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

Exhibit J

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.

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

List of Figures

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.

<u>The Case</u>:

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.

    - The roles that the defendants took varied, but most frequently involved stealing or obtaining personal identifying information and using it for personal gain.
    - 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.
    - 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.
    - 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.
    - In 50% of those cases a business (service, retail, financial industry, corporation) provided the point of compromise or vulnerability.
    - 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.
    - 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%
    - Private corporations were vulnerable to insider identity theft in about 20% of those cases.

<u>Victimization</u>:

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:
    - 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.

    - 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.
    - 59% of the victims did not know the offenders.
    - 10.5% of the victims were customers or clients of the offender.
    - 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.
    - Of those offenders, 59.7% were employed by a retail business.
    - 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. USPIS, 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
  - Gender
  - Age
  - Race
- Arrest History
  - 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
  - Utilization of methods by offenders
  - 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

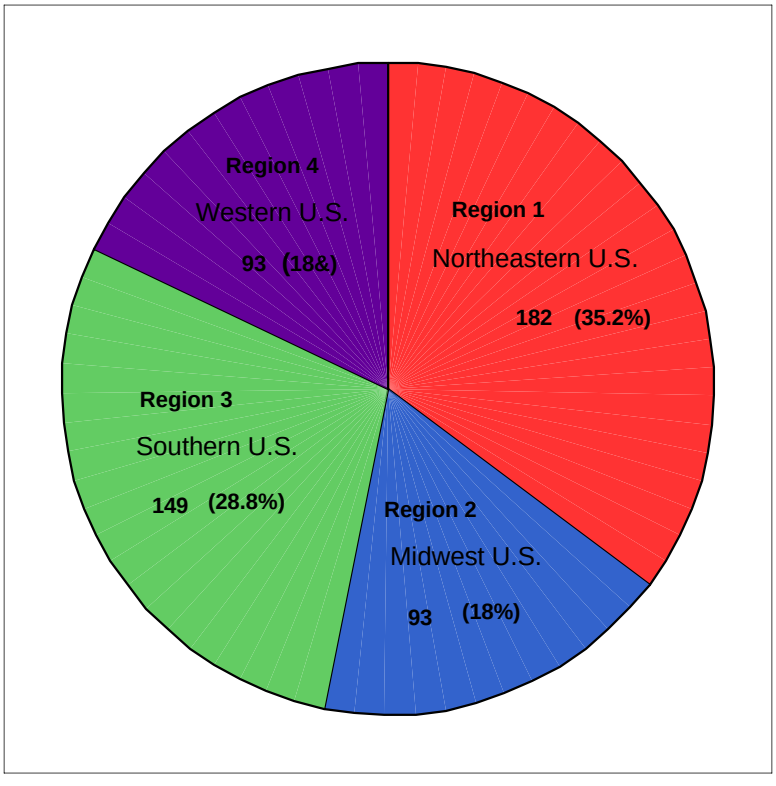
Secondary Case Type Description	Frequency	Percent
Identity Fraud	451	87.2
Significant Commuity Impact	264	51.5
Crimes Involving Use of Evolving Technology	163	31.5
Domestic Multi-District	100	19.3
Counterfeit State Drivers Licenses	70	13.5
All Other Non-Prioritization Investigations	67	12.9
Organized 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
Conterfeit 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 up18% of the total. None of those was from the Far East.

Figure 3: Secret Service Regions

N=517



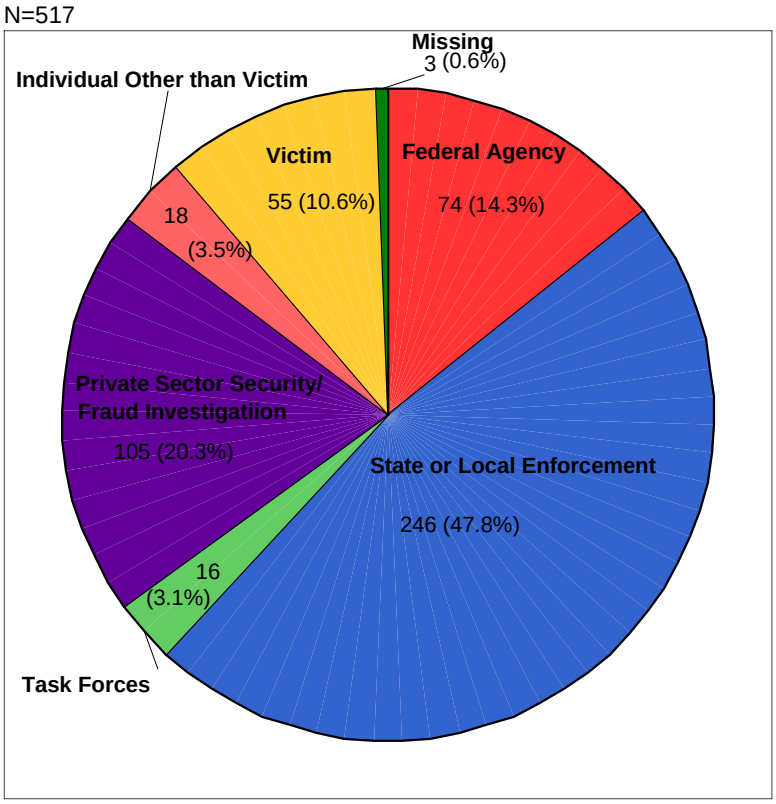
Case Referral

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
  - Includes anonymous tip, attorney, defendant turning himself in, confidential informant, private investigator, witness
- Local or state law enforcement agencies
  - Includes local and county police departments, local and county sheriff's offices, state police, district or state attorney
- Federal agencies
  - Includes Secret Service headquarters, field or regional offices, FBI, DEA, ATF, etc.
- Task forces
  - Counterfeit Crimes
  - Economic and Identity Crimes
  - Electronic Crimes
  - Financial Crimes
  - Identity Theft
  - Organized Crime
- Private sector security/fraud investigation
  - 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



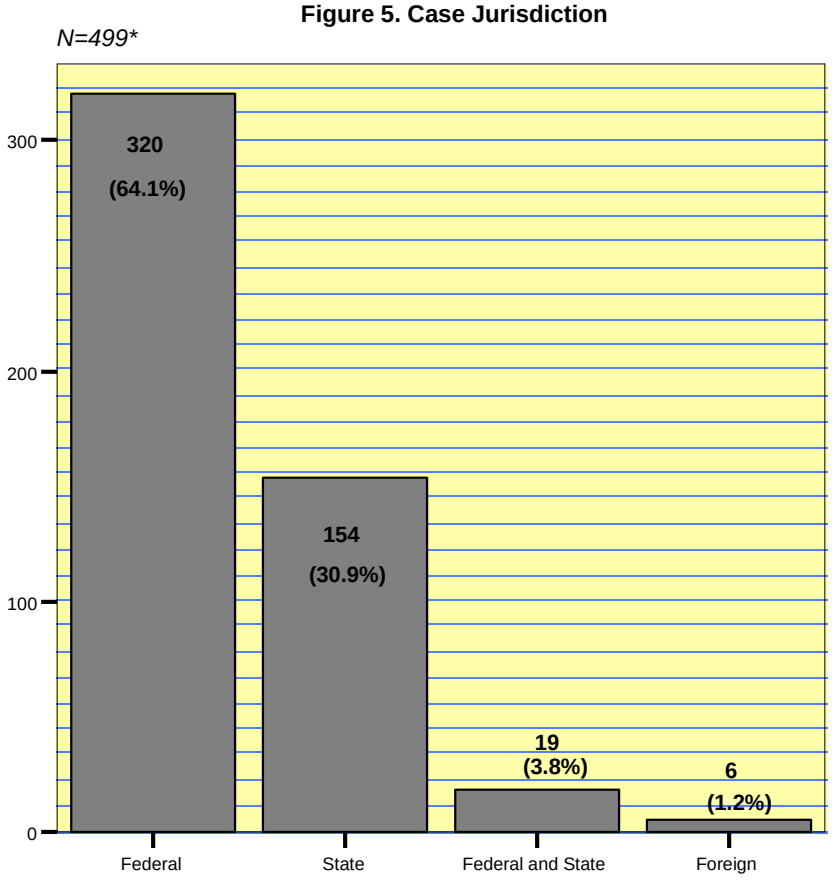
Case Referral: Local Law Enforcement

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.

Figure 5. Case Jurisdiction



**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

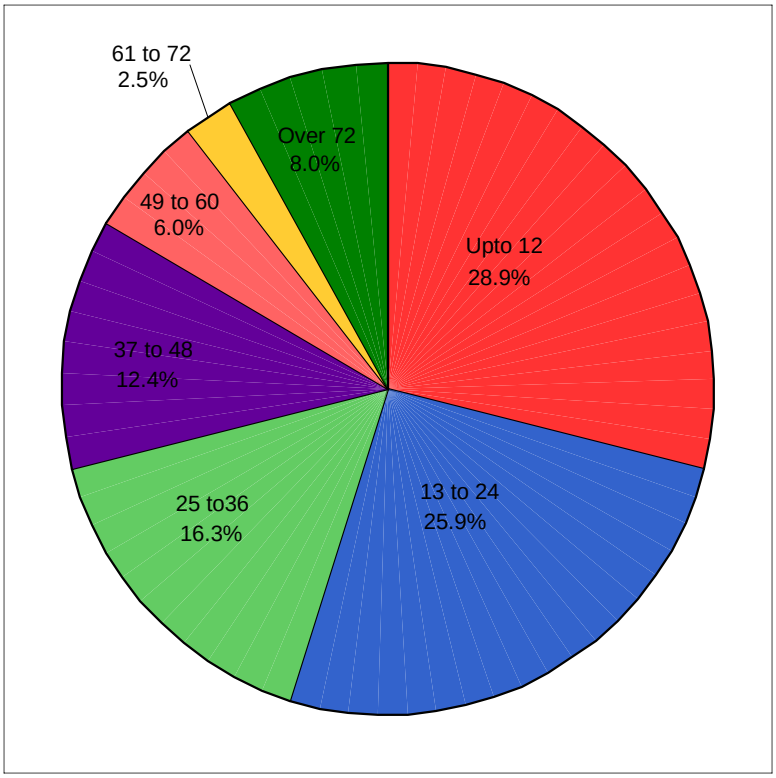
	N
Identity Theft/Fraud	82
Theft/Larceny/Stolen Property	69
Forgery	61
Credit Card Fraud	55
Bank/Check Fraud	17
Unspecified Fraud	13
Conspiracy/RICO	11
Criminal Impersonation	10
Drugs	10
Counterfeiting	7
Computer Crime	6
Miscellaneous	6
Tampering	6
Weapons	4
Assault, Violent Crimes	2

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*



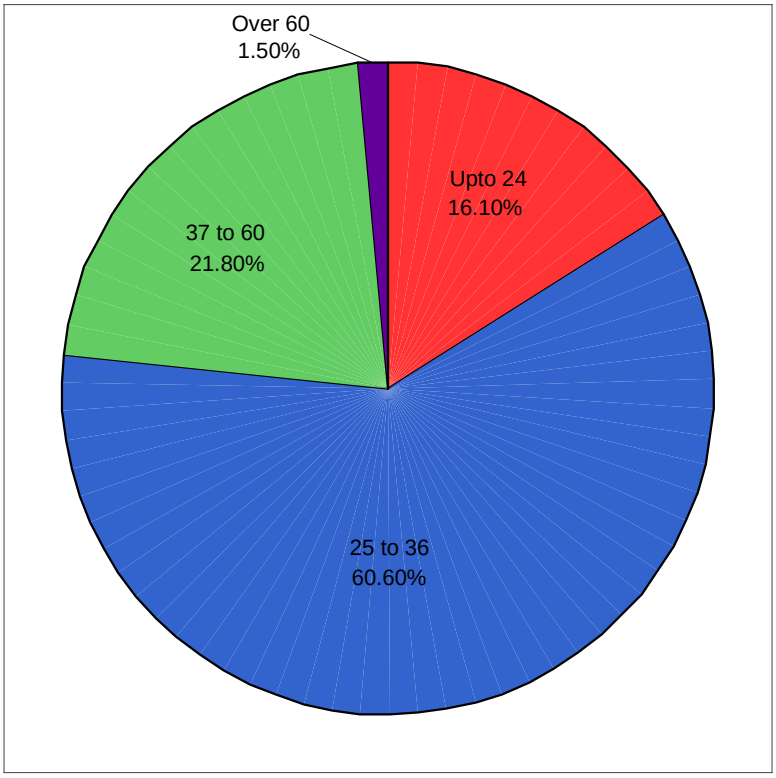
* 43 unspecified cases are excluded

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

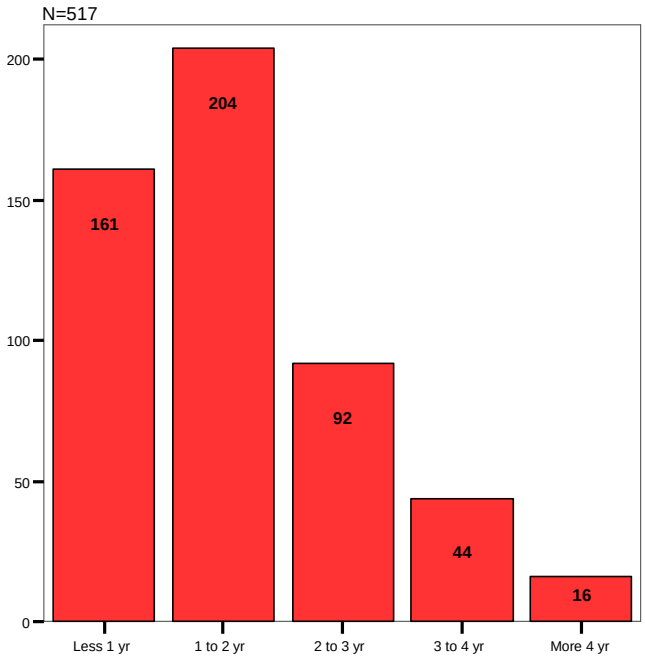
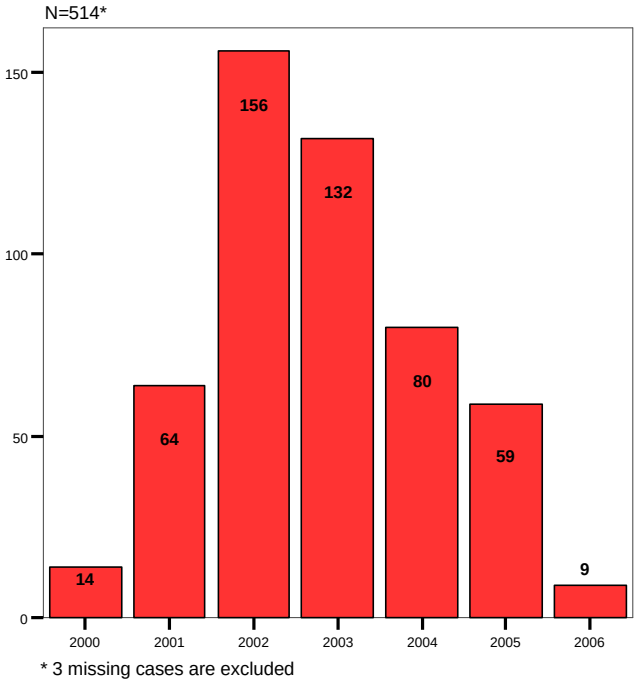


Figure 13. Year the Case Opened

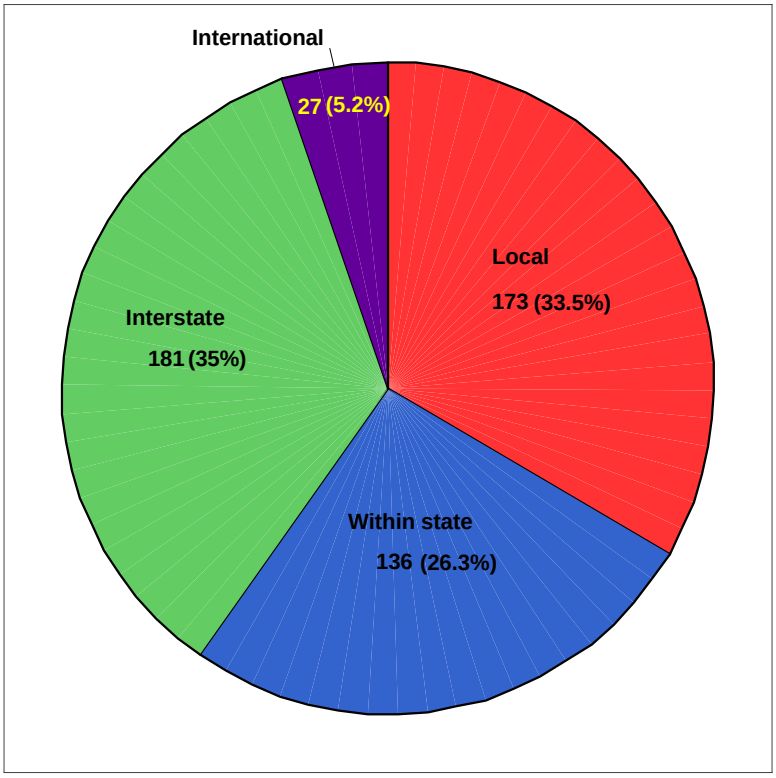


Geographical Scope

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

N=517



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%
		Subtotal 930[a]	100%*
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%
		Subtotal 817[b]	100%*
Race	White	332	38.3%
	Black	467	53.8%
	Hispanic	42	4.8%
	Asian	27	3.1%
		Subtotal 868[c]	100%*
Arrest	Yes	267	29%
	No	655	71%
		Subtotal 922[d]	100%*

* % 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

			Gender		
			Male	Female	Total
Race	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		
			Male	Female	Total
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				
			White	Black	Asian	Hispanic	Total
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		
			Yes	No	Total
Race	White	Count	84	245	329
		% within Race	25.5%	74.5%	
		% within Arrest	32.7%	40.7%	
		% of Total	9.8%	28.5%	38.3%
	Black	Count	151	310	461
		% within Race	32.8%	67.2%	
		% within Arrest	58.8%	51.5%	
		% of Total	17.6%	36.1%	53.7%
	Asian	Count	4	23	27
		% within Race	14.8%	85.2%	
		% within Arrest	1.6%	3.8%	
		% of Total	.5%	2.7%	3.1%
	Hispanic	Count	18	24	42
		% within Race	42.9%	57.1%	
		% within Arrest	7.0%	4.0%	
		% of Total	2.1%	2.8%	4.9%
Total		Count	257	602	859
		% of Total	29.9%	70.1%	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 N	Responses Percent	Percent of Cases
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