The New Face of Identity Theft:

An Analysis of Federal Case Data for the Years 2008 through 2013

November 2015

Donald J. Rebovich, Ph.D.,
Executive Director, CIMIP

Kristy Allen
Research Analyst, CIMIP

Jared Platt
Research Assistant, CIMIP

Center for Identity Management and Information Protection
Utica College

This project was supported by Grant No. 2009-D1-BX-K019 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

The authors extend their thanks to the Bureau of Justice Assistance for providing funding, guidance, and direction. The administration of Utica College provided support and grant management.

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 board of advisors is 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.. CIMIP's advisory board consists of the U.S. Secret Service, U.S. Marshals Service, Florida Highway Patrol, U.S. Postal Inspection Service, ID Analytics, Document Security Systems, Tascet,Aveksa, Strategic Information Resources, Keeping IDentities Safe/Coalition for a Secure Driver's License, Triad Biometrics, University of Alabama at Birmingham, University of Massachusetts at Lowell, and University of Texas at Dallas. To learn more about CIMIP, visit www.cimip.org

.

Table of Contents

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 the increasing number of identity theft and fraud cases committed against individuals and organizations in the U.S. As a result of this study of closed United States Attorney Office identity theft/fraud cases (2008-2013), empirical data concerning the way in which criminals are adapting to law enforcement investigative methods by designing new means for committing such crimes are available to law enforcement agencies and corporate security and fraud investigators.

The study is intended to serve as a follow-up to CIMIP's first study in this area published in October of 2007, *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement* (2007, Gordon, Rebovich, Choo and Gordon). One of the goals is to, where possible, compare results from this study with those of the 2007 study to assess the degree to which characteristics of identity fraud have remained consistent or have changed over time.The analysis will help enable law enforcement to move from a reactive posture to a proactive one. The purpose of this project is to provide law enforcement and policy makers with a proactive means of combating identity theft and fraud and enhancing the response to reports of victimization.

The data for the study was collected from open source information available on United States Attorney Office identity theft prosecutions. Twenty four hundred and fifty two (2,452) offenders involved in 1,306 cases with an identity theft component, which were prosecuted between 2008 and 2013, were reviewed; data was analyzed on 1,395 convicted offenders (involved in 844 cases), as the other indicted offenders were excluded due to lack of conviction disposition.

General 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 the state of judicial jurisdiction, and the crimes committed.

- Of the offenders convicted, the vast majority were convicted on charges of "Identity Theft" (89.1%)
- In terms of frequency, this was followed by offenders convicted on charges of "Bank Fraud" (22.6%) and "Tax Fraud" (16.7%)

- The highest percentage of offenders from a single state was from Florida.
- The second highest percentage of offenders from a single state was from California.

The Offenders:

The data analysis showed the following with regard to offender age, gender and legal status.

- *In general, identity criminals were found to be older than those in the study conducted by CIMIP in 2007. Percentage increases in the age ranges of 35 to 49 and 50 and older were noteworthy.*
  - The 25-34 age group made up 36.7% of the offenders Compared to 42.5% in the 2007 study; a decline of over 6%.
  - The 35 – 49 age group made up 40.3% of the offenders.The 35 – 49 age group made up 33% of the offenders in the 2007 study demonstrating an increase of 6%.
  - A marked change from the 2007 study was for the offenders between18-24. In the present study, 9.1% were between the ages of 18-24. In 2007, offenders in this age range accounted for 18.5% of the offenders. For this age range, the 2015 findings represented a decline of close to 10% since 2007. As a proportion of total offenders by age, identity crimes committed by offenders in this age range have declined by close to half.
  - Another marked change was in the category of oldest offenders. For the present study, 13.9% were 50 years old or older. 6% were 50 years old or older in the 2007 study, representing a rise of over 8% for this age bracket. In terms of a proportion of the total number of offenders, this represents more than double the percentage of offenders for this age range since 2007.
- 86.7% of the offenders were of legal status born within the United States; 7.2% were Foreign but of legal status, and 6.1% were Illegal. The legal status was unknown for 24 offenders.
- One third of the offenders were female. Approximately two-thirds were male, consistent with findings from the 2007 study.

The Commission of the Crime:

The data was examined to determine the modus operandi of the offenders, the points of compromise, and identity theft through employment.

- *More identity criminal criminals were found to be operating as part of criminal groups rather than by themselves, a departure from the 2007 CIMIP study*.

- Just under two thirds (63.6%) of offenders were found to commit their criminal acts in collaboration with other offenders (i.e., group offenders). 36.4% were classified as committing their crimes alone. In the earlier 2007 study, only 42.4% teamed with other criminals to commit their acts as part of a criminal "group while the majority (57.6%) operated alone.

- *The study results demonstrated that identity criminals are leaning more toward the use of technological means (e.g., computers) and the Internet to commit their crimes..*

- Cases in which Internet and/or technological devices *were* used rose from (49.1%) in the 2007 study to (62.84%) in the 2015 study.
  Cases in which the Internet or technological devices *were not* used dropped from (50.9%) in the 2007 CIMIP study to (36.16%) in the 2015 study.

- The point of compromise for stealing personally identifying information or documents was determined for 466 offenders*. A notable change in pattern from the 2015 CIMIP study is the decrease of the percentage of businesses as the point of compromise and the increase of the percentage of cases in which other points of compromise were exploited (e.g., the Internet, individuals, mail) focusing on individuals rather than businesses.* The percentage of those offenders with an identifiable point of compromise is below:

- 21.9% of the offenders used a business as the point of compromise*. This is a sharp decline from over 50% of cases in which businesses were a point of compromise in the 2007 CIMIP study*. This sharp decrease may hint that criminals are turning to commit identity fraud crimes by accessing the vulnerabilities of other points of compromise (mail, home/person etc.).

- *Mail as a point of compromise increased from (8.76%) in the 2007 study to (21.7%) in the 2015 study*. This rise in the percentage of cases involving mail may indicate that some identity criminals are shifting their offense methods to the use of the mail system.

- *The cases regarding the involvement of “insiders” (i.e., those in the workplace who criminally exploit their access to sensitive personal information to steal/sell such information) have declined since the 2007 CIMIP study.* The involvement of an insider occurred in 27% of the total cases in the 2015 study. This is a drop of approximately 7% from the 2007 study (34.1%). The types of employment were categorized in the same way as victims.

- Like, the 2007 CIMIP study, the plurality of insider cases involved the retail industry (stores, car dealerships, gas stations, restaurants, etc.).
  and the percentages were similar in the two studies (2015 – 44.7%; 2007 – 43.8%).

- A change was evident in the second highest percentage category, though. In the present study, it was the medical industry (20.6%), while in 2007 it was private corporations (20%).

- For the 1,395 convicted offenders in the study, the plurality (418, 30%) stole personal identifying information (PII) that was then converted into false identification for the offenders to commit fraud-related acts. Information stolen in these cases included Social Security numbers, dates of birth, birth certificates and Medicare identification numbers.

- The second highest offense commission category was banking/financial (313, 22.4%). These methods included false applications for credit cards, use of counterfeit credit cards, stolen credit cards, stolen bank account information and the passing of counterfeit checks.

- *The third highest category proved to be false claims with the IRS using stolen ID information (234, 16.7%), a type of offense that was relatively rare in the 2007 study results*. Offenders used a variety of approaches to commit these types of offenses. The cases involved stealing source information from a variety of sources, including prisons and entities that housed personal information of the elderly (some residing at nursing homes). In some cases, the source information for false claims for tax refunds was obtained through insiders (e.g., a nurse at a hospital). Criminal versatility was often an element in identity theft/tax return fraud with one group setting up a fake tax preparation firm to lure victims in. In identity theft/tax return cases, the trading of information between criminal groups was not uncommon.

Victimization:

- While the most common industry victimized was that of the financial services industry (24.2% of the total number of victims) this represented *a double digit drop from the 2007 CIMIP study (37.7%)*. *Even though it has declined, the financial services industry still represents nearly 1 in 4 of identity theft cases*

- *Conversely, the percentage of individuals as victims rose over 14% from the 2007 study (from 34.3% in 2007, to 48% in 2015).*

- *The percentage of cases that were committed by strangers to the victims remains consistently high*. 60.1% of offenders were strangers to their victims in the 2015 study compared to 59% in the 2007 study. This lack of significant change over time indicates that stranger-based identity crime represents an unrelenting threat to the general public.

- In the 2015 study, the second most common relationship between offenders and victims is that of customer/client - 15.5% (up from 10.5% in 2007).

Introduction

In October, 2007, the Center for Identity Management and Information Protection (CIMIP) at Utica College published its report on the state of identity theft and identity fraud in the U.S. That study was funded through the Bureau of Justice Assistance of the U.S. Department of Justice, and was designed to reveal key characteristics of identity crime cases; common characteristics of the crimes, the criminals and the victims of these offenses. The study was an exhaustive analysis of disposed United States Secret Service cases with an identity theft component for the period from the year 2000 through the year 2006. Much valuable information was gathered for this research project, one of the first of its kind in the U.S. Information on important factors relevant to the criminal behavior of identity thieves and the conditions under which they operate was made available to the law enforcement community and to the general public.

Eight years have passed since the publication of the first CIMIP report on characteristics of identity crimes. Since that time, identity theft has remained in the spotlight in the U.S. Statistics from the Federal Trade Commission (FTC), has demonstrated the ebbs and flows of this crime area over time. Identity theft complaints have consistently been one of the top complaint categories for the FTC, reaching one peak in 2008. The number of complaints decreased in both 2009 and 2010 before rising again in 2011 and 2012 (Finklea, 2014). On February 27, 2014, the FTC reported that identity theft, once again, topped the FTC’s national ranking of consumer complaints for 2013. It did so again for the year 2014 as reported on February 27, 2015 by the FTC.

But besides knowing the national statistic of victim complaints of these crimes, how much do really know about more detailed specifics of the crimes? Have characteristics of the offenses remained the same since the first focus on this crime area by CIMIP in 2007, of have they changed? And if they have changed, how have they changed? Answering these questions can help us understand variations in crime commission methods, the types of people who commit the crimes and who are the targets of their predatory acts.

To help answer these questions, CIMIP embarked upon a second follow-up study (also funded by BJA) to update the law enforcement community and the general public on what the face of identity theft looks like in 2015. The results of this study and their relevance to identity theft control and prevention is contained in this report.

The report begins with an exploration of the general goals and potential value of the research. It is followed by an account of the empirical research approach taken by this study, including an introduction to the data sources, the data elements collected and the methods of analysis employed. General findings are then presented, representing the primary body of the report. In sequence, results are presented in separate sections regarding characteristics of the overall cases, the offenders, how the crimes were committed (including vulnerability points that criminals exploit), and, finally, the victims themselves. The report concludes with a section on what can be learned from the present study and how that knowledge can be applied to strengthening identity theft control and prevention methods for the future.

Goals and Value of the Study

The analysis of the data will lead to a fuller realization of trends and patterns perpetrating identity theft. It is a step toward what is meant to be a successive series of like endeavors gauging the evolution of identity theft as a distinct crime type. The analysis 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 three goals which are intended to provide the law enforcement community with the robust empirical information necessary to enhance identity theft control and prevention efforts.

Goal: To identify key offender, offenses and victim characteristics of cases involving the commission of identity theft

Goal: To convert the analysis of collected data to the development of an empirically-based profile of identity theft offense, offender, and case characteristics.

Goal: To provide recommendations to the law enforcement community on the effective control and prevention of identity crimes based upon the analysis of collected data.

The Empirical Approach

The primary aim of this project was to perform an exploratory quantitative and qualitative analysis of United States Attorney Office 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.

Source of Data

The data for this study was collected from open source information provided through United States Attorney Office cases with an identity theft component between from the year 2008 through the year 2013. These were cases in which the offenders were charged with federal crimes of identity theft or identity fraud or fit the definition of the wrongful use of another person's identifying information, such as credit card, social security, or driver's license numbers, to commit financial or other crimes. Two-thousand four-hundred and fifty-two offenders involved in 1,306 cases were reviewed. The information available consisted of case/ disposition information accessible through the USAO district websites. Data was collected on all 2,452 of these offenders.

Elements Collected

As the information collected focused on the offenders and the offenses, several demographic and characteristic elements, including gender, legal status, and age were chosen for collection. The characteristics of the offense included the state of judicial jurisdiction, the crimes, and details of the case including the offender type, the offenders’ roles and relationships to the victim, the methods used, 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 process was repeated so that patterns and trends could be discerned and useful information could be provided for law enforcement and corporate security organizations.

Excluded Cases

43.1% of the 2,452 offenders available in the information available were excluded due to the case status. Those excluded were indicted offenders who had not yet been convicted of any of the charges. The factors used to exclude a case were:

- *No discernible connection to identity theft.*
- *Cases that were opened before 2008.*

Data Limitations

The data used in this study was collected from United States Attorney Office cases related to identity theft that were opened and closed between January 2008 and December 2013 and made available on the USAO district websites. This data does not necessarily represent all of the identity theft cases that were investigated and prosecuted during this time period by the USAO. The researchers recognize that there is an unknown figure of identity theft crimes.

Findings

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

The following characteristics of the case were examined:

- The state of judicial jurisdiction
- The crime

The offender characteristics analyzed were:

- Demographics
    - Gender
    - Age
    - Legal Status

- Offender Type

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

- Offender Methods: Internet, technological, and non-technological
- Point of Compromise

Victimization characteristics included:

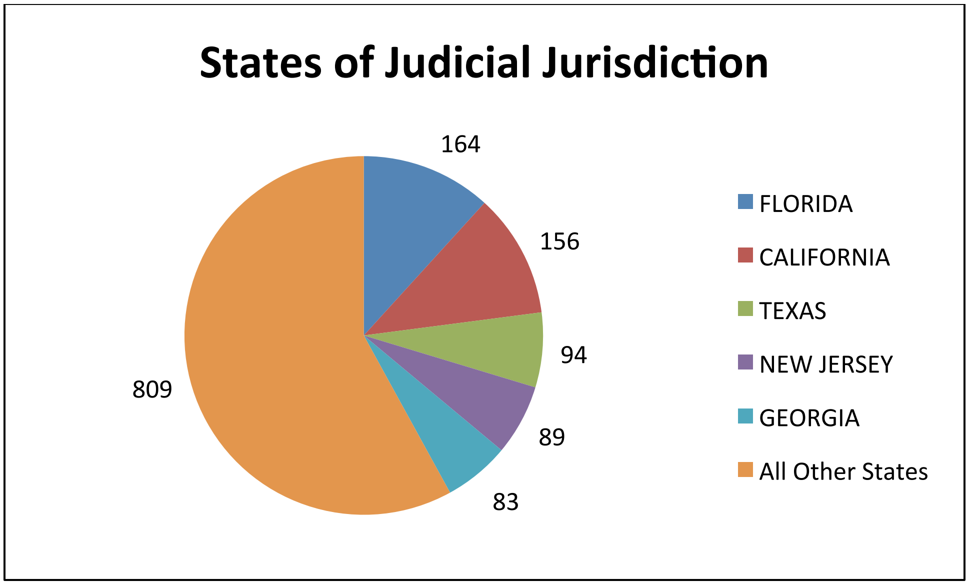
- Victim Categories
- Offender Relationship to Individual Victims

The Cases

States of Judicial Jurisdiction

Data was collected from a total of 42 of the contiguous United States of America and Alaska. Data was collected from each of the individual United States Attorney Office districts within each state. If multiple districts exist within a state then data was represented collectively by the state title for all analytical purposes. A total of 2,452 records have been entered into the database, with a single record being generated for each offender indicted for, or convicted of, an identity theft related offense. In the event that multiple suspects were named in the same indictment, or they were co-defendants in the same criminal case, the same "Case ID" has been used in each record to demonstrate the association between the offenders.

Of the 2,452 total offenders included in the dataset, 1,395 offenders were convicted during the period of study. The 1,395 offenders who were convicted during the period of study serve as the sample of interest for the study. A tabulation of the offenders convicted with identity theft related offenses, for the time period ranging from January 2008 through December 2013 is displayed below. The five states with the largest number of offenders having been convicted during the period of study and the corresponding number of offenders are, in descending order: Florida - 164 offenders, California – 156 offenders, Texas – 94 offenders, New Jersey – 89 offenders, and Georgia – 83 offenders.

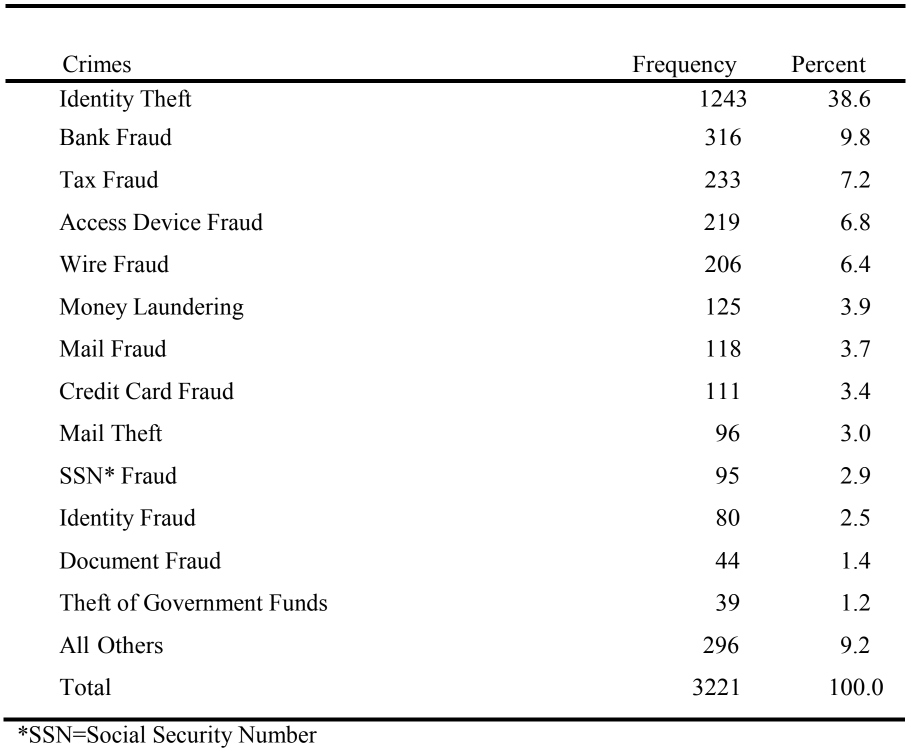


The Crimes Charged

All crimes with which an offender was charged with at least (1) one count and was subsequently convicted have been recorded in the dataset. (The total percentage distribution of what follows totals over 100% due to the presence of multiple charges.)The five most common charges upon which offenders were convicted are, in descending order, “Identity Theft” (1243 of 1,395 offenders → 89.104%), “Bank Fraud” (316 of 1,395 offenders → 22.652%), “Tax Fraud” (233 of 1,395 offenders → 16.703%), “Access Device Fraud” (219 of 1,395 offenders → 15.699%), and “Wire Fraud” (206 of 1,395 offenders → 14.767%). Collectively, the 1,395 offenders who received convictions were charged with a total of 3,221 counts of various crimes.

Figure 1 lists all of the documented crimes and the corresponding crime counts charged. It should be noted that the proportions in this section were calculated based upon the crime count (3,221 crimes), not the number of convicted offenders in the study (1,395 convicted offenders). “Identity Theft” was the crime that convicted offender were most frequently charged with, (38.6%).

Figure 1. Most Frequent Crimes



Crimes	Frequency	Percent
Identity Theft	1243	38.6
Bank Fraud	316	9.8
Tax Fraud	233	7.2
Access Device Fraud	219	6.8
Wire Fraud	206	6.4
Money Laundering	125	3.9
Mail Fraud	118	3.7
Credit Card Fraud	111	3.4
Mail Theft	96	3.0
SSN* Fraud	95	2.9
Identity Fraud	80	2.5
Document Fraud	44	1.4
Theft of Government Funds	39	1.2
All Others	296	9.2
Total	3221	100.0

*SSN=Social Security Number

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, legal status, and age at the time the case was opened.

Gender, Age, Legal Status

Within the 2,452 total offenders included in this study, there were 1,395 convicted offenders. As Figure 2 indicates, 65.9% (911) of the offenders were male. Females accounted for a sizable minority of 34.1% (471).The gender of thirteen of the offenders was not made available. Also included in Figure 2 is the distribution of age and legal status of the offender

The age statistics are based on the age of the offender during the year in which the case was opened. Information on the age of 255 offenders was not made available. The largest percentage of offenders – 40.6% -- were between 35 and 49 years of age (463). The 25-34 age group made up 36.3% of the offenders (414). 8.9% (102) were between 18 and 24 years old. The remaining 14.1% (161) were 50 years old or older. Compared to the 2007 study results, the percentage of those in the youngest and oldest ranges changed the most. The percentage of those making up range between 18-24 decreased by more than half, while the percentage comprised of those 50 and older more than doubled.

The majority of the offenders were of legal status, born within the United States: 86.7% (1,188). Foreign offenders of legal status accounted for 7.2% (99). 6.1% (84) of the offenders were Illegal. The legal status for 24 of the offenders was not made available.

The offenders' characteristics of gender have changed slightly since the 2007 report. The gender percentage from the 2007 report shows that (67.4%) of cases involved males and (32.6%) involved females. When compared to the 2015 report that showed (65.9%) cases involved males and (34.1%) involved females. This represents a slight change of (1.5%) towards females. Even though this is only a negligible difference, it still indicates a progression towards females becoming more active in identity fraud. In the future, if this trend continues on its current rate we will begin to see a shift towards an equal amount of cases involving both men and women.

Figure 2 shows the relationship between legal status and gender among the offenders. Most of the female offenders were legal 93.4% (436). Of all male offenders, 83.2% were legal.

Figure 2. Legal Status by Gender

			Gender		
			Male	Female	Total
Legal Status	Legal	Count	752	436	1188
		% within Status	63.3%	36.7%	
		% within Sex	83.2%	93.4%	
		% of Total	54.9%	31.8%	86.7%
	Foreign	Count	84	15	99
		% within Status	84.8%	15.2%	
		% within Sex	9.3%	3.2%	
		% of Total	6.1%	1.1%	7.2%
	Illegal	Count	68	16	84
		% within Status	81.0%	19.0%	
		% within Sex	7.5%	3.4%	
		% of Total	5.0%	1.2%	6.1%
Total		Count	904	467	1,371
		% of Total	65.9%	34.1%	100.0%*

*% calculation in each variable excludes unknown cases

A more detailed analysis provides some insight into the age at which females are involved in identity theft, as shown in Figure 3. Females tend to demonstrate greater identity theft activity between the ages of 35-49, 47.1% (181). 32.3% (124) of all the females were between 25 and 34 years old in the year the case was opened, while 39.0% (290) of the males fell into that age bracket. 36.7% (273) of males were between the ages of 35 and 49 at the time the case was opened.

Figure 3. Age by Gender

			Gender		
			Male	Female	Total
Age	18-24	Count	64	38	102
		% within Age	62.7%	37.3%	
		% within Gender	8.6%	9.9%	
		% of Total	5.7%	3.4%	9.1%
	25-34	Count	290	124	414
		% within Age	70.0%	30.0%	
		% within Gender	39.0%	32.3%	
		% of Total	25.7%	11.0%	36.7%
	35-49	Count	273	181	454
		% within Age	60.1%	40.9%	
		% within Gender	36.7%	47.1%	
		% of Total	24.2%	16.1%	40.3%
	50+	Count	116	41	157
		% within Age	73.9%	26.1%	
		% within Gender	15.6%	10.7%	
		% of Total	10.3%	3.6%	13.9%
Total		Count	743	384	1,127
		% of Total	65.9%	34.1%	100.0%*

*% calculation in each variable excludes unknown cases

Figure 4 shows the relationship between legal status and age. In the first two age categories, 25-34 and 35-49, the percentages of Legal, Foreign and Illegal offenders are representative of the total percentage of all offenders.

Within the 25-34 age group, among the offenders for whom both legal status and age was known, 36.0% of legal offenders, 46.9% of foreign offenders and 40.7% of illegal offenders were in the age group. The percentages are similar in the next category: 35-49, 40.3% of legal offenders, 36.0% of foreign offenders and 42.4% of illegal offenders were in the age group.

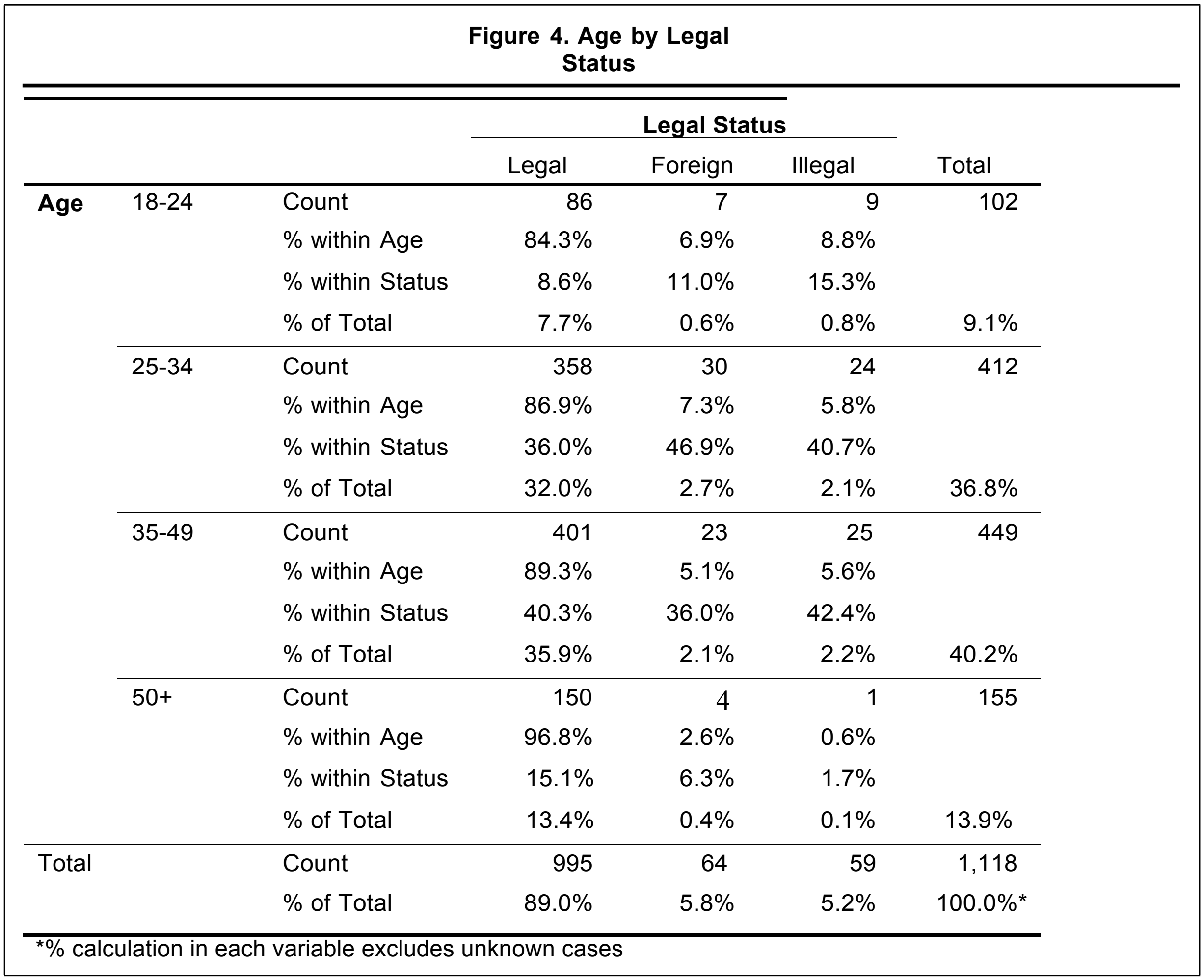


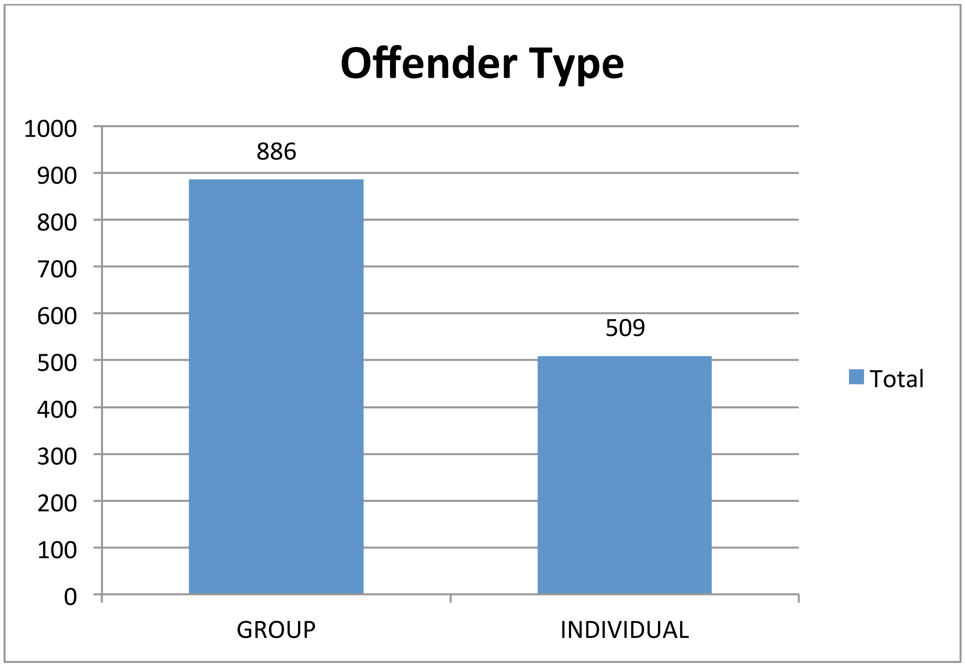
Figure 4. Age by Legal Status

			Legal Status			
			Legal	Foreign	Illegal	Total
Age	18-24	Count	86	7	9	102
		% within Age	84.3%	6.9%	8.8%	
		% within Status	8.6%	11.0%	15.3%	
		% of Total	7.7%	0.6%	0.8%	9.1%
	25-34	Count	358	30	24	412
		% within Age	86.9%	7.3%	5.8%	
		% within Status	36.0%	46.9%	40.7%	
		% of Total	32.0%	2.7%	2.1%	36.8%
	35-49	Count	401	23	25	449
		% within Age	89.3%	5.1%	5.6%	
		% within Status	40.3%	36.0%	42.4%	
		% of Total	35.9%	2.1%	2.2%	40.2%
	50+	Count	150	4	1	155
		% within Age	96.8%	2.6%	0.6%	
		% within Status	15.1%	6.3%	1.7%	
		% of Total	13.4%	0.4%	0.1%	13.9%
Total		Count	995	64	59	1,118
		% of Total	89.0%	5.8%	5.2%	100.0%*

*% calculation in each variable excludes unknown cases

Offender Type

The offenders were classified as one of two types: individual offenders or group offenders (those acting in cooperation with at least one other individual. 63.6% (886) of offenders were classified as group offenders and 36.4% were classified as committing their crimes alone. This finding departs markedly from the 2007 study in which only 42.4% operated in concert with other offenders and 57.6% operated alone. The offender types are displayed below.



Some of the group crime cases involved small groups (e.g., cases involving 2 -4 offenders working in concert). Some were husband-wife teams like the case described below. This was a case that intersected with the methamphetamine trade

Husband-Wife Team

While working narcotics tips, local police were patrolling a local apartment complex when they encountered Offender A. He was in possession of both methamphetamine and a small glass smoking pipe. He also had numerous checks, account statements and IDs belonging to other individuals. A search warrant of the Offender A's residence yielded numerous items of false identification, account statements and checks belonging to dozens of victims. Authorities determined that Offender A worked with Offender B (Offender A's wife) in a sophisticated identity theft scheme to obtain the personal information from unsuspecting victims via stolen mail and other documents, and then used this information to create fake Arizona Driver's Licenses and counterfeit checks. Offender A and Offender B would then cash these fraudulent checks at local businesses. During the three years that they were operating, there were over 180 victims of either identity theft or check fraud, with estimated losses well over $25,000. Neither offender had legitimate employment during this period and both had chronic methamphetamine addictions.

An example of another group crime case that was larger is described below. It involved student loan fraud.

Group Crime – Student Loan Fraud

Four women were indicted used a variety of identities to register for on-line classes at a local college to apply for federal student financial aid in the form of loans and grants. The federal government approved more than $150,000 in funds based on fraudulent applications, with approximately $71,000 having been disbursed. An investigation conducted by the U.S. Department of Education revealed that dozens more fraudulent applications were in the works at the time of the arrests.

The Commission of the Offense

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 and how stolen information was used.

For the 1,395 offenders, the plurality (418, 30%) stole personal identifying information (PII) that was then converted into false identification for the offenders to commit fraud-related acts. Information stolen in these cases included Social Security numbers, dates of birth, birth certificates and Medicare identification numbers.

The second highest offense commission category was banking/financial (313, 22.4%). These methods included false applications for credit cards, use of counterfeit credit cards, stolen credit cards, stolen bank account information and the passing of counterfeit checks.

Banking/Financial Offense

Offender A obtained personal identifying information of numerous people, and used this information to apply for credit cards in the victims' names. Offender A and co-conspirator Offender B used the unauthorized credit cards to purchase gift cards and merchandise at retail stores in the Eastern District of Virginia. Offender A also accessed bank accounts belonging to others.

The third highest category proved to be false claims with the IRS using stolen ID information (234, 16.7%), a type of offense that was relatively rare in the 2007 study results. Offenders used a variety of approaches to commit these types of offenses. The cases involved stealing source information from a variety of sources, including prisons.

Tax Fraud – Multiple Sources

Offender A admitted that between January and April 2011, she conspired with others to defraud the United States by obtaining or aiding to obtain the payment of false, fictitious and fraudulent claims, in particular by filing false tax returns using stolen identities. She admitted that she and others filed at least 155 fraudulent tax returns using stolen identities and sought at least $494,242 in tax refunds. Offender A further admitted that she unlawfully obtained and stored at her home tens of thousands of unlawfully obtained names and social security numbers of actual persons from a multinational business and technology services, prisons and health clinics and used these means of identification to prepare and file false tax returns. According to the plea agreement, she admitted that the fraud loss was between $400,000 and $1 million and that the offenses involved 250 or more victims.

In some cases, offenders were able to cash in over long periods of time through the use of criminal insiders supplying personal information. The case below resulted in significant cost to the U.S. Treasury Department.

Tax Fraud – Conspiracy with Insider

Offender A and Offender B engaged in a large scale identity theft tax fraud scheme that operated over an 18 month period. During the course of the fraud scheme, there were approximately 2,000 fraudulent tax returns submitted to the Internal Revenue Service for payment seeking $11 million dollars in refunds. The Department of Treasury paid out approximately $3.5 million dollars into bank accounts held in the name of and controlled by the offenders, who withdrew approximately $1.9 million in cash. Offender A filed a majority of the fraudulent tax returns from her house and other locations. Offender B filed many of these fraudulent returns using compromised personal identification information obtained from a nurse at a local hospital. Offender B filed several hundred fraudulent tax returns from her house and other locations.

Some criminally creative offenders actually opened up tax preparation businesses to lure in their victims.

Tax Fraud – Tax Preparation Firm

Offender A and others in an identity theft ring were involved with the filing of over 400 fraudulent tax returns using stolen identities. These returns sought at least $2,181,879 in tax refunds. All of the returns had been filed through a tax preparation business which Offender A opened in the name of another individual in order to conceal her own involvement. The indictment alleged that the refunds were often directed to prepaid debit cards and in the plea agreement, Offender A admitted to using a debit card loaded with a fraudulently obtained refund to receive cash.

While some in these tax refund fraud schemes used the identification of victims who were deceased, others preyed upon others living, but, nonetheless, vulnerable, like in the case below.

Tax Fraud - Nursing Home

Offender A conspired with others, to obtain the names and social security numbers of various individuals and to prepare false and fraudulent federal income tax returns for filing with the IRS. Some of these names and social security numbers were of residents at area nursing homes. Names and social security numbers were traded or purchased between co-conspirators. The conspiracy included falsely claiming that taxpayers had been self-employed and had earned income to maximize the refund amount obtained. In all, Offender A's participation in this scheme involved over 40 false tax returns claiming refunds totaling over $135,000.

The fourth highest category here was identity theft perpetrated through the theft of the victim's mail (112, 8%). These offenses were represented by a variety of offender approaches, but most involved simply stealing personal information from unattended mailboxes.

Mail Theft

Offender A and Offender B admitted that they stole checks, credit cards and other mail from business and residential mailboxes in southwest Missouri. They altered and forged the stolen checks by adding the names of other individuals to the payee lines of the stolen checks. They cashed the checks or deposited them into Offender B's bank account. The amount of those checks in the scheme, which lasted over two months, totaled close to $45,000.

Remaining methods were represented by small percentages among a number of diverse categories (e.g., counterfeiting identification documents, forgery) that comprised the general category of "other."

Use of Technology

For this study, researchers also examined the level of the use of technology in the commission of the offenses. 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
    - Phishing
    - Hacking
    - Malware/viruses
    - Online database searching
    - Online ID purchase and/or sale
    - Other (e.g. PayPal accounts, chat rooms, online purchases)
- Technological Devices
    - Computer to file false claims
    - Computer to produce documents
    - Computer to scan documents
    - Device-making equipment
    - Insider Hacking
    - Skimming
    - Cell phones
    - Telephone
    - Computer software to make counterfeit checks
    - File-sharing programs

    - Other
- Non-technological means
    - Mail theft
    - Stolen access devices
    - Recruiting individuals to supply PII

As shown in Figure 5, for 51% (712) of the offenders the use of Internet, technological devices, or non-technological devices was not specified. For 274 of the offenders (19.7%) there was some use of technological devices, but no use of the Internet or non-technological means. 17.7% (247) of offenders used only non-technological means. All three – Internet, technological devices, and non-technological devices were employed by only 2 offenders (0.1%).

It is interesting to note, that when factoring out unknowns (i.e., cases in which the means of commission was not evident in case material) from figure 6, cases in which Internet or technological devices were not used went from (50.9%) in the 2007 report to (36.16%) in the 2015 report. Also, cases in which Internet and/or technological devices were used went from (49.1%) in the 2007 report to (62.84%) in the 2015 report.

When comparing the two reports this shows a (14.74%) decrease in no Internet or technological devices cases and a (14.73%) increase in Internet and/or technological devices cases. This means that cases in which Internet or technological devices cases were not used are decreasing while Internet and/or technological devices cases are increasing.

The data illustrates an upward trend in the rate of Internet and/or technological devices cases. Since the 2007 report, the Internet and technology in general have also illustrated an upward trend of prevalence in our everyday life; unfortunately this includes crime as well. This shift to Internet and/or technological devices based cases is easy to understand due to its positive correlation with our technologically progressing society.

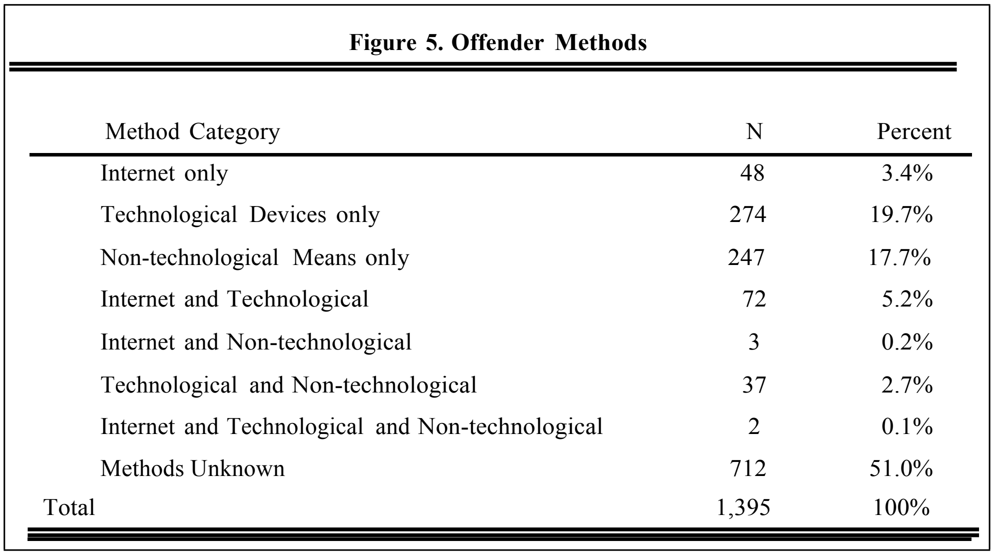
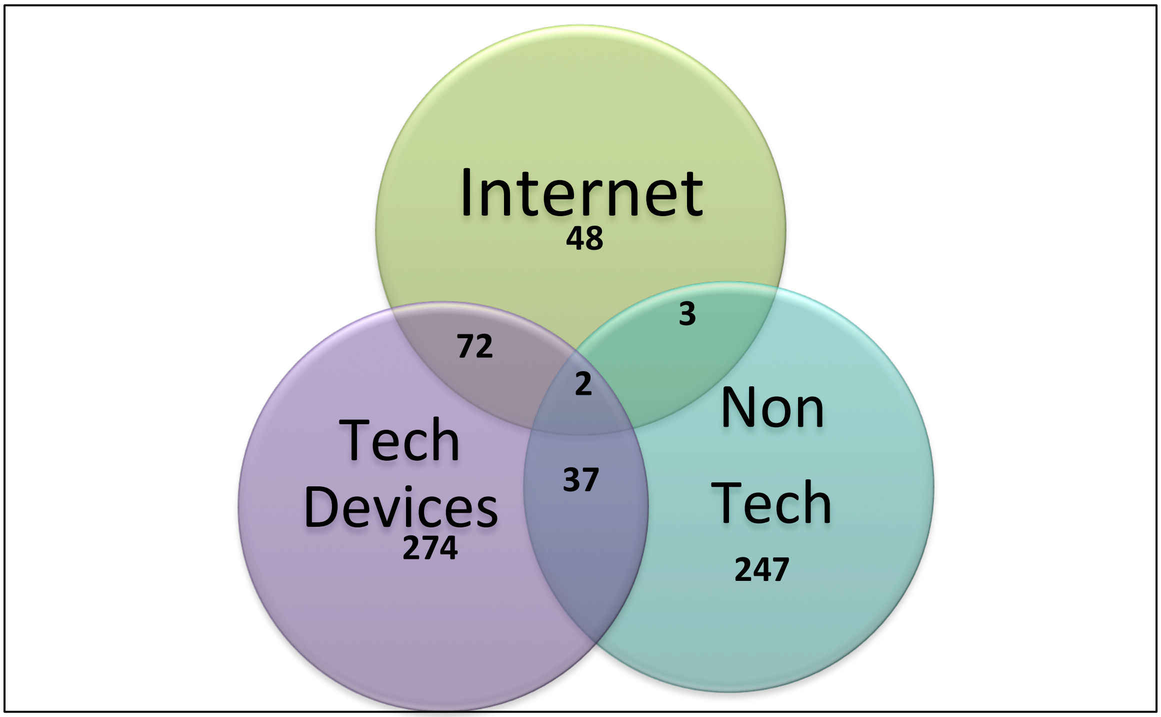


Figure 5. Offender Methods

Method Category	N	Percent
Internet only	48	3.4%
Technological Devices only	274	19.7%
Non-technological Means only	247	17.7%
Internet and Technological	72	5.2%
Internet and Non-technological	3	0.2%
Technological and Non-technological	37	2.7%
Internet and Technological and Non-technological	2	0.1%
Methods Unknown	712	51.0%
Total	1,395	100%

Figure 6 depicts graphically the interrelationships among the various methods used by offenders, when the methods are known. This excludes the 712 offenders for which the method was unspecified in data examined.

Figure 6. Interrelationships among Methods



Utilization of Methods by Offenders

Internet

There were 125 offenders who used the Internet in some fashion. The most frequent use was Hacking by 50 offenders. It was used for Phishing by 38 offenders, to search databases by 17 offenders, and for online identification document purchase and/or sale by 7 offenders. Unspecified Internet use was employed by 12 offenders. The Internet was used for Malware/Viruses/ Botnet attacks by only 1 convicted offender.

Technological Devices

Technological devices, including computers and other devices, whether used alone or in conjunction with the Internet and/or non-technological means, were used by 385 offenders. Computers were used most frequently for insider hacking – by 108 offenders. They were used for producing documents by 66 offenders, and for unspecified use by 115 offenders. Device-making equipment was used by 29 offenders and skimming devices were used by 49 offenders. The telephone was used by 18 offenders.

Use of Internet and Technological Devices

In one case the defendants and their co-conspirators obtained stolen credit/debit card information that had been obtained through computer intrusions and “carding” websites, which are Internet-based forums where users sell and exchange stolen credit and debit card information. Using the stolen account information, they manufactured counterfeit credit/debit cards that were encoded with the stolen account information and embossed with the names of “shoppers”—i.e., co-conspirators responsible for making unauthorized purchases with the counterfeit cards. Other members of the conspiracy acted as “drivers,” who coordinated teams of “shoppers” and transported them to retail stores located throughout the country, including Texas, North Carolina, Virginia, Pennsylvania, and New Jersey. The “shoppers” were given dozens of counterfeit credit/debit cards and used them to make purchases of retail items, including gift cards, electronics, cosmetics, clothing, and other merchandise worth thousands of dollars. To convert these items to cash, the defendants then transported the goods to New York and California, where they

Non-technological Means

Non-technological means, including mail theft, stolen access devices, and recruiting individuals to supply personally identifying information. One such scheme exploited the homeless and drug addicts.

Exploiting the Homeless/Drug Addicts

Offender A admitted that he had approached homeless individuals and drug users and had given them money in exchange for their names and social security cards. In September the offender used the name and social security number of another in order to obtain a fraudulent driver’s license in his state of residence under a presumed name and social security number with his photograph. The offender used the fraudulent driver’s license with his photograph to open a bank account under the presumed name and to write fraudulent checks on the account.

In other situations, offenders would use deception to tempt victims to engage in false business enterprises simply to gain personal identifying information from the victims to commit identity fraud. Such was the case below involving the opening of an ambulance service.

Business Offer

Offender A entered into an agreement with another individual to open an ambulance service and convinced the other person to provide Offender A with her personal information, such as her date of birth and social security number. Offender A used this information to open an account at Wachovia Bank and at Advanta Bank Corporation. Offender A wrote checks on the Wachovia Bank account but did not have funds to cover the checks. Offender A also applied for credit and financing with Advance Business Capital, Amerifund, Alliance Funding Group, Brick house, Capital National Bankers Trust, PenTech Financial Services, and Fleet One, LLC., using the other individuals name and personal identifying information. As a result of Offender A's activities, Wachovia Bank lost over $22,000.00.

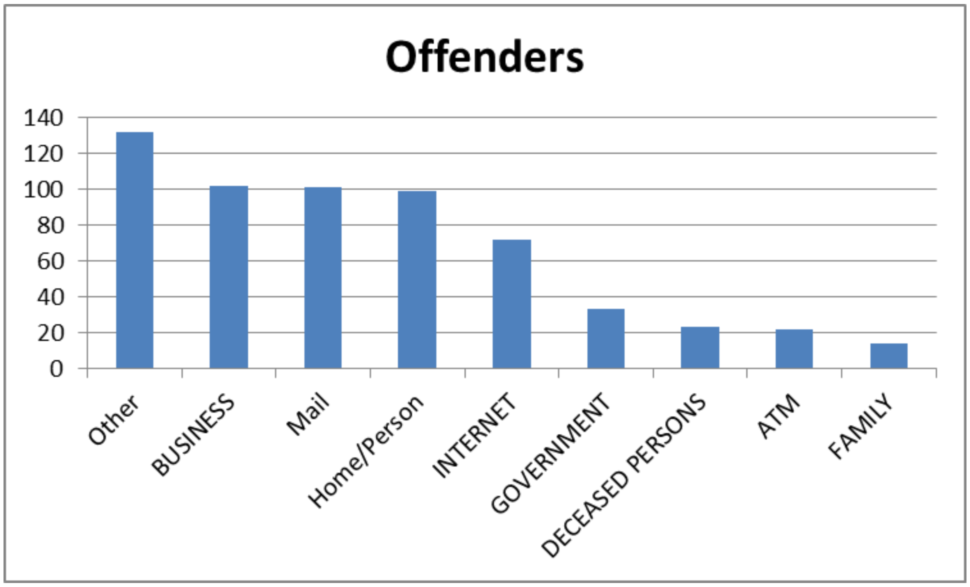
Points of Compromise

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 for 466 offenders. As Figure 7 shows, businesses (all business: service, retail, financial industry, corporations) accounted for 21.9% (102) of all the offenders point of compromise, when one could be identified. The two next highest categories are mail, 21.7% (101) and home/person 21.2% (99). For 15.4% (72) of the offenders, the Internet was the point of compromise. The personal identifiers were stolen from a Government agency by 7% (33) of the offenders. Theft from deceased persons occurred by 4.9% (23) and through an ATM by 4.7% (22) of the offenders. Family members were the point of compromise for 3% (14) of the offenders.

Business continues to be the main point of compromise, representing (17.01%) of all cases in the 2015 report. However, this is a sharp decline from (over 50%) of cases that it represented in the 2007 report. This approximately over 30% decrease tells us that criminals are deciding to commit identity fraud crimes by accessing the vulnerabilities of other points of compromise (mail, home/person etc.).

It is also important to note, that when comparing the two reports the percentage of family as a point of compromise also fell from (15.69%) in the 2007 study to only (3%) in the 2015 study. Mail as a point of compromise has increased from (8.76%) in the 2007 study to (21.7%) in the 2015 study. This marked increase of percentage of cases for mail may indicate that identity criminals are shifting their offense methods to the use of the mail system.

Figure 6. Points of Compromise for Identity Theft



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, etc.)
- Government agency (federal, state, and local)
- Medical (hospitals, doctors' offices, etc.)
- Utility (electric, cable, etc.)
- 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 8 categories is 2741. 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 8 shows, the largest percentage of victims was individual – 48.0% (1316).The next largest group of victims was the financial service industry – 24.2% (664). 23.1% (632) of the victims were Government Agency.

When comparing the 2007 and 2015 reports, the type of victims associated with the cases has changed drastically in 3 main categories: individual, financial services industry and retail.

Individuals represented (34.3%) of cases in the 2007 report and (48.0%) in the 2015 report. This increase of (13.7%) now makes it the largest category for victims. The category of individuals becoming the largest category of victims supports the idea that criminals have shifted their focus towards exploiting individuals over all other categories.

While the category of individuals increased, the financial services industry and retail both decreased. The decrease in financial services industry by (12.9%) and retail by (17.7%) shows that criminals are beginning to move away from these industries. Instead criminals are now focusing their efforts on individuals as their primary target. This trend could be indicative that criminals are finding it easier to victimize individuals than any other category.

It is also important to note that even though it has declined, the financial services industry still represents (24.2%) or nearly 1 in 4 of cases. Therefore, it should still be considered a main victimization concern along with individuals

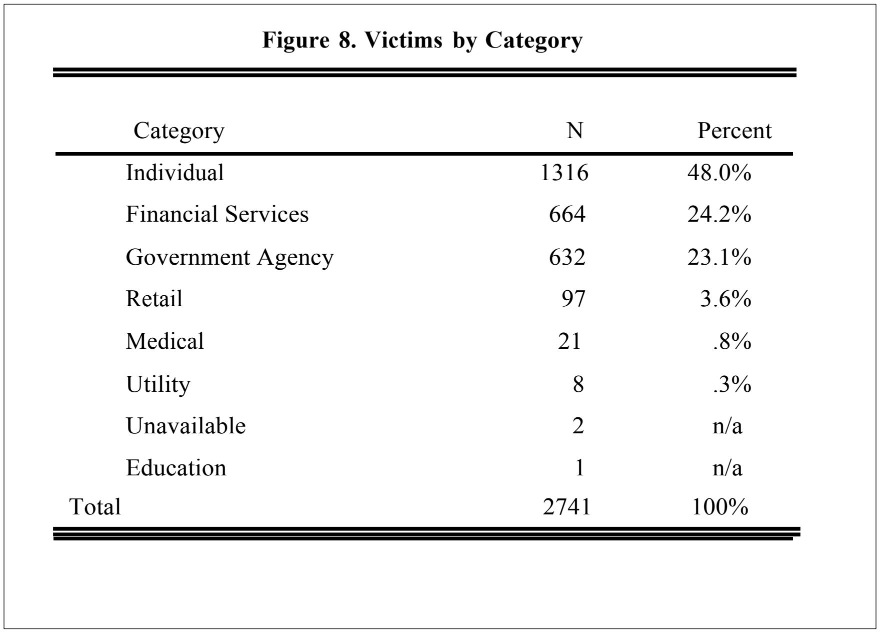


Figure 8. Victims by Category

Category	N	Percent
Individual	1316	48.0%
Financial Services	664	24.2%
Government Agency	632	23.1%
Retail	97	3.6%
Medical	21	.8%
Utility	8	.3%
Unavailable	2	n/a
Education	1	n/a
Total	2741	100%

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:

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

Figure 9 shows that the majority of offender – victim relationships involved an individual or individuals whom the offender did not know. Of the total 1,395 offenders, 60.1% (838) were categorized as strangers to the victims. The next most frequent relationship specified was customer/client. In 15.5% (216) of the relationships, the offender victimized an individual who had been a customer or client at his or her place of employment. In 3.6% of the relationships, the offender victimized a coworker or employer. The offender victimized a friend or acquaintance in 2.9% (41) of the relationships. Family relationships accounted for 1.9% (26).

It is interesting to note that strangers continue to represent the majority of offender - victim relationships. Stranger relationships saw a small increase from (59.4%) in the 2007 report to (60.1%) in the 2015 report. This lack of significant change indicates that stranger relationship cases consistently have an approximate ratio of 3:5 when compared to all other offender relationships.

Significant changes in offender – victim relationships occurred in the family and customer/client categories. Family relationships decreased from (5.0%) in the 2007 report to only (1.9%) in the 2015 report. Customer/client relationships increased from (10.5%) in the 2007 report to (15.5%) in the 2015 report. These differences indicate that there is a shift from family relationship cases to more customer/client cases.

Figure 9. Offender and Victim Relationships

Category	N	Percent
Stranger	838	60.1%
Customer/Client	216	15.5%
Family	26	1.9%
Friend/Acquaintance	41	2.9%
Coworker/Employer	50	3.6%
Other	20	1.4%
Unavailable	204	14.6%
Total	1395	100%

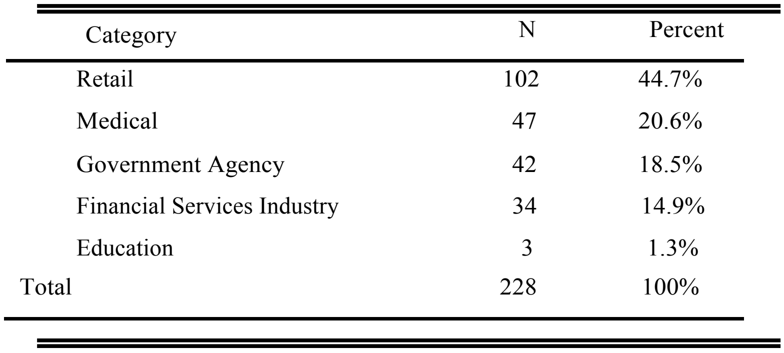
Defendants Stealing Identifying Information through Employment

Data was collected regarding the theft of personal identifying information from the offender's place of employment. Out of 844 cases, 27% (228) involved employees accessing records at their place of employment in order to perpetrate identity theft. This is a drop of approximately 7% from the 2007 study (34.1%). The types of employment were categorized in the same way as victims.

- Financial Services Industry (banks, credit unions, American Express, Discover, MasterCard, Visa)
- Retail (stores, car dealerships, gas stations, casinos, sports clubs, restaurants, hotels, etc.)
- Government agency (federal, state, and local)
- Medical (hospitals, doctors' offices, etc.)
- Education (public and private, all levels)

Of the remaining cases, 66.9% (565) involved no insiders, while in 7.2% (51) of the cases the involvement of an insider was unknown. Figure 10 displays the insider distribution by employment category.

Figure 10. Insider Employment



Category	N	Percent
Retail	102	44.7%
Medical	47	20.6%
Government Agency	42	18.5%
Financial Services Industry	34	14.9%
Education	3	1.3%
Total	228	100%

When an insider did play a role in the case, 44.7% (102) cases involved an insider in the retail industry like the one below. The second most frequently exploited industry was that of the medical industry, 20.6% (47) of cases. In the 2007 study, this category was folded into a larger one due to low numbers. In the 2015 study, researchers found offenders were victimizing medical organizations from the inside in a variety of manners. The case below involves a temporary employee at two medical facilities

Temporary Employee at Medical Facilities

Offender A used her temporary employment at two medical facilities to steal the names, dates of birth, social security numbers and other identifying information of over 40 individuals. She and her co-conspirators used the stolen identities to purchase goods at retail stores and a Maryland car dealership, where some of her co-conspirators worked. The co-conspirators were paid for allowing Offender A to purchase items at these stores. Offender A used stolen identity information of a victim to forward the victim's mail to a mail box that Offender A controlled. Offender A also used the victim's stolen identity to obtain $35,560.20 from a bank to finance her purchase of a Mercedes-Benz coupe.

Discussion of Results

As expressed at the beginning of this report, the general aim of the study the report is based on is to decipher present characteristics of identity crimes, criminals and victims to determine, what changes, if any, have taken place since the first CIMIP study of identity crimes published in 2007. Expectedly, a number of characteristics have stayed the same. But, the types of characteristics that have changed, point to a new breed of identity criminal; one that is gravitating toward increased use of technology, operating in criminal groups and preying more upon individuals. What this means, is open to speculation. This concluding section offers some thoughts on the possible interpretations of these findings and how an appreciation of this knowledge can assist in the development of evidence-based strategies directed at identity theft control and prevention.

When the original 2007 CIMIP study was released, there was some surprise regarding the gender distribution of offenders; two thirds male, and one third female. At the time, it was the proportion of female offenders that received the most attention. Somehow, this ran against conventional wisdom at the time. Well, eight years later, this phenomenon has not changed. The examination of federally prosecuted cases from 2008 through 2013 has demonstrated a remarkable level of consistency since the first study. Once again, males make up two thirds of the total with females representing one third. In a way, this probably should not be unexpected. Identity crime can be committed by anyone. It is crime that poses little physical risk to the offender (as opposed to crimes like armed robbery, for instance) and can be committed as a "crime at a distance," employing the use of the Internet, mail or telephone to draw victims in. In addition, there may be a neutralizing effect to potential victims if the offender is relying on social engineering methods and is also female. In studies of incarcerated identity thieves conducted by Heith Copes and Lynne Vieraitis (2012), the authors alluded to how female offenders depended on a certain aura of trust that could disarm their prey. Some were even found to enhance this "trust element" by posing as nurses in full uniform. Unlike "street crimes", there seems to be a higher proportion of females engaging in identity crimes, a trend that does not seem likely to change in the near future.

A marked change has occurred, however, in the area of offender age. Comparing results of the present study to that of the 2007 study, offenders turned out to be, generally, older. The 2015 study displayed increases in the proportion of offenders in the 35 to 49 year bracket, and the 50 years and older range. There are several possible explanations for this trend. One is that offenders are remaining with this type of crime technique (i.e., stealing identities of others to commit fraud) because it has worked over time without them being caught. Indeed, many of the present study cases occurred over protracted periods of time before the offenders were caught.

The original 2007 study noted that many of the offenders brought to justice, had been involved in the area of identity theft for some time before being caught. Copes and Vieraitis (2012) explain that many of the offenders they interviewed were not concerned with the risk of being detected and believed that their penalties would be light if arrested and convicted. Some even rationalized that their crimes were doing little harm to their victims, making the criminal actions more acceptable in the minds of the offenders. Another possible explanation is related to financial insecurity of the offenders. Copes and Vieraitis (2012) note that some of the offenders interviewed were compelled to commit their acts because they had fallen on hard financial times. In the end, it is difficult to explain why the offenders seem to be aging, but the pattern revealed is intriguing.

Besides the change in the age make-up of identity criminals, another change stood out; a sharp upsurge, from the 2007 study, in offender involvement with “criminal groups” in the commission of the crimes. These are not cases of organized crime, but crimes in which offenders ally with one or more other individuals to conduct the criminal act. This type of group involvement was present in the 2007 study, but not to the extent it was in this study. The work of Copes and Vieraitis (2012) may also supply some food for thought on this pattern. They explain that some of those they interviewed were seeking to minimize their level of culpability if they were acting as part of a group rather than acting alone. The 2015 results could be a reflection of a growth in this type of rationalization. It also could represent a proclivity of offenders to specialize their criminal skills to the point that they are valuable to the criminal group but are also dependent on the criminal skills of others to pull the crimes off.

Two additional findings surfaced in the present study that may seem contradictory on the surface, but when examined more closely present an interesting phenomenon. First, the use of technology (e.g., computers, cell phones) by offenders sharply increased since the 2007 study. Like other white collar criminals, identity thieves are finding it increasingly convenient, efficient and able to attack more potential victims at any given time. In and of itself, this is not surprising. What is surprising is that offenders seem more likely to attack individuals rather than organizations/ businesses than in the past. “Points of compromise” in the identity theft attacks showed a concentration on individuals, particularly with the use of mail and the Internet as a criminal conduit. The use of mail in the commission of the crimes actually doubled since the last study. One possible explanation is that social engineering efforts by offenders are becoming more effective, possibly because potential victims are letting down their guard or cognitive skills of a growing population of the elderly are worsening. Another possibility is that businesses and government agencies housing sensitive personal information that can be stolen and used for identity fraud, have been devoting greater efforts to protecting that information. In a sense, they would be hardening the target against those who would seek to penetrate sensitive information systems. On the same note, the proportion of cases involving “insiders” has dropped, possibly signifying inroads into strategies used by both the private and public sectors in preventing insider breaches (e.g., limiting legitimate access to sensitive information, limiting the number of employees with such access, enhancement of internal surveillance methods).

The 2007 CIMIP study of identity crimes offered broad recommendations generated by the study results. They centered on issues like the integration of the findings into enforcement briefings and existing training programs. The 2015 CIMIP study results underscore those practical suggestions but with an emphasis on a greater urgency to elevate training and awareness to the next logical level. Based upon recent study results, the average identity thief has progressed as a criminal innovator in the present day. The offender tends to be older, more experienced and more cunning than in the past. Further, the average offender seems to comprehend the significance of functioning as a member of a “team” to be successful in their criminal acts. What this means for enforcers is that they must have a greater understanding of what lies beneath the surface of the initial observable offense.

In the 2007 study, one case seemed to exemplify the types of offenses that are occurring more often now. That case involved what appeared, at first sight, to be a petty burglary of wallets and purses of residents of a nursing home. The perpetrators, in fact, had impersonated nursing home attendants to steal personal information of the residents for use in the perpetration of identity crimes. As the present study stresses, the increasing use of organized units to commit the offenses, calls for a recommendation that enforcement entities must dig deeper into these cases to root out the complete portrait of the breadth of what may seem like rudimentary criminal cases on the surface.

It is also important to acknowledge the apparent shift to individuals from organizations as primary targets and the use of simple means (mail, telephone) to connect with the potential victims. This is a clear indication that offenders are zoning in on what they see as the vulnerable points of compromise, turning away from choice targets of the recent past. This translates into a dire need for enriched programs of crime awareness, particularly for those susceptible to being victimized by strong social engineering techniques; groups like the elderly and those who may be suffering from cognitive deficiencies due to medical maladies. Such awareness programs must be supported and administered nationally in a decisive effort to thwart manipulative tactics used by the new breed of identity criminals that society faces.

While recognizing the use of these basic criminal engineering methods, law enforcers must not lose sight of the role that technology plays in other identity crime approaches, for the battle lies on more than one front. Law enforcement must not only use current empirical information to help them navigate the terrain of identity offender tools used, but serve to predict what new advances in computerized technology can open opportunities for the identity criminals of the future. In addition, law enforcement is obligated to keep abreast of technological advances made available to consumers (e.g., online tax return submissions) to help predict where the identity thieves will move next. As pointed out by entities like the Alliance for Medical Identity Fraud (MIFA) and the Institute for National Standards (INSA) such an arena for the present and the future is the misuse of personal medical information for the purpose of identity fraud. In the 2007 study, these types of crimes hardly registered. In the present study, they play a much more important role. Law enforcement must be able to realistically assess where the next ripe area for exploitation is for identity thieves, to engage in proactive control/ enforcement, rather than depend on the historic reactive approach to identity criminality in the United States.

References

Copes, H. and Vieraitis, M. (2012). Identity Thieves: Motives and Methods. Northeastern University Press:Boston.

Gordon, G., Rebovich, D., Choo, K. and Gordon J. (2007, October) Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement. Center for Identity Management and Information Protection: Utica, New York.

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

Appendix

Collection Template

Open Source Data Collection Form

For use with USAO press releases
(Instructions follow)

Labeling Information
Case Identifier: _ _ _ _ _   State: ___________________   Prosecuting Entity: _ _ _ _-_ _

Agency Involvement
Assisting Agency: _______________________   Assisting Agency 2:
____
Assisting Agency 3: _____________________   Assisting Agency 4:
____
Assisting Agency 5: _____________________   Assisting Agency 6:
____
Assisting Agency 7: ___________________

Procedural
Date: _ _/_ _/_ _ _ _   Case Status: _______________________

Offender
Offender Name: ____________________ Offender Gender: ____ Offender Age: _____
Offender Legal Status: ____________

Crime
Crimes Committed Against: Corporate, Government, Private: _________________
Crime: _______________
Additional Crime 1: _____________________   Additional Crime 2:
____
Additional Crime 3: _____________________   Additional Crime 4:
____
Additional Crime 5: _____________________

Means of Victimization
Offender Relation to Identity Owner: _________________
Victim Category: ______________________ Offender Type: _____________________

Methods Used
Internet Methods: ________________________
Technological Methods: _______________________
Non-Technological Methods: __________________________
Point of Compromise: _____________________ Insider Type: _____________________
Insider Service Type: _____________________

Other
Additional Case Info:
____

Case Identifier: Enter a unique case identifier. This will be generated for each individual case and should be alphanumeric beginning with the state abbreviation, followed by a three digit number assigned sequentially. When entering a new case for each state, first refer to the previously entered cases for that state to determine the next case identifier that should be assigned. Remember that an individual record is created for each defendant, so when multiple defendants are linked be sure to use the same case identifier to demonstrate the relationship. All letters should be capitalized and there should be no spaces. All text within the database is Calibri, 12pt. font.

State: Enter the name of the state. Use all capital letters.

Prosecuting Entity: Enter the identifier for the prosecuting entity. Use all capital letters and no spaces. Separate the United States Attorney Office from the state abbreviation with a dash (-).

Assisting Agency: Enter the assisting agencies in these columns using the abbreviations for major agencies when applicable. A list of agency abbreviations is included in the database supplement.

Date: Enter the date of the most recent case development (indictment or conviction). Use the format mm/dd/yyyy.

Case Status: Enter the status of the case, either indicted or convicted. Use all capital letters.

Offender Name: Enter the name of the defendant in the traditional format (capitalizing only the first letter of each name). If nicknames or aliases etc. are included enter these as well. This can be done by entering the legal name, followed by “aka” and then the alias etc. This may be repeated as needed to include all of the additional identifiers.

Offender Gender: Enter the offender’s gender, if discernable from the information provided. Enter either “M”, “F”, or “UNKNOWN”.

Offender Age: Enter the age of the offender, if known.

Offender Legal Status: Enter the offender’s citizenship status. Enter either L for legal, I for Illegal, or F for foreign. Use all capital letters.

Crimes Committed Against: Enter the sector of the population the crime(s) impact. Enter either CORPORATE, GOVERNMENT, or PRIVATE. If multiple sectors are impacted, separate each category by a forward slash (/). All letters should be upper case. CORPORATE should include any company or group of people authorized to act as a single entity (legally a person) and recognized as such in law. For example, retail stores, banks, credit card companies, etc. GOVERNMENT should include all agencies and departments in all levels of government (local, state, and federal). For example, the IRS, SSA, military, etc. PRIVATE should include individual persons who have had their personal identifying information stolen.

Crime: Enter the crime committed by the offender in this column. All letters should be upper case. See section A, subsection IV for code words. It is important to refer to this section of the database supplement when making entries in this column because the offenses are somewhat condensed and broad code words are used to encompass several variants certain crimes.

Additional Crime(s): Enter the additional crimes in the same manner.

Offender Relation to Identity Owner: Enter the relationship between the offender and the victim of the crime(s) whose personally identifying information was stolen in this column. If the relationship is not known, enter UNKNOWN. All letters should be upper case. See section A, subsection IV. for code words.

Victim Category: Enter the category victims of the crime may be identified with. Enter GOVERNMENT AGENCY, INDIVIDUALS, FINANCIAL SERVICES, RETAIL. If multiple categories are appropriate, separate each with a forward slash (/). All letters should be upper case. See section A, subsection IV. for code words.

Offender Type: Enter whether the offender acted alone or with others by entering either INDIVIDUAL or GROUP. All letters should be upper case.

Internet Methods: Enter if any internet methods were used in the perpetration of the crime. Enter HACKING, MAILWARE/VIRUS/BOTNET, PHISHING, INTERNET HIJACKING, ONLINE DATABASE SEARCHING, etc. All letters should be upper case. See section A, subsection IV. for code words.

Technological Methods: Enter any technological methods that were used in furtherance of the crime. All letters should be upper case. See section A, subsection IV. for code words.

Non-Technological Methods: Enter any non-technological methods that were used in furtherance of the crime. All letters should be upper case. See section A, subsection IV. for code words.
This column is the most complex. It encompasses a wide range of code words and serves as somewhat of a conglomerate category. It is essential to review the list of previously entered code words in order to gain a better understanding of the information included in this column.

Point of Compromise: Enter the specific condition or circumstance which enabled the offender to steal identifying information. All letters should be upper case. See section A, subsection IV.

Insider Type: If the point of compromise was an insider, enter the business type or industry which the insider had access to. If one did not exist, enter NONE. All letters should be upper case. See section A, subsection IV. for code words.

Insider Service Type: Enter the function or role that the insider had which enabled them to have access to the identifying information. If one did not exist, enter NONE. All letters should be upper case. See section A, subsection IV. for code words.

Additional Info: Copy and paste the summary of the case which includes information not yet entered in to the database in the other columns. This may be found in separate paragraphs, in which case you may copy multiple paragraphs, or portions of those paragraphs and piece them together to create a case summary. See the second screen shot on the next page.