INFORMATION ON IDENTITY THEFT FOR CONSUMERS AND VICTIMS FROM JANUARY 2002 THROUGH DECEMBER 2002

Summary

The Federal Trade Commission (FTC) began collecting consumer reports in the Identity Theft Data Clearinghouse (Clearinghouse) on November 1, 1999. This report summarizes the data collected from the 218,714 reports the FTC processed during calendar year 2002. Of these, 161,819 (74%) were from victims of identity theft, and 56,895 (26%) were from other consumers concerned about identity theft. Not all identity theft victims file complaints with the FTC. However, while not reflective of all identity theft victims nationwide in 2002, the data provide useful information about the nature of identity theft activity.

Consumers' information reaches the Clearinghouse in a variety of ways. In 2002, 74% of the consumers in the database contacted the FTC through its toll-free Identity Theft Hotline (877-ID-THEFT); 13% of the consumers contacted the FTC via its online complaint form located at www.consumer.gov/idtheft; 2% reached the agency by postal mail, and 11% contacted outside agencies that then provided the complaint information to the FTC. For example, the Social Security Administration's Office of the Inspector General (SSA-OIG), which operates a Consumer Fraud Hotline, contributed 22,790 consumer identity theft complaints to the Clearinghouse in 2002.

The volume of calls to our Hotline grew substantially during 2002. In January 2002, the Hotline answered around 3,640 calls per week. By December 2002, the Hotline was answering 4,502 calls per week. The volume of complaints received via the Internet also grew, going from 511 received in January 2002 to 788 received in December 2002.

How the Suspect Misused the Victim's Personally Identifying Information

The Clearinghouse data, which represent complaints received by both the FTC and the SSA-OIG, indicate how victims report that the thieves have used the stolen identifying information. The 2002 data, summarized below, help provide a broad picture of the forms identity theft can take.[1] (*See Figures 1 and 2.*)

- *Credit Card Fraud:* Forty-two percent of the victims' complaints in the Clearinghouse reported credit card fraud. This breaks down to 24% indicating that one or more new credit cards were opened in their name, 12% indicating that unauthorized charges were made on an existing credit card, and about 5% reporting credit card fraud without specifying whether the thief had obtained new or used existing credit cards.
- *Telecommunications or Utility Fraud:* Twenty-two percent of the victims' complaints in the Clearinghouse reported that the identity thief obtained unauthorized telecommunications or utility equipment or services using their personal information. This is comprised of 11% complaining that the thief obtained new wireless telecommunications equipment and service, 5% reporting new land line telephone service or equipment, 3% reporting that new utilities accounts for services such as electricity or cable were opened using their personal information, 2% not specifying the type of new telecommunications or utility fraud opened, and fewer than 1% reporting unauthorized charges to their existing telecommunications or utility accounts.
- *Bank Fraud:* Seventeen percent of all victims reported fraud on their demand deposit

[1]Approximately 22% of consumers reported experiencing more than one form of identity theft. Therefore, the percentages add to more than 100%, and represent the number of consumers whose personal information was used for each illegal purpose.

(checking or savings) accounts. This encompasses about 8% reporting fraudulent checks written on their existing account, 4% reporting a new bank account opened using their personal information, 3% reporting unauthorized electronic withdrawals from their account, and 2% not specifying.

- *Employment:* Nine percent of the victims in the database reported that the identity thief used their personal information to obtain employment.
- *Fraudulent Loans:* Six percent of all victims reported that the identity thief obtained a loan in their name. This includes 3% complaining that the thief obtained a personal, student, or business loan using their personal information, 2% reporting auto loans or leases, 1% reporting real estate loans, and .5% not specifying the type loan.
- *Government Documents or Benefits:* Eight percent of the all victims in the Clearinghouse reported that the identity thief obtained government benefits or forged or obtained government documents in their name. This contains 3% reporting that the identity thief had obtained or used a driver's license in their name; fewer than 2% reporting that the thief had obtained or used a social security card in their name; and .3% reporting the thief used another official document in their name.[2] It also includes nearly 2 % reporting fraudulent claims for tax returns in their name; nearly 1% reporting that the thief received government benefits in their name; and .1% not providing specific information about the type of government documents or benefits the thief used or received in their names.

[2]Because victims usually do not know the details about how the thief actually committed his or her fraud against the financial or other institutions involved, these numbers may understate how frequently these false documents are used in the commission of identity theft.

- *Other Identity Theft:* Sixteen percent of all the victims in the database reported various other types of identity theft. This breaks down to 2% reporting that the thief assumed their identity to evade legal sanctions and criminal records (thus leaving the victim with a wrongful criminal or other legal record), almost 2% reporting that the thief obtained medical services in their name, 1% reporting that the thief opened or accessed Internet accounts, 1% reporting that the thief leased a residence, .4% reporting that the thief declared bankruptcy using their personal information, and .2% reporting that the thief purchased or traded in securities and investments using their personal information. It also includes about 9% whose complaints were coded simply as "Other," indicating that they did not fit into any of the above-listed categories. Many of these were from victims who had learned recently of the misuse of their identity but had not yet determined the exact nature of the identity theft. Others involved types of identity theft that are reported infrequently, such as insurance fraud. We monitor the complaints in this category to determine if they merit developing new categories or possible re-categorization.
- *Attempted Identity Theft:* Eight percent of the victims in the database reported that someone had obtained their personally identifying information but had been unsuccessful in attempts to misuse it. These attempts are counted as identity theft complaints because all of the elements of an identity theft crime are present. However, they are not categorized by the type of misuse, such as obtaining a new credit card or wireless phone, that the thief was attempting.

Age of Victims

Ninety-four percent of victims reporting to the FTC in 2002 provided their age.[3] The largest number of these victims (27%) were in their thirties. The next largest group includes consumers from age eighteen to twenty-nine (26%), followed by consumers in their forties (22%). Thirteen percent of victims were in their fifties, and 11% of victims were age 60 or over. Almost 2% of victims were consumers under age 18. (*See Figure 3*.)

Geographic Information

While the geographic distribution of identity theft complaints in the Clearinghouse may be affected by regional variations, including consumer awareness of our resources and complaint program, the distribution of complaints was fairly consistent from 2001 to 2002. The 2002 data show that on a *per capita* basis (*per* 100,000 citizens), the District of Columbia had the highest percentage of victim complaints in the Clearinghouse, followed by California, Arizona, Nevada, Texas, Florida, New York, Washington, Maryland, and Oregon. (*See Figures 4a-b*.) In 2001, the top ten states were the same, except that Georgia was in the top ten, and Texas was not. The order of the top ten states in 2001 was also somewhat different, with the District of Columbia as the top ranked, followed by California, Nevada, Maryland, New York, Arizona, Oregon, Florida, Washington, and Georgia, in that order.

Time Between First Misuse of Identity and Initial Discovery by Victim

Fifty-nine percent of victims who contacted the FTC in 2002 reported both when their information was first misused and when they first discovered that they were victims of identity theft.[4]

[3]The statistics regarding consumers' age reflect the experience only of the consumers who contacted the FTC directly, and do not reflect consumers who contacted the SSA-OIG, which does not collect such information.
[4]The statistics regarding when victims discover the crime reflect the experience only of the consumers who contacted the FTC directly, and do not reflect consumers who contacted the SSA-OIG, which does not collect such

Some victims experience multiple instances of identity theft and discover different misuses at different times. The figures collected by the FTC do not track the amount of time it takes for the victim to discover each particular instance of identity theft, but rather, the amount of time between the initial misuse of the victim's information and when the victim first discovers that their information has been misused.

A significant percentage of the victims (48%) reported discovering they were victims of identity theft less than one month after the thief first misused their information. Twenty-two percent learned that they were victims of identity theft within 6 months of its first occurrence. However, 15% were unaware of the initial misuse of the their identity for more than two years. On average, 12 months elapsed between the initial misuse of the consumer's identifying information and when the victim first discovered that they were identity theft victims. (*See Figure 5*.)

Steps Taken by Victim in Response to Identity Theft[5]

At the time of their initial contact with the FTC in 2002, 60% of the victims reporting this data indicate that they had already contacted a consumer reporting agencies (CRAs). Fifty-seven percent of all victims reporting, or 94% of the victims who had contacted a CRA, had placed a fraud alert on one or more of their credit files. (*See Figure 6*.) The FTC counsels those victims who have not contacted any of the CRAs prior to contacting the FTC (40% of all victims reporting) to do so, and to request a fraud alert on their credit files and copies of their credit reports as a first step for resolving their identity-theft related problems.

information.

[5]The statistics regarding what steps the victims have taken reflect the experience only of the consumers who contacted the FTC directly, and do not reflect victims who contacted the SSA-OIG, which does not collect such data.

Forty-seven percent of all victims contacting the FTC in 2002 reported that they had already contacted one or more local police departments. Consumer contacts with the police break down into three categories: 1) 36% of all victims contacting the FTC reported that the police department took a report of their identity theft; 2) 9% reported that although they contacted the police, they did not obtain a report; and 3) 2% did not indicate if a report was taken. (*See Figure 7.*) Fifty-three percent of the victims who complained to the FTC in 2002 had not yet contacted the police. They were advised to do so and to get a police report.

Other Information About Identity Theft

Nearly 70% of the complaints received by the Clearinghouse in 2002 contained some information about the person who is suspected of committing the identity theft. Victims often learn a name, address, or phone number used by the suspect from the creditors, collection agencies, or other entities involved in trying to collect the fraudulent debt or investigate the crime. This information is useful to law enforcement in linking seemingly unrelated complaints to a common suspect.

Twenty-eight percent of the victims who contacted the FTC reported that they thought they knew how the thief obtained their personal information. This includes about 15% who indicated that someone they knew personally had stolen and misused their identity. The relationships reported include family members (5%), friends and neighbors (2%), roommates (1%), personal associates from the victim's workplace (1%), and persons known to the victim in some other capacity (5%).

Another 13% of all victims reported an event or incident that they believe led to the identity theft. This includes nearly 8% reporting that their wallet or purse had been lost or stolen, and 2% reporting mail theft or fraudulent address changes. It also includes 3% reporting that the thief obtained

their information in various other ways, including burglary, solicitation over the telephone or Internet, theft of information from employment or financial records, database hacking, and pretexting information from financial institutions.[6]

Techniques such as stealing information from employment or financial records, database hacking, skimming consumers' credit or ATM cards, shoulder surfing, combing through public records, and purchasing information from the black market can be employed without the victim's knowledge. Thus, it is no surprise that 72% of the victims contacting the FTC do not know how the identity thief obtained their information.

Conclusion

The FTC's Identity Theft Data Clearinghouse is the federal government's centralized repository of identity theft complaint data. In December 2002, after three years of operation, it contained over 279,134 complaints. The Clearinghouse is a rich source of information for law enforcement investigations. The FTC, in conjunction with the U.S. Secret Service and other government law enforcement agencies, mines the Clearinghouse data to uncover significant patterns of identity theft activity, develops investigatory reports based on the data, and refers the reports to the appropriate criminal law enforcement officials for possible investigation and prosecution. The FTC also shares the Clearinghouse information with nearly 600 law enforcement agencies nationwide via the FTC's secure law enforcement Web site, Consumer Sentinel. (*See www.consumer.gov/sentinel*.) The FTC and other government entities also use the aggregate information in the Clearinghouse to understand more about where identity theft occurs, what forms it takes, and how victims are affected.

[6]The very low number of reports in these categories is likely to understate substantially the actual extent of the use of these methods to obtain personal information.