IDENTITY THEFT
Data Clearinghouse

IDENTITY THEFT

COMPLAINT DATA

Figures and Trends On Identity Theft

January 2001 through December 2001

FEDERAL TRADE COMMISSION

INFORMATION ON IDENTITY THEFT FOR CONSUMERS AND VICTIMS FROM JANUARY 2001 THROUGH DECEMBER 2001

Summary

The Federal Trade Commission (FTC) began collecting consumer complaints in the Identity Theft Data Clearinghouse (Clearinghouse) on November 1, 1999. This report summarizes the data collected during calendar year 2001. The FTC processed 117,210 reports in 2001, 86,168 (74%) from victims of identity theft and 31,042 (26%) from other consumers concerned about identity theft. We believe that this does not capture all identity theft victims nationwide in 2001. Thus, while not reflective of all identity theft victims nationwide in 2001, the database can reveal general information about the nature of identity theft activity.

Consumers' information reaches the Clearinghouse in a variety of ways. In 2001, 73% of the consumers in the database contacted the FTC's toll-free Identity Theft Hotline (877-ID-THEFT); 12% of the consumers contacted the FTC via our online complaint form located at www.consumer.gov/idtheft; 2% reached us by postal mail, and 13% 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 15,611 records to the Clearinghouse in 2001.

The volume of calls to our Hotline grew substantially during 2001. In January 2001, the Hotline answered around 2,330 calls per week. By December 2001, the Hotline was answering over 3,000 calls per week. The volume of complaints received via the Internet also grew, going from 688 received in January 2001 to 1,172 received in December 2001.

How the Suspect Misused the Victim's Personally Identifying Information

The Clearinghouse data, which represents complaints received by both the FTC and the

SSA-OIG, reveal how the thieves use the stolen identifying information. The 2001 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 in the Clearinghouse reported credit card fraud. Twenty-six percent of victims indicated that one or more new credit cards were opened in their name, making this the most commonly reported misuse of victims' information. Ten percent of the victims indicated that unauthorized charges were made on their existing credit card. About 6% of the victims reported credit card fraud but were not specific as to whether the thief obtained new or used existing credit cards.
- *Telecommunications or Utility Fraud:* Twenty percent of the victims in the Clearinghouse report that the identity thief obtained unauthorized telecommunications or utility equipment or services in their name. Almost 10% of all victims complained that the thief obtained new wireless telecommunications equipment and service in their name. Five percent of all victims reported new land line telephone service or equipment, new utilities such as electric or cable service was reported by just over 2%. Two percent of all victims did not specify the type of telecommunications or utility fraud, and .5% reported unauthorized charges to their existing telecommunications or utility accounts.
- *Bank Fraud:* Thirteen percent of all victims reported fraud on their demand

[1]Many consumers experience more than one form of identity theft. Therefore, the percentages represent the number of consumers whose information was used for each various illegal purpose.

deposit (checking or savings) accounts. About 6% of all victims reported fraudulent checks written on their existing account, 3% reported a new bank account opened in their name, 2% reported unauthorized electronic withdrawals from their account, and about 2% of these complaints were not specific.

- *Employment Fraud:* Nine percent of the victims in the database reported that the identity thief used their personal information to obtain employment.
- *Fraudulent Loans:* Seven percent of all victims reported that the identity thief obtained a loan in their name. Over 3% of all victims complained that the thief obtained a personal, student, or business loan, nearly 2% reported auto loans or leases, nearly 1% concerned real estate loans, and .6% did not specify the type of loan.
- *Government Documents or Benefits Fraud:* Six percent of all victims reported that the identity thief obtained government benefits or forged or obtained government documents in their name. About 3% of victims in the Clearinghouse reported that the identity thief had used a driver's license in their name, fewer than 1% reported that the thief had used a social security card in their name, and .3% reported the thief used another official document in their name.[2] Almost 2% of all victims reported fraudulent claims for tax returns in their name, .4% reported that the thief received government benefits in their name, and .2% of these victims were not specific about the type of government documents or benefits the thief used or

[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, we believe these numbers may understate how frequently these false documents are used in the commission of identity theft.

received in their names.

- *Other Identity Theft:* Nineteen percent of the victims in the database reported various other types of identity theft. Almost 2% of all victims reported 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% reported that the thief obtained medical services in their name, 1% reported that the thief opened or accessed Internet accounts, almost 1% reported that the thief leased a residence, .4% reported that the thief declared bankruptcy in their name, and .2% reported that the thief purchased or traded in securities and investments. About 13% of the complaints were coded simply as "Other," indicating that they did not fit into any of the above-listed categories. Many of them were from victims who have just learned 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. We monitor the complaints in this category to determine if they merit the development of new categories or possible recategorization.
- *Attempted Identity Theft:* Ten percent of the victims in the database reported that someone had obtained their personally identifying information and had attempted to misuse it, but had not yet been successful in their attempts. 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

Eighty-eight percent of victims reporting to the FTC provide their age.[3] The largest number of these victims (28%) 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 9% of victims were age 60 or over. Almost 2% of victims were consumers under age 18. (*See Figure 3)*

Geographic Information

While the data on geographic distribution of identity theft complaints in the Clearinghouse may be affected by regional variations, including consumer awareness of our Hotline, it was fairly consistent from 2000 to 2001. The 2001 data show that California had the greatest overall number of victims in the Clearinghouse, followed by New York, Texas, Florida, and Illinois. *(See Figures 4a-b)* On a *per capita* basis, (*per* 100,000 citizens), the District of Columbia had the most victims in the Clearinghouse, followed by California, Nevada, Maryland and New York. *(See Figures 5a-b)* The cities with the highest number of victims reported in the database are New York, Chicago, Los Angeles, Houston and Miami. *(See Figure 6)*

Fifty-five percent of the complaints in the Clearinghouse reported the state in which the suspect operated. The data indicates that on a *per capita* basis, (*per* 100,000 citizens), in 2001 the District of Columbia had the most suspects in the Clearinghouse, followed by Nevada, Florida, California and New York. *(See Figures 7a-b)*

---

[3]The statistics regarding consumers' age reflect the experience only of the consumers who contacted the FTC directly, and do not reflect data contributed by the SSA-OIG, which does not collect information about the victim's age.

Time Between First Misuse of Identity and Initial Discovery by Victim

Forty-four percent of victims who contacted the FTC in 2001 reported both the dates on which their information was first misused, and on which they first discovered that they were victims of identity theft.[4] 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, rather, the FTC tracks 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.

The majority of victims (69%) reported discovering they were victims of identity theft within 6 months of its first occurrence. In fact, 44% learned that they were victims of identity theft within one month of when the thief first misused their information. However, 16% were unaware of the initial misuse of their identity for more than two years.

On average, 12.3 months elapsed between the initial misuse of the consumer's identifying information and when the victim first discovered that they were identity theft victims. The 12.3 month average is about twice as long as the majorities' experience of discovering that they were identity theft victims within 6 months of its first occurrence, due to the skewing effect of the smaller number of victims who did not discover the identity theft for two years or longer. *(See Figure 8)* This skewing effect is demonstrated by other measures of the data, including the fact that amount of time most frequently reported by victims was one month (the mode), whereas the midpoint between the least amount of time reported and the greatest was 9 months (the median).

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

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

At the time of their initial contact with the FTC, 65% of victims report that they have already contacted at least one of the three major consumer reporting agencies (CRAs). Sixty-three percent of all victims, or almost 98% of the victims who had contacted a CRA, had placed a fraud alert on one or more of their credit files. *(See Figure 9)* The FTC counsels those victims who had not contacted any of the CRAs prior to contacting the FTC (35% of all victims) 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.

Almost half (49%) of all victims contacting the FTC reported that they had already contacted one or more local police departments. Forty percent of all victims contacting the FTC reported that the police department took a report of their identity theft, 9% of all victims (or 18% of victims who had already contacted the police) reported that although they contacted the police, they did not obtain a report. *(See Figure 10)* Those victims who had not yet contacted the police (51% of all victims) were advised to do so and to get a police report.

Other Information About Identity Theft

Although 87% of the victims said that they did not personally know their identity thief, 68% of the complaints in the Clearinghouse did contain 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

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

in linking seemingly unrelated complaints to a common suspect.

Only about 13% of victims who contacted the FTC indicated that they personally knew the person who had stolen and misused their identity. These relationships include family members (6%), friends, neighbors (2%) and persons known to the victim in a similar capacity (3%), roommates (1%), and personal associates from the victim's workplace (1%).

Other victims, while they did not know the suspect personally, recalled an event or incident that they believe led to the identity theft. Almost 8% reported that their wallet or purse had been lost or stolen. Mail theft or fraudulent address changes were reported by nearly 3%.

A very small number of consumers reported various other ways the thief obtained their information, including burglary, telephone or Internet solicitation, 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, pulling information off of public records, and purchasing information from the black market, can be employed without the victim's knowledge. Thus it is no surprise that nearly 80% 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. The aggregate information presented in this report is taken from identity theft victims' complaints, and provides general information about the nature of

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

identity theft. The FTC and other government entities use this information to understand more about where identity theft occurs, what forms it takes, and how victims are affected. Moreover, the Clearinghouse is a rich source of information for law enforcement investigations. In December 2001, after two years of operation, it contained over 118,000 complaints. The FTC in conjunction with the U.S. Secret Service and other government law enforcement agencies mines the Clearinghouse database to uncover significant patterns of identity theft activity in numerous complaints related to common suspects, develops investigative reports based on those complaints, and refers them out to the appropriate law enforcement officials for possible investigation and prosecution. The Clearinghouse information is also shared electronically with more than 352 law enforcement agencies nationwide via the FTC's secure law enforcement Web site, Consumer Sentinel. (*See www. consumer.gov/sentinel)*