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

Individual Activity vs. Organized Group Activity: Roles

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

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

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

Figure 24. Number of Defendants

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

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

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

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

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

One Offender – Several Opportunities and Roles

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

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

A small level group crime case

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

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

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

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

Offender Methods

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

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

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

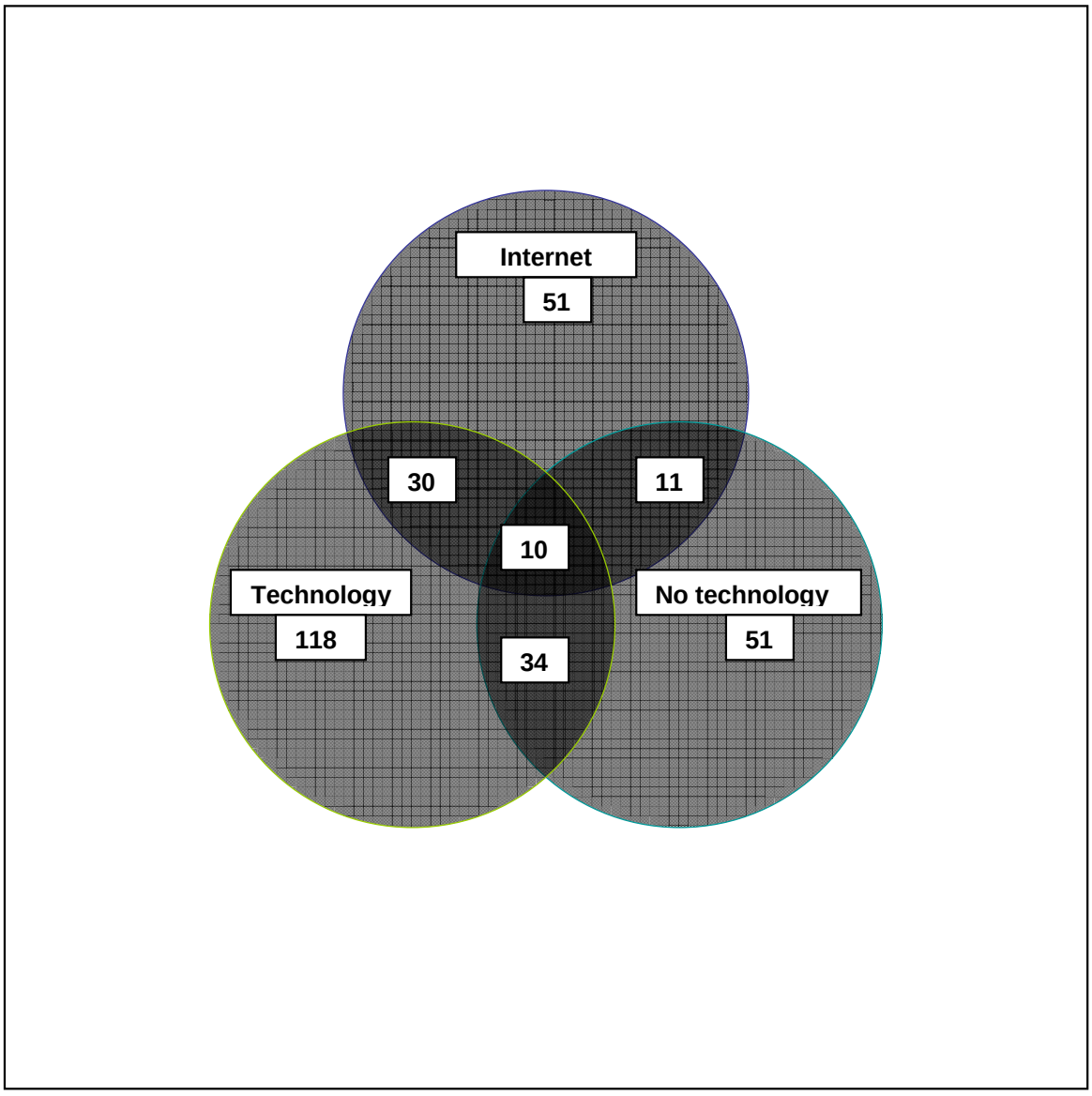
As shown in Figure 25, in 41% (212) of the cases, there was no use of the Internet, technological devices, or non-technological means. In 51 of the cases (9.9%) the offenders used the Internet in some manner, but did not use any other technological devices or non-technological means. In 5.8% (30) the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

Figure 25. Offender Methods

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

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

Figure 26. Interrelationships among Methods



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

Utilization of Methods by Offenders

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

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

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

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

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

Patterns of Offender Methods

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

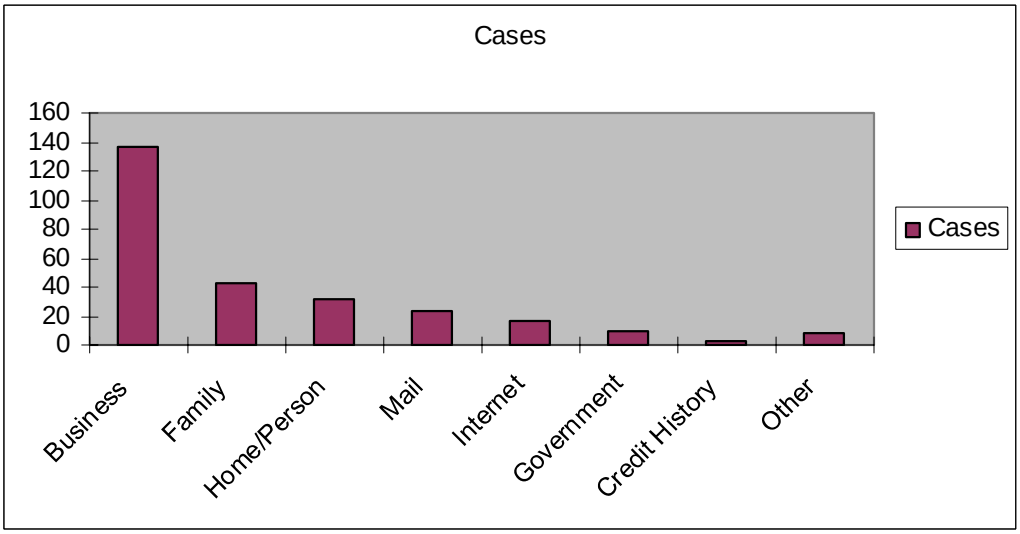
Unfortunately, any trending analysis is premature, as there are very few 2005 and 2006 closed cases. A continuation study is planned that will collect the necessary data to provide for this level of analysis. The following preliminary findings were observed.

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

Points of Compromise

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

Figure 27. Points of Compromise for Identity Theft



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

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

The Commission of the Offense in Summary

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

Victimization

The Victims

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

- Individual (people)
- Financial Services Industry (banks, credit unions, American Express, Discover, MasterCard, Visa)
- Retail (stores, car dealerships, gas stations, casinos, sports clubs, restaurants, hotels, hospitals, doctors' offices, etc.)
- Government agency (federal, state, and local)
- Credit Bureau
- Insurance (life, car, property, casualty, health)
- Education (public and private, all levels)
- Unavailable (There was no indication of the victim in the file.)

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

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

Figure 28. Victims by Category

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

Methods of Victimization (other than individuals)

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

Figure 29. Methods of Financial Services Industry Victimization

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

*FOPII=fraudulently obtained personal identifying information

Victimization of Financial Services Industry

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

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

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

Offender Relationship to Individual Victims

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

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

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

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

Figure 30. Offender and Victim Relationships

Category	N	Percent
Stranger	540	59.4%
Customer/Client	95	10.5%
Family	46	5.0%
Friend/Acquaintance	28	3.1%
Coworker/Employer	28	3.1%
Unavailable	172	18.9%
Total	909	100%

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

Offender-Victim Relationship: Caretaker-Employer

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