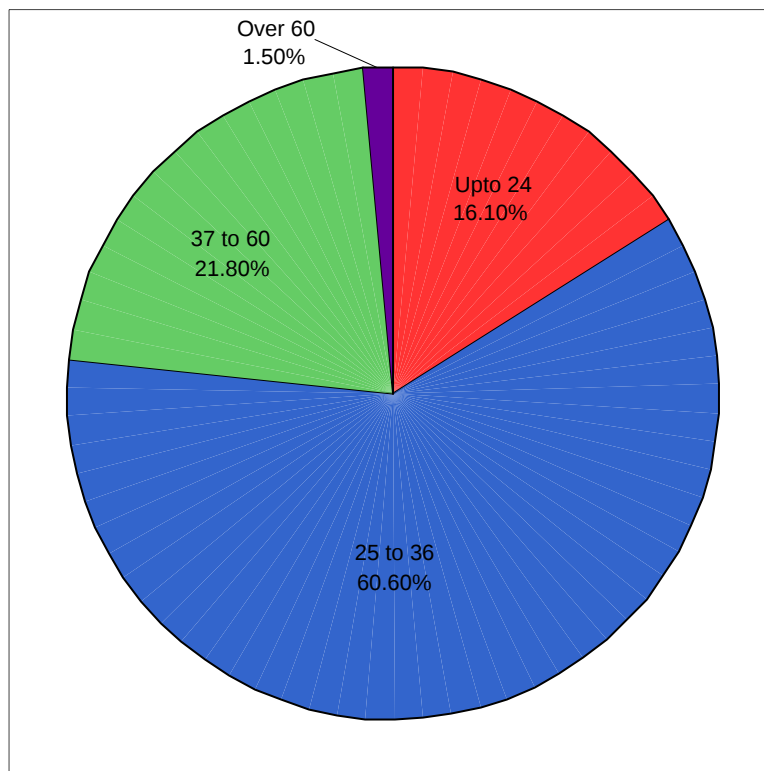
Federal Jurisdiction, 18 USC 1028 and 1029, Incarceration

In this case, which was referred to the Dallas, Texas field office by a local police department, the defendant confessed to stealing personal identifier information from members of the athletic club where he worked. Using the information, he produced counterfeit identification document on his home computer and opened numerous credit accounts. He purchased merchandise with the fraudulent accounts and sold it to friends at a discount. His arrest history included misdemeanor theft and possession of marijuana. He was charged with both 18 USC 1028 and 1029 and was sentenced to 15 months incarceration, 36 months probation, and \$54,720 in restitution.

Four hundred and eighty (51.4%) defendants received a sentence of probation; the term was not collected for three of them. Figure 9 depicts the range of probation sentences and the frequency. Of the known probation sentences, the majority 60.6 % (289) received a 25 to 36 month probation term. 21.8 % (104) of the defendants received a probation sentence between 37 and 60 months. A small percentage, 1.5 %, (7) received over 60 months. The remainder (16.4%, 77) received a sentence of up to 24 months.

Figure 9. Months of Probation

N=477*



*3 unspecified cases are excluded

In most cases, those sentenced to incarceration also received a period of probation. Three hundred and eleven, or 65%, of the 479 defendants who received incarceration were also given probation. One hundred and sixty nine defendants (18%) were sentenced to probation with no incarceration.

Three hundred and sixty one (38.7%) of the 933 defendants were ordered to pay restitution. In most cases, the amount of the restitution was congruent with the reported actual loss. Figure 10 illustrates the restitution ranges and the frequency in each grouping. One hundred and fifty six of those (43.2%) who received restitution sentences were required to pay less than \$20,000.

Figure 10. Restitution		
	N	Percent
Up to 10,000	97	26.9%
10,001 to 20,000	59	16.3%
20,001 to 30,000	45	12.5%
30,001 to 40,000	34	9.4%
40,001 to 50,000	16	4.4%
50,001 to 60,000	16	4.4%
60,001 to 70,000	14	3.9%
70,001 to 80,000	2	.6%
80,001 to 90,000	9	2.5%
90,001 to 100,000	4	1.1%
Over 100,000	65	18.0%
Total	361	100.0%

Two hundred and twenty four defendants were sentenced to both incarceration and probation and were required to pay restitution. In some cases, defendants received probation and restitution. In a few, the defendant's only sentence was restitution.

Actual Loss

The amount of loss caused by the cases varied greatly, from no dollar loss in 34 to \$13,000,000 in one case. In 47 cases, the actual loss was not available to the researchers. The median loss among the cases was \$31,356. As shown in Figure 11, the actual loss varied with the number of defendants in the case. The median loss in cases where the offender worked alone was \$22,526. That figure rose to \$42,710 in cases with two defendants, and to \$84,439 in cases with 5.

Figure 11. Number of Defendants and Actual Loss*

Actual \$ Loss			
# of Defendants	N	% of Total N	Median
1	268	57.0%	\$22,526
2	109	23.2%	\$42,710
3	37	7.9%	\$31,532
4	18	3.8%	\$48,547
5	17	3.6%	\$84,439
6 or more	21	4.5%	\$150,000
Total	470	100.0%	\$31,356

*47 unknown cases are excluded

Actual Loss: the Extremes

In a case representative of a zero dollar loss, a Houston area task force was contacted by a bank fraud investigator concerning an employee of the bank who was involved in a fraudulent transaction. The bank employee, the single defendant in the case, applied for and received a loan in another individual's name. When the car dealership refused the loan check because it was not made out in the defendant's name, he attempted to deposit it into his account at the bank where he was an assistant manager. He had applied for the loan online, using the victim's Social Security number, date of birth, and home and work phones. The defendant changed the victim's first name from Jane to Jan, and used his own address and utility bill. The victim was unaware of the car loan, but knew that someone had attempted to apply for a credit card using her personal identifiers.

In the case where the actual loss was \$13,000,000, a bank investigator contacted the Dallas Secret Service field office concerning a case of identity theft related to bank fraud. The defendant, acting alone, used false information about his identity and financial status to receive millions of dollars of loans to purchase luxury vehicles. He used the identity of a person serving life in prison for several of these, as well as to open credit accounts and buy two houses. He also used the identities of incarcerated individuals to establish several shell companies and attract investors, whom he subsequently defrauded.

Timing of Cases

For the purposes of this study, case duration is defined as the time between the dates that the case was opened and closed by the Secret Service. Figure 12 shows that the duration for the majority of the cases was two years or less – 365 of 517 cases or 70.6%. Figure 13 shows that most of the cases in the study were opened in 2002 (30.4%,156) and 2003 (25.7%,132).

Figure 12. Case Duration

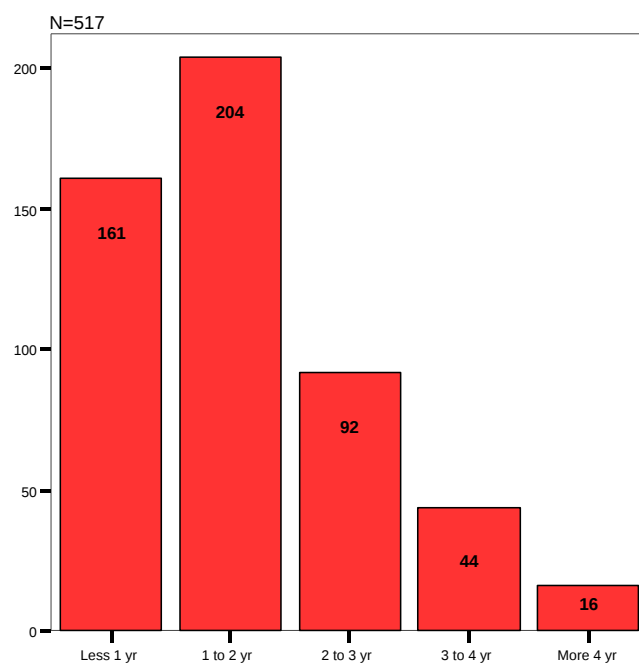
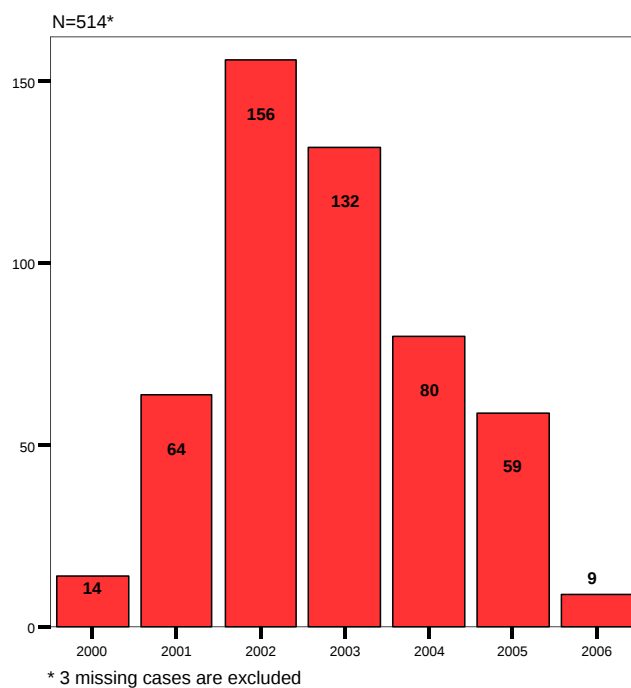


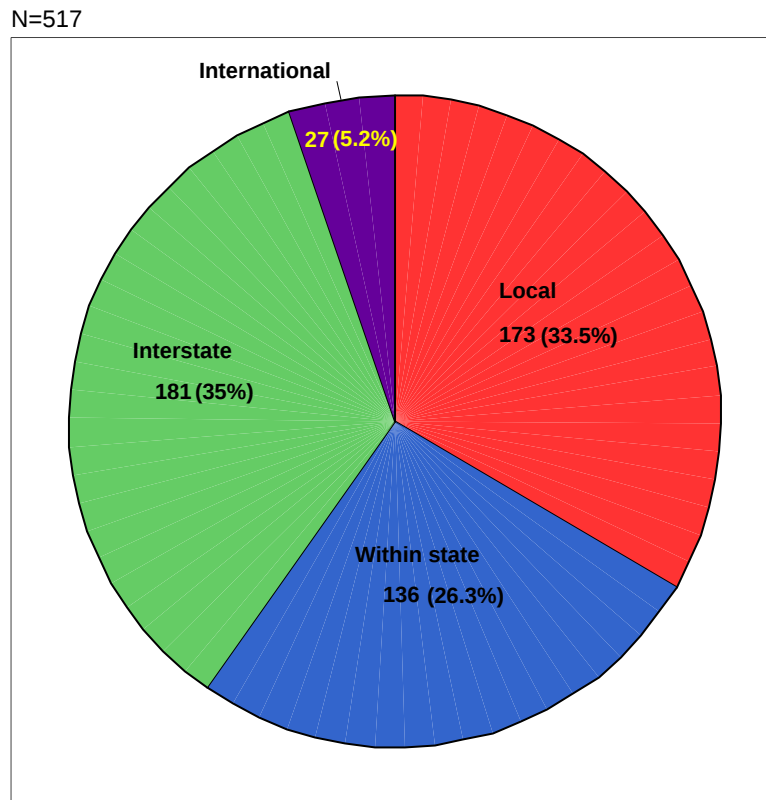
Figure 13. Year the Case Opened



Geographical Scope

Data was collected concerning the geographic range of the cases. If the offenders and their victims were located in one place, such as a metropolitan area, the case was considered “local.” If they operated in several cities and towns within one state, the designation was “within state.” “Interstate” was for cases in which the offenders operated in more than one state or in which the offenders were in one state or states and the victims in another state or states. In “international” cases the offense reached from the United States to another country. As shown in Figure 14, the cases were fairly evenly divided among local, state, and interstate.

Figure 14. Geographical Scope



The Case in Summary

Based on the findings, a typical closed Secret Service case involving identity theft was referred to a field or regional office in Region 1 (Northeastern United States and Europe) by local or state law enforcement. The case was opened in 2002 or 2003 and closed within two years, and its geographical scope was local or interstate. The case's primary classification was Fraudulent Use of Account Numbers, with a secondary classification of Identity Theft. The jurisdiction was federal and either 18 USC 1029 or 18 USC 1028 was violated. The actual loss was \$20,000 or less. At least one defendant was convicted and given a sentence including incarceration of 24 months or less, probation of 2 -3 years, and restitution less than \$20,000. The following case illustrates this, with the exception of the referral to the Secret Service.

A "Typical" Case

The victim contacted the Newark, New Jersey field office in August 2002. He reported that he had received numerous credit card account statements from retail stores, none of which he had authorized. The case's primary classification was Fraudulent Use of Account Numbers. One of the secondary classifications was Identity Fraud. The defendant had purchased a birth certificate and W-2 form in the name of the victim. He used those to obtain a duplicate driver's license, which he used to open store credit card accounts in the local area. The actual loss was \$13,175. The case fell under federal jurisdiction. The defendant pled guilty to charges of 18 USC 1029(a)(2), Access Device Fraud, and was sentenced to 18 months in prison, 3 years of probation, and ordered to pay \$13,175 in restitution. The case was closed in March 2004.

The Offenders

In order to gain a greater understanding of the type of individual who is likely to commit identity theft, data collected on the offender included gender, race, age at the time the Secret Service case was opened, and place of birth. Information was also gathered from the files concerning arrest history and the types of prior offenses, and motivating factors.

Gender, Race, Age, Place of Birth

Within the 517 cases included in this study, there were 933 defendants or offenders. As Figure 15 indicates, 67.4% (627) of the offenders were male. Females accounted for a sizable minority of 32.6% (303). The gender of three of the offenders was not made available. Also included in Figure 15 is the distribution of age, race, and whether or not the defendant had an arrest history. The age statistics are based on the age of the defendant during the year in which the case was opened. Information on the age of 116 offenders was not made available. The largest percentage of offenders – 42.5% -- were between 25 and 34 years of age (347). The 35 – 49 age group made up 33% of the offenders (270). 18.5% (151) were between 18 and 24 years old. The remaining 6% (49) were 50 years old or older.

The majority of the offenders were black: 53.8% (467). White offenders accounted for 38.3% (332). 4.8% (42) of the offenders were Hispanic and 3.1% (27) were Asian. The race for 65 of the offenders was not made available.

Information on arrest history was available for 922 of the defendants. Most of them – 71% (655) did not have any prior arrest history, while 29% (267) did.

Figure 15. Characteristics of Offenders

Total		Number	Percent
		933	100%
Gender	Male	627	67.4%
	Female	303	32.6%
		<u>Subtotal 930^a</u>	<u>100%*</u>
Age	18-24	151	18.5%
	25-34	347	42.5%
	35-49	270	33.0%
	50-64	42	5.1%
	65 or older	7	0.9%
		<u>Subtotal 817^b</u>	<u>100%*</u>
Race	White	332	38.3%
	Black	467	53.8%
	Hispanic	42	4.8%
	Asian	27	3.1%
		<u>Subtotal 868^c</u>	<u>100%*</u>
Arrest	Yes	267	29%
	No	655	71%
		<u>Subtotal 922^d</u>	<u>100%*</u>

* % calculation in each variable excludes unknown cases

a. 3 unknown due to various reasons

b. 116 unknown due to various reasons

c. 65 unknown due to various reasons

d. 11 unknown due to various reasons

Information on the offenders' place of birth was available for 660 offenders. While a clear majority of these offenders was born in the United States, almost one quarter (24.1%, 159) were not. The top five countries represented were Mexico (21), Nigeria (20), the United Kingdom (12), Cuba (11), and Israel (7).

Figure 16 shows that there is a relationship between race and gender among the offenders. Most of the female offenders were black 61.6% (172). 30.8% (86) were white. Of all white offenders, 25.9% were female, as opposed to the black offenders where 36.9% were female. The distribution of blacks and whites among male offenders was more even – 41.8% (246) of the males were white; 50% (294) were black.

Figure 16. Race by Gender					
Race			Gender		Total
			Male	Female	
White	Count		246	86	332
	% within Race		74.1%	25.9%	
	% within Sex		41.8%	30.8%	
	% of Total		28.4%	9.9%	38.3%
Black	Count		294	172	466
	% within Race		63.1%	36.9%	
	% within Sex		50.0%	61.6%	
	% of Total		33.9%	19.8%	53.7%
Asian	Count		19	8	27
	% within Race		70.4%	29.6%	
	% within Sex		3.2%	2.9%	
	% of Total		2.2%	.9%	3.1%
Hispanic	Count		29	13	42
	% within Race		69.0%	31.0%	
	% within Sex		4.9%	4.7%	
	% of Total		3.3%	1.5%	4.8%
Total	Count		588	279	867
	% of Total		67.8%	32.2%	100.0%
Percentages and totals are based on responses.					

A more detailed analysis provides some insight into the age at which females are involved in identity theft, as shown in Figure 17. Females tend to demonstrate greater identity theft activity at younger ages than men do. 51.9% (137) of all the females were between 25 and 34 years old in the year the case was opened, while only 38% (210) of the males fell into that age bracket. About the same percentage of males – 36.5% (202) were between the ages of 35 and 49 at the time the case was opened, as opposed to 25.8% (68) of the females who were in that age grouping.

Figure 17. Age by Gender

		Gender		Total
		Male	Female	
Age				
18-24	Count	102	49	151
	% within Age	67.5%	32.5%	
	% within Gender	18.4%	18.6%	
	% of Total	12.5%	6.0%	18.5%
25-34	Count	210	137	347
	% within Age	60.5%	39.5%	
	% within Gender	38.0%	51.9%	
	% of Total	25.7%	16.8%	42.5%
35-49	Count	202	68	270
	% within Age	74.8%	25.2%	
	% within Gender	36.5%	25.8%	
	% of Total	24.7%	8.3%	33.0%
50-64	Count	35	7	42
	% within Age	83.3%	16.7%	
	% within Gender	6.3%	2.7%	
	% of Total	4.3%	.9%	5.1%
65 or older	Count	4	3	7
	% within Age	57.1%	42.9%	
	% within Gender	.7%	1.1%	
	% of Total	.5%	.4%	.9%
Total	Count	553	264	817
	% of Total	67.7%	32.3%	100.0%

Percentages and totals are based on responses.

Figure 18 shows the relationship between race and age. In the first two age categories, 18-24 and 25-34, the percentages of whites and blacks are representative of the total percentage of black and white defendants. Within the 18-24 age group, among the defendants for whom both race and age was known, 50.7% were black and 37.3% were white. The percentages are similar in the next category: 25 – 34, 55.5% black, 36% white. In the next two categories, the percentage of whites is higher than the percentage of all white offenders: 35 – 49, 52.4% black, 40.9% white; 50 – 64, 40.5% black, 54.8% white.

Figure 18. Age by Race

			Race				Total
			White	Black	Asian	Hispanic	
Age	18-24	Count	56	76	6	12	150
		% within Age	37.3%	50.7%	4.0%	8.0%	
		% within Race	17.7%	17.8%	24.0%	28.6%	
		% of Total	6.9%	9.4%	.7%	1.5%	18.5%
	25-34	Count	124	191	11	18	344
		% within Age	36.0%	55.5%	3.2%	5.2%	
		% within Race	39.1%	44.6%	44.0%	42.9%	
		% of Total	15.3%	23.5%	1.4%	2.2%	42.4%
	35-49	Count	110	141	6	12	269
		% within Age	40.9%	52.4%	2.2%	4.5%	
		% within Race	34.7%	32.9%	24.0%	28.6%	
		% of Total	13.5%	17.4%	.7%	1.5%	33.1%
	50-64	Count	23	17	2	0	42
		% within Age	54.8%	40.5%	4.8%	.0%	
		% within Race	7.3%	4.0%	8.0%	.0%	
		% of Total	2.8%	2.1%	.2%	.0%	5.2%
	65 or older	Count	4	3	0	0	7
		% within Age	57.1%	42.9%	.0%	.0%	
		% within Race	1.3%	.7%	.0%	.0%	
		% of Total	.5%	.4%	.0%	.0%	.9%
Total		Count	317	428	25	42	812
		% of Total	39.0%	52.7%	3.1%	5.2%	100.0%

Percentages and totals are based on responses.

Arrest History

Defendant arrest history information was available for 859 of the 922 defendants. Within that number, the majority, 71%, had no previous history. As shown in Figure 19, the racial breakdown of the 29.9% with prior arrests is of interest. Although Hispanic offenders made up only 4.9% (42) of the offenders, 42.9% of them had previous arrests. 25.5% Of white offenders had previous arrests, as did 32.8% of the black offenders.

Figure 19. Race by Arrest

		Arrest		Total
		Yes	No	
Race	White	Count	84	245
		% within Race	25.5%	74.5%
		% within Arrest	32.7%	40.7%
		% of Total	9.8%	38.3%
	Black	Count	151	461
		% within Race	32.8%	67.2%
		% within Arrest	58.8%	51.5%
		% of Total	17.6%	53.7%
	Asian	Count	4	27
		% within Race	14.8%	85.2%
		% within Arrest	1.6%	3.8%
		% of Total	.5%	3.1%
	Hispanic	Count	18	42
		% within Race	42.9%	57.1%
		% within Arrest	7.0%	4.0%
		% of Total	2.1%	4.9%
Total		Count	257	859
		% of Total	29.9%	100.0%

Percentages and totals are based on responses.

Offenders with criminal histories tended to have committed fraud related crimes or property offenses. As shown in Figure 20, of the 595 previous arrests noted in the case files, 33.2% (197) were for fraud, forgery, or identity theft or fraud. 26.6% (158) were for theft/larceny. The previous arrests were for violent crimes in only 12.6% (75) and for drug offenses in only 9.4% (56).

Figure 20. Arrest Type		
	Responses	
	N	Percent
Theft/Larceny	158	26.6%
Fraud	89	15.0%
Forgery	76	12.8%
Violent Crime	75	12.6%
Drugs	56	9.4%
ID Theft and Fraud	32	5.4%
Disorderly Behaviors	20	3.4%
Traffic Offense	19	3.2%
Weapons	15	2.5%
Terrorism	13	2.2%
Immigration	12	2.0%
Counterfeit	3	.5%
Child Endangerment	4	.7%
Offender Supervision Violation	9	1.5%
Miscellaneous	14	2.4%
Total	595	100.0%

Motivating Factors

The data collection included a paragraph summary or synopsis of the case, based on the description of the investigation in the files, for 503 of the cases. These summaries provided information about the factors which motivated the offenders to commit the offense that provided them with fraudulently obtained or fictitious personally identifying information. In most of the cases there was more than one motive. Figure 21 shows the frequency and percentage of the eight most prevalent motives for committing identity theft or fraud.

Figure 21: Motivating Factors

Motive	Number	Percentage
Use stolen ID to obtain and use credit	228	45.3%
Use stolen ID to procure cash	166	33%
Use stolen ID to conceal actual identity	114	22.7%
Use stolen ID to apply for loans to buy vehicles	105	20.9%
Use stolen ID to manufacture and sell fraudulent IDs	39	7.7%
Use stolen ID to obtain cell phones and services	23	4.6%
Use stolen ID to gain government benefits	19	3.8%
Use stolen ID to procure drugs	11	2.2%

Use stolen or fraudulent ID to obtain and use credit: This includes using stolen identification documents and information, fraudulent and altered identity documents, counterfeit credit cards and identity documents, fictitious identity information, and fraudulently obtained credit cards to obtain credit, obtain access to credit card accounts or open credit accounts, and use them to make purchases. As shown in Figure 21, this was a motive in 45.3% (228) of the cases.

Use stolen ID to procure cash: This includes opening bank accounts, uttering counterfeit checks, transferring funds between and among accounts, and uttering forged or stolen checks using stolen or fraudulent identification documents. Obtaining cash was a motivating factor in 33% (166) of the cases.

Use stolen ID to conceal actual identity: This includes purchasing fraudulent ID documents or stealing them to hide ones' true identity, to gain employment, to

conceal credit history, and to obtain “new” identity documents. This motive occurred in 22.7% (114) of the cases.

Use stolen ID to apply for loans to buy vehicles: In 20.9% (105) of the cases, the offenders used fraudulently obtained personally identifying information to apply for loans, obtain loans, and purchase motor vehicles.

Use stolen ID to manufacture and sell fraudulent IDs: The business of providing fraudulent identification documents for profit was a motive in 7.7% (39) of the cases. The offenders manufactured and sold driver’s licenses and Social Security cards, often to match stolen credit cards. They sold counterfeit and fraudulent identification documents, credit card numbers, and fraudulently obtained personally identifying information.

Use stolen ID to obtain cell phones and services: Fraudulently obtained personally identifying information was used to open cellular phone accounts and procure services in 4.6% (23) of the cases.

Use stolen ID to gain government benefits: Offenders used fraudulently obtained personally identifying information to collect entitlement payments and to file income tax returns to get refunds in 3.8% (19) of the cases.

Use stolen ID to procure drugs: In 2.2% (11) of the cases, drugs were a motivating factor. The offenders used stolen identity information in some way to get the cash to support their drug addictions.

It is clear that the primary motive of the offenders in these cases was financial gain. With the possible exceptions of using the fraudulent information to conceal actual identity and to obtain cell phones and services, all of these motives point to a need or desire for money. Some of the offenders were involved in perpetuating the offenses as a profitable business. Others simply wanted the ability to purchase a car or other merchandise or pay their bills. In some cases, drug addicts used identity theft offenses as a means of supporting their habits.

Motivating Factor: Supporting a Drug Habit

In this case, which was opened in 2003, the three defendants worked together to steal mail from mailboxes in suburban towns when they needed money to support their methamphetamine habit. They looked for mail containing government, payroll, and personal checks and personal identifiers. One defendant used his computer to produce counterfeit state driver’s licenses, Social Security cards, and counterfeit checks. Each of the defendants was sentenced to incarceration and probation.

An Identity Theft Offender in Summary

It seems, based on the Secret Service case data, that the characteristics of an identity theft offender are complex. There is considerable diversity among race, age, gender, and criminal background. There were more black offenders than white. A third of the offenders were women and were younger than their male counterparts. Overall, the offenders in the examined cases were born in the United States, but it is difficult to ignore the fact that close to one quarter were not. And while most of these offenders show no evidence of arrests for prior offenses, those who do demonstrate a clear past participation in like crimes: fraud and other property-related offenses. The overriding motive was financial gain.

Identity Theft Offenders

In this case two of the defendants were black females and two were black males. There were between the ages 25 and 29 at the time the case was opened. They all had prior records, including forgery, narcotics violations, assault, weapons possession, and obtaining property via false pretenses. The two females directed the activities of the other two. In an effort to procure cash, the younger woman produced and passed counterfeit checks, using a fraudulent driver's license in another woman's name, searched the Internet for routing numbers for local banks and made up account numbers.

The Commission of the Crime

Offenses Facilitated by Identity Theft

Although 517 cases were studied, there were more than that number of offenses, as more than one offense could be committed within each case. Therefore, data was collected concerning 1093 offenses that were facilitated by identity theft. In almost every case, a situation presented itself which allowed the offender to commit crimes by taking advantage of an opportunity or vulnerability. Figure 22 illustrates the types of crimes which identity theft facilitated.

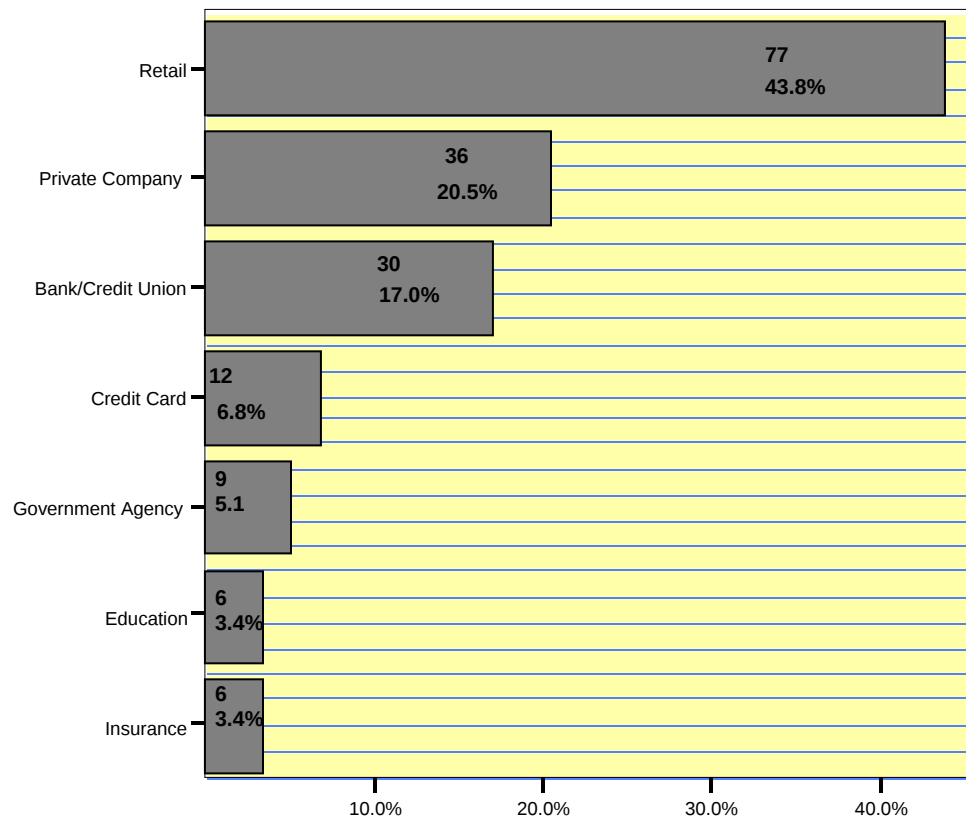
Figure 22. Offenses Facilitated by ID Theft			
Offense	Responses		Percent of Cases
	N	Percent	
Fraud	436	39.9%	87.0%
Larceny/Theft	375	34.3%	74.9%
Forgery/Counterfeiting	208	19.0%	41.5%
Drug Possession	13	1.2%	2.6%
Immigration	11	1.0%	2.2%
Weapons	10	.9%	2.0%
Drug Trafficking	8	.7%	1.6%
Embezzlement	8	.7%	1.6%
Other	24	2.3%	4.4%
Total	1093	100.0%	100% (N=501)

The most frequent offense that was committed through or with identity theft was fraud. It occurred in 87% of the cases, accounting for 39.9% (436) of the total offenses. This is not surprising, as a component of identity theft is fraudulent behavior, such as opening new accounts using another individual's personal identifying information. Larceny/theft was the next most frequent, as once new accounts are opened, the offender uses the money or credit to acquire merchandise or services, therefore stealing from the institutions (bank, retail) and/or the individual. It was a component of 74.9% of the cases, occurring 375 times. Forgery/counterfeiting was part of 41.5% of the cases, and constituted 19.0% (208) of the total offenses. Again, this is to be expected, as counterfeiting includes producing fraudulent identity documents, based on stolen personal identifying information. The other offenses listed occurred much less frequently. Credit card skimming, family offenses, and Internet and telephone scams are included in "Other."

Insider Identity Theft

By and large, these offenses were not perpetrated by insiders (e.g., employees of entities housing the identity information/documents stolen). In 65.9% (341) of the cases, the offenses were not committed through the employment of the offenders, while the point of vulnerability was the offenders' place of employment in 34.1% (176). Identity theft through employment, as shown in Figure 23, occurred most often among offenders employed in the retail industry – stores, gas stations, car dealerships, casinos, restaurants, hospitals, doctors' offices, hotels, and the like. Offenders stole personal identifier information from these places of employment in 77 cases – 43.8% of the cases involving identity theft through employment. It occurred 36 times in private companies (20.5%).

Figure 23. Identity Theft at Types of Employment



Identity Theft through Employment

The defendant was employed by a cleaning service (service industry) and cleaned the victim's residence. While on the job, he stole the brokerage account number belonging to the victim's company and through telephone transfer, using the victim's date of birth and Social Security number, had \$80,000 placed in a bank account. He later withdrew it, placed it in another bank account, and used the money to purchase a vehicle. The victim was on an airplane at the time of the call requesting the transfer. He became aware of the fund transfer when the brokerage called him to confirm the transaction.

Individual Activity vs. Organized Group Activity: Roles

The data collected from the Secret Service cases included the number of defendants and the roles which they played in the commission of the crime. The roles the defendants took were:

- Steal or obtain personal identifying information (e.g. personal identifying information that could be captured from credit card databases, client and employee records, credit card receipts, bank statements, stolen mail, checks)
- Steal or obtain personal identifier documents (e.g. driver's licenses, birth certificates, Social Security cards, employee badges)
- Steal or obtain bank cards (credit, debit, ATM)
- Alter identification documents (e.g. driver's licenses, Social Security cards, birth certificates, employee badges)
- Produce counterfeit identification documents (e.g. driver's licenses, Social Security cards, birth certificates, employee identification cards)
- Distribute personal identifier information to others (so that they could use it for personal gain)
- Sell identification documents (genuine and counterfeit)
- Use identification documents for own use (The offender used genuine or counterfeit documents for his or her own personal gain.)
- Use identification documents to obtain more identification documents (e.g. using a utility bill and birth certificate to procure a driver's license)
- Direct others' activities (within an organized crime group, giving instructions or orders to the others in the group)
- Other (includes credit card skimming, encoding or re-encoding bank cards)

It is clear that the majority of the 517 cases involved a single offender, As Figure 24 shows, 57.6% (298) of the cases were ones in which there was only one defendant. In close to a quarter of the cases (22.8%,118), however, two offenders worked together to commit the identity theft offenses. There is a significant drop in the frequency of cases with more than two offenders. There were three in 7.9% (41) cases, and four in 3.5% (18). From there the number of cases with multiple offenders continues to decrease. Seven cases had 10 or more offenders, with the largest number being 45.

Figure 24. Number of Defendants

	Frequency	Percent
1	298	57.6
2	118	22.8
3	41	7.9
4	18	3.5
5	17	3.3
6	8	1.5
7	3	.6
8	5	1.0
9	2	.4
10	2	.4
13	1	.2
16	1	.2
18	1	.2
21	1	.2
45	1	.2
Total	517	100.0

Analysis of the roles that the offenders played in the commission of their crimes provides information on how the criminal actions differed according to the number of offenders involved in each case. It should be noted that a defendant or defendants could take more than one role within a case. Thus, the numbers are varied. Personal identifying information was stolen or obtained by 609 defendants. Of those 609, this role was taken most frequently by an offender who worked alone (one offender case) – in 40.2% (245) of these instances. The next most frequent role was using identification documents for own use. This role was taken by 476 defendants. Again, those offenders who worked alone took this role most frequently – 46% (219). In 43.1% (81) of those cases in which offenders used identification to obtain additional identification documents there was only one offender. Two offender cases accounted for 19.7% (37). In 70.4% (69) of the instances in which offenders took the role of altering identification documents,

there were one or two defendants involved in the case. As would be expected, one offender cases accounted for only 12% of cases in which others' activities were directed, while cases with five or more offenders accounted for 37% (51). Again not surprisingly, information was distributed to others in a only a small number of one offender cases (13.5%, 20). This role was most often taken in cases with five or more offenders, 35.1% (52).

It is interesting to note that the most frequent role, no matter how many offenders were involved, was stealing or obtaining personal identifying information. While it seems obvious that identity theft involves obtaining personal identifying information, conventional wisdom may have dictated that it is personal identifier documents or bank cards that are most often the point of vulnerability. With the exception of cases with four offenders, the second most frequent role is using identification documents for own use. In other words, once the offender had identification documents (genuine or counterfeit), he or she used them for personal gain, whether or not a group was involved. The two roles that are directly related to group criminal activity are directing others' activities and distributing information to others. The data show that while these roles were taken most frequently in cases with two or more offenders, they accounted for 10% or less of the roles that these multiple offenders took in committing their crimes. However, a comparison between one offender and five or more in terms of directing other's activity shows a logical disparity – 1.68% for one offender, 10.16% for five or more. The same is true for distributing information to others -- 2.10% for one, 10.36% for five or more.

As the results show, the most common types of identity theft cases in the sample are those in which one individual operated alone or worked with one other person to initiate and complete an offense(s) of identity theft. These cases generally entailed obtaining or stealing personal identifying information and using it for their own use. Based on more detailed qualitative information provided in case investigation notes, those cases in which only one offender was involved were often driven by criminal opportunities that were assessed as desirable by the offender, with no recruitment of or consultation with criminal others. These offenders started with identity theft to lead to other criminal activity, and took on several roles. In the description below, the offender took advantage of a website to obtain personal identifying information. He used that information to further his scheme of selling counterfeit DVDs and to open credit accounts. A temporary job offered another point of opportunity. He obtained personal identifying information from the company and used it to produce counterfeit identification documents and open accounts. This offender identified points of vulnerability, obtained personal identifier information, used it to produce counterfeit identification documents, and used it in illegal activity for his own gain.

One Offender – Several Opportunities and Roles

The offender purchased a fake ID from www.counterfeitlibrary.com and used it to procure a mailbox at Mailboxes Etc., as he needed an address to use in selling counterfeit DVDs that he obtained from Taiwan on eBay (auction fraud). Using www.counterfeitlibrary.com, the defendant purchased a fraudulent ID from an individual in England and used it to obtain a pre-paid credit card from Rite-Aid in another's name. He also bought a counterfeit birth certificate and a Netbank account in another name, and received information on setting up Netbank accounts. He traded Netbank account information for credit card information. He also purchased 10 blank counterfeit birth certificates. While working as a temporary employee at an insurance company, he stole the names and personal identifiers of approximately 12 people and used them to obtain pre-paid credit cards using counterfeit licenses which he manufactured on his home computer. He purchased and used personal identifiers and credit card information to add users to the account, to get additional cards, and to change the address.

The crimes involving two offenders can be considered small level group crimes in that they can involve continuing actions designed to perpetuate the crimes. They can also be opportunistic in nature, as one of the offenders may serve as the "host" of the low level enterprise, having access to source identification information that becomes the catalyst for commission of the offense. This is consistent with the President's Identity Task Force Report which states on page 12, "Occasionally, small clusters of individuals with no significant criminal records work together in a loosely knit fashion to obtain personal information and even to create false or fraudulent documents." The following description of a small level group crime case illustrates this, as the second defendant had access to information which enabled the first defendant to perpetrate several crimes. Defendant two's roles were stealing or obtaining personal identifying information, producing counterfeit identification documents, distributing the information to others, and selling identification documents. Defendant one obtained personal identifying information and identification documents, and used them both for her own use and to procure more identification documents.

A small level group crime case

Defendant two obtained personal identifying information from a source at a state Secretary of State office, for the purpose of selling it to people who needed to change their identities. Defendant one bought information, as well as birth and marriage certificates, from him and used them to obtain a driver's license and Social Security number. She obtained several credit cards in the names and paid the bills for them. She used the false name at her place of employment and later received disability checks in that name. She also filed income taxes in that name. She stated that she had to change her identity to protect herself from the family of a person whom her brother murdered in self-defense approximately 30 years ago. Neither defendant had a prior arrest history.

As the number of offenders increases within cases, there is a greater similarity to operations within an actual criminal enterprise. There is a good chance that a specialization of services will exist within some of these larger groups, as well as a diversification of responsibilities in others. There may be a director of activities within the identity theft group, instructing others on their function within the group (i.e., altering authentic IDs, creating counterfeit IDs, laminating counterfeit IDs). In some cases there is more than one director of activities. The director may be the provider of raw materials that are dispersed or shared with the “line workers” within the group for activation in the field. Criminal proceeds are usually shared among the group. In other situations, fraudulent identification documents are sold to others outside of the group, and proceeds are shared within the group.

Roles taken in an organized group case

In a case with 16 defendants, the group used unauthorized credit card numbers to purchase airline tickets in their own names and to reserve hotel rooms through websites. They also used the names of others and driver’s licenses in those names as identification when flying. Several of the defendants accessed workplace computers to obtain customers’ personal identifying information, which they distributed to the rest of the group. Billing documents were also used as a source of personal identifying information. One defendant skimmed credit card numbers (other) at hotels where she was employed. Two of the defendants were involved in distributing the information to others in the group. Three of them directed others. For example, they instructed and paid others to purchase tickets for them. They all used the stolen personal identifying information for their own use – purchasing tickets and booking hotel rooms for travel to various cities where a social organization to which they all belonged held meeting.

In essence, the results show that while most of the crimes examined were one offender or two offender cases, special note should be taken of the close to 20% of the cases that involved 3 or more offenders. All of the crimes in the sample were planned and took advantage of some opportunity that presented itself to the offender(s). The cases involving larger numbers of offenders, however, distinguished themselves from the others in that the degree of coordination and organization was more pronounced. The activities of these groups were designed to take advantage of criminal opportunities, create opportunities for crime, and avoid detection. In that sense, they sought to preserve the continuity of their enterprise, as any other ongoing criminal enterprise would.

Offender Methods

In addition to examining the roles that the defendants took in the commission of the crimes, data was collected on the methods used to perpetrate them. The information was gathered in three categories: the Internet and the various ways in which it was used, technological devices, and non-technological means. The items in each category are as follows:

- The Internet
 - o Unspecified use
 - o E-mail
 - o Phishing
 - o Hacking
 - o 419 scam
 - o Malware/viruses
 - o Online database searching
 - o Online ID purchase and/or sale
 - o Other (e.g. PayPal accounts, chat rooms, online purchases)
- Technological Devices
 - o Computers to scan documents
 - o Computers to produce documents
 - o Computer printers to produce documents
 - o Photocopier
 - o Typewriter
 - o Digital camera
 - o Cell phones
 - o Telephone
 - o Other (access device reader, credit card encoder, fax machine, laminating machine, etc.)
- Non-technological means
 - o Mail theft
 - o Rerouting of mail (change of address cards)
 - o Dumpster diving – residential and business
 - o Public records

This data was collected in an effort to determine the extent of Internet and technological use in committing identity theft and fraud. The report of the President's Identity Theft Task Force states, "Criminals first gather personal information either through low-tech methods such as stealing mail or workplace records, or 'dumpster diving,' or through complex and high-tech frauds such as hacking and the use of malicious computer code" (April 2007, p. 10). The data collected in this area also relates to the way in which technology was used to produce counterfeit documents and devices.

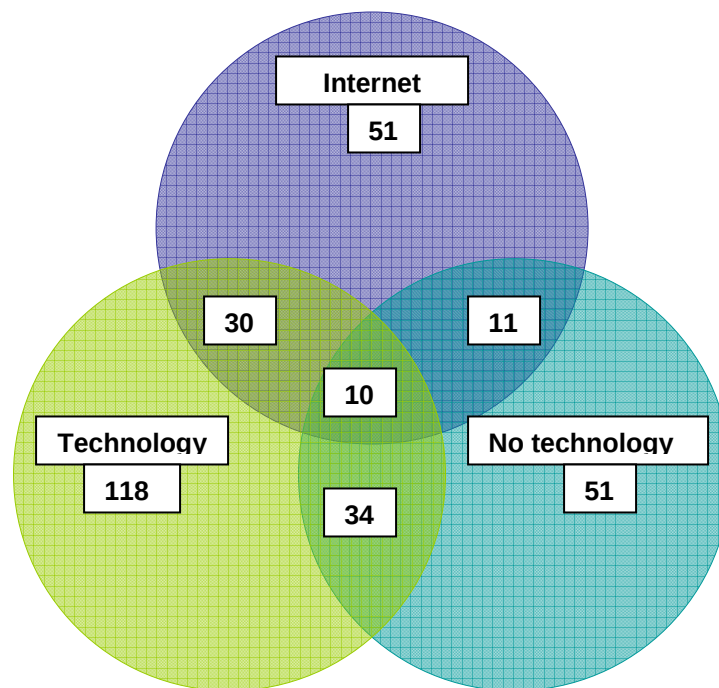
As shown in Figure 25, in 41% (212) of the cases, there was no use of the Internet, technological devices, or non-technological means. In 51 of the cases (9.9%) the offenders used the Internet in some manner, but did not use any other technological devices or non-technological means. In 5.8% (30) the Internet and technological devices were used. All three – Internet, technological devices, and non-technological means were employed by offenders in only ten cases (1.9%). Technological devices, without the use of the Internet or non-technological means, were used in 118 cases (22.8%).

Figure 25. Offender Methods

Method Category	N	Percent
Internet only	51	9.9%
Technological Devices only	118	22.8%
Non-technological Means only	51	9.9%
Internet and Technological	30	5.8%
Internet and Non-technological	11	2.1%
Technological and Non-technological	34	6.6%
Internet and Technological and Non-technological	10	1.9%
None of the above	212	41.0%
Total	517	100%

It is interesting to note, as graphically depicted in Figure 26, that offenders used the Internet and/or other technological devices in approximately half of the cases (49.1%). In 50.9% (263) no Internet or technological devices were used. However, in 51 of those cases, offenders used non-technological means to facilitate their crimes.

Figure 26. Interrelationships among Methods



Offender Methods: Internet Alone

The defendant in this case employed pharming to create duplications of an opera house website in at least 9 cities worldwide. When customers attempted to purchase opera tickets, the defendant captured their personal identifying information – names, addresses, phone numbers, and credit card numbers. The customers either received tickets at a higher cost or to a performance other than the one they requested. Some customers did not receive tickets.

Utilization of Methods by Offenders***Internet***

There were 102 cases that included the use of the Internet. Unspecified Internet use occurred most frequently – in 51 cases. It was used to search databases in 27 cases, for e-mail in 16 cases, and for online identification document purchase and/or sale in 19 cases. In some cases more than one method of Internet use was used and therefore, recorded during data collection. For that reason, the number of uses totals more than 102.

Technological Devices

Technological devices, including computers and the other items listed above, whether used alone or in conjunction with the Internet and/or non-technological means, were used in 192 cases. Computers were most frequently used for producing documents – in 106 cases. They were used for scanning documents in 62 cases and for unspecified purposes in 93. Computer printers were used in 68 cases for producing documents, checks, and currency. Other frequently used technological devices were photocopiers (31 cases), telephone (31), and other, including access device readers (28). Again, there were combinations of computer uses and of computers and other technological devices in some of the cases, so the numbers total more than 192.

Using Computers to Produce Documents

The defendant procured personal identifying information by placing ads in newspapers stating that he was hiring and would accept applications at a local hotel. He would interview the individuals and collect their applications which included Social Security numbers, dates of birth, and bank account information for direct deposit of a payroll check. He would then create birth certificates and employment cards on a computer and use them to get driver's licenses with his photograph and others' names. He used the driver's licenses to open bank accounts. He then manufactured counterfeit checks with the victims' names on the computer.

Non-technological Means

Non-technological means, including mail theft, mail rerouting, and dumpster diving were used in 106 cases. The most frequent of these was the rerouting of mail through change of address cards and change of address for credit cards

and bank accounts. It occurred in 62 cases. Mail theft was an element of 46 cases and dumpster diving was employed in 12 cases. Again, these means were used in combination in some cases, so the numbers total more than 106.

Patterns of Offender Methods

The data was examined to track variations in the use of the Internet, technological devices, and non-technological means according to the year in which the case was opened. The Secret Service opens cases once they have been referred to them and accepted. The year the case is opened is generally the year in which the crime was detected.

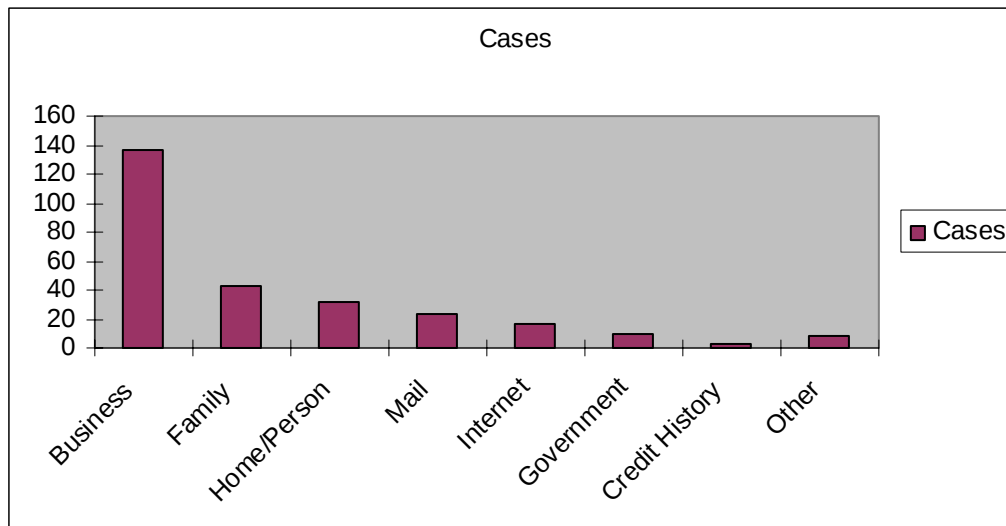
Unfortunately, any trending analysis is premature, as there are very few 2005 and 2006 closed cases. A continuation study is planned that will collect the necessary data to provide for this level of analysis. The following preliminary findings were observed.

- There is very little variation in the use of the Internet to commit identity theft from 2001 through 2004. The data indicate that in approximately 20% of the 2001–2004 cases the Internet was used.
- An interesting pattern in the use of technological devices was observed during a similar time period. There is a steady decline in the use of technology other than the Internet in the cases opened between 2001 and 2004. In 2001 42.2% (27) of the cases involved the use of a technological device. That number dropped to 30% (17) in 2004. The decrease was steady in the intervening years: 38.5% (60) in 2002 and 34.8% (46) in 2003.
- The use of non-technological means remained fairly steady across the 4 years (2001-2004). The percentages were in the low twenties for this period. Offenders continued to use low-tech means such as mail theft, mail rerouting, and dumpster diving, but only in a small percentage of the cases. It should be noted that in some cases, the non-technological means were used in combination with the Internet and/or other technological devices.
- The limited data provided by closed 2005 and 2006 cases indicate the potential for shifts in the patterns above. However, the numbers are too small to draw any conclusions at this time.

Points of Compromise

The case summaries were analyzed to discern the point of compromise or vulnerability at which personal identifying information was stolen. Such a point could be discerned in 274 of the cases. As Figure 27 shows, businesses (all business: service, retail, financial industry, corporations) accounted for 50% (137) of all the cases in which a point of compromise could be identified. When compared to Figure 23, this number is lower than the number of cases involving identity theft through employment at private companies, insurance, retail business, the credit card industry, the service industry, and banks and financial institutions, which when added together total 161. There are two reasons for this: 1. In some cases the researcher indicated that the identity theft occurred through employment, but did not mention it in the paragraph describing the offense and investigation; and 2. While the identity theft may have occurred at the offender's place of employment, the theft may have been from a co-worker, not from the business. The next highest category is family, which for this analysis includes friends, as well. In 15.69% (43) of the cases, a family member or friend was the victim of identity theft. The personal identifiers were stolen from a home, car, or person (wallet, pocketbook) in 11.68% (32) of the offenses. Theft from mail occurred in 8.76% (24) and through the Internet in 6.20% (17) of the cases. Other includes well-known public people and crimes in which the victim participated in the criminal activity.

Figure 27. Points of Compromise for Identity Theft



Point of Compromise: A Business

This case originated when a bank fraud investigator contacted the Secret Service. The defendant was employed at a candy store and was terminated for stealing cash from the register during transactions. He also skimmed credit cards while employed there. Two major credit card issuers identified the business as a common purchase point for credit cards that were later used as counterfeit credit cards. The defendant admitted that he was paid by another person to skim the credit card numbers. The other person then used them to produce counterfeit credit cards which he sold with corresponding counterfeit identification documents.

Point of Compromise: A Family Member

The victim in this case notified the Secret Service regarding the fraudulent use of her identity. Her ex-husband used her information to open two American Express card accounts and make charges to them. The defendant completed the credit card applications via the Internet.

The Commission of the Offense in Summary

Identity theft or fraud and larceny/theft were the offenses most frequently facilitated by identity theft. The majority of the cases did not involve insiders; most did not involve identity through employment. However, the point of vulnerability for identity theft was a business in half of the cases in which such a point could be discerned. In most of the cases, the offense(s) was committed by a single individual. The individual was most likely to steal or obtain personal identifying information and use it for his or her own use. In cases with more than one defendant, the most common roles were also stealing or obtaining personal identifying information and using it for personal gain. The methods used to commit the offenses included the Internet, other technologies, and non-technological means. The Internet use was unspecified in most of the cases in which it was involved. Computers were used most frequently to produce fraudulent documents. The most common non-technological method use was change of address.

Victimization

The Victims

Data was collected and categorized concerning who or what the victim of the identity theft or fraud crime was. The categories include:

- Individual (people)
- 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 (federal, state, and local)
- Credit Bureau
- Insurance (life, car, property, casualty, health)
- Education (public and private, all levels)
- Unavailable (There was no indication of the victim in the file.)

In some cases, more than one type of victim was identified. Therefore the total number of victims included in the 9 categories is 1102. For example, if a defendant stole personal identifying information by accessing computer records at the bank where he worked and used that information to open credit card accounts, the bank, the individuals, and the credit card company would all be victims.

As Figure 28 shows, the largest percentage of victims was the financial services industry – 37.1% (409). The next largest group of victims was individuals – 34.4% (379). 21.3% (234) of the victims were retail establishments.

Figure 28. Victims by Category		
Category	N	Percent
Financial Services Industry	409	37.1%
Individual	378	34.3%
Retail	234	21.3%
Government Agency	38	3.4%
Credit Bureau	7	.6%
Insurance	7	.6%
Education	5	.5%
Unavailable	24	2.2%
Total	1102	100%

Methods of Victimization (other than individuals)

There are many ways in which the financial services industry was victimized. The most prevalent methods were using fraudulently obtained personal identifying information (FOPII) to obtain new credit card accounts, using FOPII to change credit card accounts (names, addresses, credit limits), applying for and obtaining fraudulent loans, using FOPII to open bank accounts, using FOPII to transfer funds from and between bank accounts, and uttering bad, forged or counterfeit checks using fraudulent identification documents. Figure 29 shows the frequency with which these occurred and the percentage of the cases in which they occurred. It should be noted that more than one of these could occur in the same case, so the numbers total more than the 409 cases in which financial services were victimized. For example, in one case the defendant used an individual's genuine Social Security number to procure an automobile loan and to open several credit card accounts. The percentage is based on the 517 cases in the study.

Figure 29. Methods of Financial Services Industry Victimization

Method Category	N	% of Cases
Use FOPII* to obtain new credit card accounts	200	38.7%
Fraudulent loans and loan applications	105	20.3%
Utter bad, forged, counterfeit checks using fraudulent identification	97	18.8%
Use FOPII* to open bank accounts	55	10.6%
Use FOPII* to change credit card accounts	54	10.4%
Use FOPII* to transfer funds	28	5.4%

*FOPII=fraudulently obtained personal identifying information

Victimization of Financial Services Industry

In a case brought to the attention of the Secret Service by a bank fraud investigator in 2004, the defendant used his deceased's father's Social Security number and name to obtain three loans and a credit card from the bank. He secured a vehicle loan from another bank and paid it off with a loan from a third bank, which he obtained with the same identifiers. He opened checking accounts using the fraudulent information at each of the banks. He admitted using a false income tax form to show income high enough to qualify for the loans. The defendant confessed that he used his father's Social Security number and name to open all of the accounts and credit cards, and to apply for the loans. At the time of this criminal behavior, he was a resident of a halfway house on supervised release for a prior federal criminal conviction for financial fraud. He pled guilty to Social Security Fraud (42 USC 408(a)(7)(b)) and was sentenced to two years of incarceration, three years of probation, and \$64,000 in restitution.

The retail industry was also victimized by opening credit card accounts, as new credit card accounts include both store accounts and accounts such as MasterCard and Visa. Other methods of victimization include purchasing merchandise with fraudulent credit cards and purchasing merchandise with fraudulent credit cards and returning it for cash or store credit. Methods of government agency victimization included uttering stolen U.S. Treasury checks and bonds using fraudulent identification documents, using FOPII to collect entitlement payments, and using FOPII to file income tax returns and get refunds.

All of these industries were vulnerable to victimization through employees stealing customer or client records to gain access to personal identifying information. The section on identity theft through place of employment shows that the financial services industry and the retail industry were most frequently victims of employee theft of personal identifying information.

Offender Relationship to Individual Victims

It is stated in the President's Identity Theft Task Force report that "identity thieves have been known to prey on people they know, including coworkers, senior citizens for whom they are serving as caretakers, and even family members" (April 2007, p. 12). In collecting data for this research project, special attention was paid to the relationship between the offender and victim. The categories into which the relationships were classified include:

- Stranger (The victim had never met the offender.)
- Customer/Client (includes retail customers, client lists, and the like)
- Family (immediate and extended – spouses, parents, siblings, grandparents, aunts, uncles, nieces, nephews, cousins)
- Friend/acquaintance
- Co-worker/employer
- Unavailable (There was no indication of the victim – offender relationship in the file.)

Because in many cases there was more than one defendant and/or more than one victim, the number of relationships found is 909 among the 517 cases that were examined. For example, in one case the five defendants used credit cards belonging to one defendant's parents to obtain new credit cards. They made false identification documents in the names of that defendant's parents. One defendant also stole mail to gather personal identifying information. In that case, one offender-victim relationship is family. Since the four others were acquainted with his parents, the offender – victim relationships there are friend/acquaintance. Because the defendant who stole the mail did not know those victims, that relationship is stranger.

Figure 30 shows that the majority of offender – victim relationships involved an individual or individuals whom the offender did not know. Out of 909 relationships, 59.4% (540) were categorized as stranger. The next most frequent relationship (other than those which were not indicated in the files) was customer/client. In 10.5% (95) of the relationships, the offender victimized an individual who had been a customer or client at his or her place of employment. Family relationships accounted for 5% (46). The offender victimized a friend or acquaintance in 3.1% (28) of the relationships. (These numbers differ from those shown in the point of compromise analysis. The family category in that analysis includes family, friends, coworkers, and employers. Here, while they were the victims, they were not necessarily the point of compromise.) The numbers are the same for relationships between the offender and a co-worker or employer.

Figure 30. Offender and Victim Relationships		
Category	N	Percent
Stranger	540	59.4%
Customer/Client	95	10.5%
Family	46	5.0%
Friend/Acquaintance	28	3.1%
Coworker/Employer	28	3.1%
Unavailable	172	18.9%
Total	909	100%

As the President's Identity Theft Task Force reported, identity thieves often prey on people they know, but in most of the Secret Service cases they did not. However, there were cases of offenders taking advantage of the people for whom they were caring – both disabled and elderly, as well as cases in which spouses, parents, children, and extended family members were victimized.

Offender-Victim Relationship: Caretaker-Employer

In this case, the defendant was employed by a blind man who owned a management company. The defendant, a white female in her forties, embezzled over one million dollars in approximately three and a half years. Her employer trusted her implicitly and signed whatever documents she directed him to. Thus, she was able to make purchases, bill them to her employer, and pay for them from his personal checking account. She issued checks from his account, which he signed, to pay her personal bills, including credit cards, tuition, vacations, medical expenses, clothing, jewelry, insurance policies, and home improvements. She used his date of birth and Social Security number to obtain unauthorized credit card accounts in his name and requested a second card for the accounts in her name. She also changed the address on the cards to her own. She used wire transfer and computer generated checks on his revocable trust and limited partnership checking accounts to pay the credit card bills.

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 pursuing 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 losses 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:
DEFENDANT(S):

CASE #

	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