Prepared Statement of
the Federal Trade Commission on

Identity Theft: the FTC'S Response

Before the

Subcommittee on Technology, Terrorism and Government Information
of the
Senate Judiciary Committee

Washington, D.C.

March 20, 2002

I. Introduction

Madam Chairman, and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[(1)] I appreciate the opportunity to present the Commission's views on one of the most serious consequences that can result from the misuse of consumers' personal information: identity theft.

The passage of the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act")[(2)] brought identity theft to the forefront of the public's attention. Media attention and high profile cases[(3)] have heightened concerns about the serious injury caused by identity theft.

In particular, the specter of identity theft has focused consumers' concern about the misuse of their personally identifying information. There is good reason for this concern. Identity theft can result in temporary and sometimes permanent financial loss when wages are garnished, tax refunds are withheld, or liens are placed on victims' property as a result of someone else's criminal use of their identity. Beyond direct financial loss, consumers report being denied employment, credit, loans (including mortgages and student loans), government benefits, utility and telecommunications services, and apartment leases when credit reports and background checks are littered with the fraudulently incurred debts or wrongful criminal records of an identity thief.

The 1998 legislation positioned the FTC to play a key role in the national dialogue on identity theft. The FTC enforces a number of laws that address consumers' privacy,[(4)] and intends to increase substantially the resources devoted to privacy protection. The FTC's identity theft program is an important part of that initiative. Consumer and victim assistance, data sharing with law enforcement and financial institutions, and cooperative efforts with the private sector are among the most visible examples of the FTC's efforts.[(5)] Recent FTC initiatives, including a Spanish language version of our consumer brochure, law enforcement training, and a standard Identity Theft Affidavit, complement the measures we have already undertaken to fulfill our mandate under the 1998 Act.

II. The FTC's Response to the Identity Theft Act

The Identity Theft Act directed the Commission to establish procedures to: log the receipt of complaints by victims of identity theft; provide identity theft victims with informational materials; and refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[(6)] To fulfill the purposes of the Act, the Commission implemented a plan with three principal components: a toll-free telephone hotline, a database of identity theft complaints, and consumer and business education.

(1) Toll Free Hotline. The Commission established its toll-free telephone number (the "hotline"), 1-877-ID-THEFT (438-4338) in November 1999. The hotline now responds to an average of over 3000 calls per week. When consumers call to report identity theft, the hotline counselors enter information from their complaints into the Identity Theft Data Clearinghouse (the "Clearinghouse") - a centralized database used to aid law enforcement and track trends involving identity theft.

The counselors advise the callers to contact the credit reporting agencies and the entities where the fraudulent accounts were opened in order to place a fraud alert on their credit files and shut down the fraudulent accounts, respectively. They also encourage consumers to contact their local police departments to file a police report, both because local law enforcement may be in the best position to catch and prosecute identity thieves and because a police report helps consumers demonstrate to creditors and debt collectors that they are in fact genuine victims of identity theft. Forty-seven states have enacted their own identity theft laws and the FTC hotline phone counselors, in appropriate circumstances, will refer consumers to other state and local authorities. Lastly, when another federal agency has a program in place to assist consumers, callers are referred to that agency.[(7)]

Of the callers to our hotline, thirty-four percent are seeking information about how to guard against identity theft.[(8)] The phone counselors provide suggestions on steps they should take to minimize their risk.

(2) *Identity theft complaint database.* The information that the consumers share with the phone counselors can provide the foundation for investigation. The telephone counselors enter the complaints received by the FTC through the hotline, by mail, and through the FTC's secure on-line identity theft complaint form into the FTC's Clearinghouse database. In addition, the Social Security Administration's Office of Inspector General transfers into the Clearinghouse complaints of identity theft received by its consumer hotline.

The Clearinghouse is the federal government's centralized repository of consumer identity theft complaint information. It contains detailed information regarding the identity theft victim, the suspect, and the ways the identity thief misused the victim's personal information. More than 270 law enforcement agencies nationwide have signed confidentiality agreements that grant them membership and access to the Identity Theft Data Clearinghouse. The Clearinghouse information is available directly on members' desktop PCs via the FTC's secure law enforcement Web site, *Consumer Sentinel*. Access to the Clearinghouse information supports law enforcement agencies' efforts to combat identity theft by providing a range of complaints from which to augment their ongoing investigations and spot new patterns of illegal activity.

(3) *Consumer and business education*. The FTC has taken the lead in coordinating with other government agencies and organizations to develop and disseminate comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. For example, in collaboration with other federal agencies, the FTC published a comprehensive informational booklet, *Identity Theft: When Bad Things Happen to Your Good Name,* in February 2000. Since its publication through February 2002, the FTC has distributed more than 600,000 hard copies of the booklet and recorded over 609,500 visits to our Web version. Other federal agencies have also printed and distributed this publication.

Consumers can also find comprehensive information about preventing and recovering from identify theft at the FTC's identity theft Web site, *www.consumer.gov/idtheft.* The site also links to a secure Web-based complaint form, allowing consumers to send complaints directly to the Clearinghouse. The FTC now receives an average of 400 complaints per week *via* the Internet; overall, more than 18,000 victims filed their identity theft complaints online as of the end of December 2001. The FTC's identity theft Web site had received more than 699,000 hits since it was launched in February 2000.

To expand the reach of our consumer education message, the FTC has begun an outreach effort to Spanish-speaking victims of identity theft. Just last month, we released a Spanish version of the *Identity*

Theft booklet (*Robo de Identidad: Algo malo puede pasarle a su buen nombre)* and the *ID Theft Affidavit* (discussed below in Section III). In addition, we have added Spanish-speaking phone counselors to our hotline staff. We will soon launch a Spanish version of our online complaint form.

III. The FTC's Recent Collaborative and Outreach Efforts

Over the past year, the Commission has worked closely with other government agencies and private entities to encourage the investigation and prosecution of identity theft cases, and help consumers resolve identity theft problems.

(1) *Law Enforcement*. One of our goals is to provide support for identity theft prosecutions nationwide. In the past year, the Commission launched an identity theft case referral program in coordination with the United States Secret Service, which assigned a special agent on a full-time basis to the Commission to assist with identity theft issues.[(9)] The identity theft team, assisted by the special agent, develops case leads by examining significant patterns of identity theft activity in the database and by refining the data through the use of additional investigative resources. Then, the team refers the case leads to one of the Financial Crimes Task Forces located throughout the country for further investigation and potential prosecution.

We provide support for law enforcement in other ways as well. Just last week, the FTC, in cooperation with the Department of Justice and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. This first session was held in Washington, D.C.; subsequent sessions are planned in Chicago, Dallas, and San Francisco. The training seminar provides officers with technical skills and resources to enhance their efforts to combat identity theft, including strategies for both traditional and high-tech investigations. The training also identifies key components for successful actions by local, state, and federal prosecutors, and identifies resources, such as the Clearinghouse database, that are available to law enforcement when conducting identity theft investigations. Our goal is to encourage the prosecution of these cases at all levels of government.

(2) *Private Industry.* Identity theft victims spend significant time and effort restoring their good name and financial histories. Such burdens result, in part, from the need to complete a different fraud affidavit for each different creditor where the identity thief opened or used an account in their name.[(10)] To reduce that burden, the FTC worked to develop the *ID Theft Affidavit* ("*Affidavit*"). The *Affidavit* was the culmination of an effort we coordinated with private industry and consumer advocates to create a standard form for victims to use in absolving identity theft debts with each of the creditors where identity thieves opened accounts. The *Affidavit* is accepted by the three major credit reporting agencies and many creditors. From its release in August 2001 through February 2002, we have distributed more than112,000 print copies of the *Affidavit.* There have also been nearly 185,000 hits to the Web version.

The FTC will continue working with private sector financial institutions to find additional ways to assist consumers. For example, we plan to work with businesses to highlight the importance of securing business records containing personally identifying information from would-be identity thieves, and providing consumers with notification in the event that their business records are compromised.

The FTC is examining other ways to lessen the difficulties and burdens faced by identity theft victims. One approach under consideration is to develop a joint "fraud alert initiative" with the three major credit reporting agencies ("CRAs"). This initiative would allow the FTC to transmit regularly to the three major CRAs requests from identity theft victims that fraud alerts be placed on their consumer report and copies of their reports be sent to them. This would eliminate the victim's need to contact each of the three major CRAs separately.

The CRAs have also asked the FTC to help promote their recent "police report initiative," which follows an earlier program supported by the FTC. After learning from our first twelve months of data that over 35% of victims contacting the FTC were not able to file police reports on identity theft, the FTC began working

with the International Association of Chiefs of Police ("IACP") to encourage local police officers to write police reports for victims of identity theft. In November 2000, the IACP passed a Resolution in support of providing police reports to victims of identity theft and referring victims to the FTC's hotline.[(11)] In 2001, the consumers reporting to the FTC that the police would not issue a report dropped to 18%.[(12)] Under their new initiative, the CRAs have agreed to block inaccurate information resulting from the identity thief's activities from a victim's credit report if the victim provides the CRA with a police report on the incident. This program further speeds the process of rehabilitating the victim's good name.

IV. Identity Theft: How it Happens

Access to someone's personal information, through legal or illegal means, is the key to identity theft. Unlike most crimes where the victim is immediately aware of the assault, identity theft is often silent and invisible. Identity thieves do not need direct contact with their victims. All they need is access to some key components of a victim's personal information, which, for most Americans, may be maintained and used by numerous different public and private entities. Thus, it is hardly surprising that nearly 80% of the victims who report identity theft to the FTC do not know how or where the identity thief obtained their personal information.[(13)]

Some victims can recall an event or incident that they believe led to the identity theft. Eight percent of the victims who contacted the FTC had their wallet or purse lost or stolen. Three percent of the victims discovered that their mail had been stolen or that a fraudulent address change had been filed with a creditor. One percent of victims contacting the FTC recalled giving out personal information in response to a solicitation over the telephone or Internet, and another 1% reported that their identification had been stolen from their residence or car.[(14)]

Notably, 13% of the victims who contact the FTC report that they personally know the suspect. These relationships include family members (6%), other personal relationships, such as friends (3%), neighbors (2%), "significant others" or roommates (1%), or someone from the victim's workplace (1%).

The FTC also receives reports of identity theft from victims who learn of it only upon notification by their employer or an entity with whom they do business that their employee or customer records were stolen. This is called "business record identity theft." Between March 2000 through late December 2001, the Clearinghouse received reports regarding thirty-five different companies or institutions in which identity thieves stole records containing employees' or clients' personal information. The institutions included hospitals, tax preparers, municipalities and schools.[(15)] In many of these instances the records were stolen by insiders. Some of these thieves sold the records, while others exploited the information themselves. Some of the targeted companies sought our assistance in dealing with the aftermath of the theft, and in other cases, we reached out to them to offer assistance. When we provide assistance, we encourage the entities to contact the persons whose records were compromised, notify them that they were potential victims of identity theft, and advise them to contact the FTC's hotline.

While most victims do not know how or where the identity thief obtained their personal information, 68% of the complaints in the Clearinghouse do contain some identifying information about the suspect, such as a name, address, or phone number.[(16)] This includes any identifying information victims can provide about the suspect, which might be gleaned from the bills, letters or phones calls of would-be creditors and debt collectors, or from a victim's credit report. Such information about suspects allows law enforcement investigators to link seemingly unrelated complaints of identity theft to a common suspect.

V. Summary of Database Information

The Clearinghouse database has been in operation for more than two years.[(17)] For calendar year 2001, the Clearinghouse database contains over 86,000 complaints from ID theft victims. It also contains over 31,000 inquiries from consumers concerned about becoming victims of identity theft. These figures include contacts made directly to the FTC and data contributed by SSA-OIG.

While not comprehensive, information from the database can reveal information about the nature of identity theft activity. For example, the data show that California has the greatest overall number of victims in the FTC's database, followed by New York, Texas, Florida, and Illinois. On a *per capita* basis, *per* 100,000 citizens, the District of Columbia ranks first, followed by California, Nevada, Maryland and New York. The cities with the highest numbers of victims reporting to the database are New York, Chicago, Los Angeles, Houston and Miami.

Eighty-eight percent of victims reporting to the FTC provide their age.[(18)] 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%). Consumers in their fifties comprised 13%, and those age 60 and over comprised 9%, of the victims. Minors under 18 years of age comprised 2% of the victims.

As noted above, consumers often do not become aware of the crime for some time. Forty-four percent of victims who contact the FTC provide information on when the identity theft occurred and when they discovered it. The majority of these victims (69%) reported discovering the identity theft within 6 months of its first occurrence.[(19)] In fact, 44% noticed the identity theft within one month of its occurrence. However, 5% were unaware of the theft for longer than five years. On average, 12 months elapsed between the date the identity theft occurred and when the victim discovered it.

Thirty-five percent of the victims had not yet notified any credit bureau at the time they contacted the FTC;[(20)] 46% had not yet notified any of the financial institutions involved.[(21)] Fifty-four percent of the victims had not yet notified their local police department of the identity theft. By advising the callers to take these critical steps, we enable many victims to get through the recovery process more efficiently and effectively.

The Clearinghouse data, which represents complaints received by both the FTC and the SSA-OIG, also reveal how the thieves use the stolen identifying information. This data, summarized below, help provide a broad picture of the forms identity theft can take.[(22)]

- *Credit Card Fraud:* Forty-two percent of the victims in the Clearinghouse report credit card fraud. Sixty-two percent of these victims indicate that one or more new credit cards were opened in the victims' name. Twenty-four percent of these victims indicate that unauthorized charges were made on an existing credit card. Thirteen percent of the credit card fraud victims were not specific as to new or existing credit.

- *Unauthorized Telecommunications or Utility Services:* Twenty percent of the victims in the Clearinghouse report that the identity thief obtained unauthorized telecommunications or utility equipment or services in their name. New wireless telecommunications equipment and service comprised 48% of these complaints, new land line telephone service or equipment comprised 26%, new utilities such as electric or cable service comprised 12%, 11% of these complaints were not specific, and 2% comprised unauthorized charges to the victims' existing telecommunications or utility accounts.

- *Bank Fraud:* Thirteen percent of the victims report fraud on their demand deposit (checking or savings) accounts. Forty-seven percent of these victims report fraudulent checks written on their existing account, 20% report a new bank account opened in their name, 15% report unauthorized electronic withdrawals from their account, and 18% of these complaints were not specific.

- *Employment:* Nine percent of the victims in the database report that the identity thief used their personal information for employment purposes.

- *Fraudulent Loans:* Seven percent of the victims report that the identity thief obtained a loan in their name. Fifty-three percent of these complaints relate to a personal, student, or business loan, 28% concern auto loans or leases, 10% concern real estate loans, and 9% are unspecified.

- *Government Documents or Benefits:* Six percent of the victims report that the identity thief obtained government benefits or forged government documents in their name. Forty-four percent of these victims report a false driver's license, 11% report a false social security card, and 4% report the falsification of other government documents. Thirty-one percent report fraudulent claims for tax returns, 6% report fraudulent claims for government benefits, and 3% of these victims were not specific.

- *Other Identity Theft:* Nineteen percent of the victims in the database reported various other types of identity theft. Nine percent of these victims report 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), 9% report that the thief obtained medical services, 6% report that the thief opened or accessed Internet accounts, 5% report that the thief leased a residence, 2% report that the thief declared bankruptcy in their name, 1% report that the thief purchased or traded in securities and investments, and 69% of these complaints were miscellaneous or unspecified.

- *Multiple Types:* Twenty percent of the victims in the database reported experiencing more than one of the above types of identity theft.

VI. Conclusion

Identity theft, once an unknown term, is now the subject of day time talk shows. The economic and non-economic injury caused by the misuse of consumers' personal information is significant. But there are real and positive steps we can take to alleviate the harm to consumers, and reduce the incidence of this crime. We are committed to working with our partners in the public and private sectors and will continue to forge a comprehensive approach to this challenge. I would be pleased to answer any questions you may have.

Endnotes:

1. The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner. The statistical information summarized in this statement covers the period of time from January 1 through December 31, 2001.

2. Pub. L. No. 105-318, 112 Stat. 3010 (1998).

3. Celebrities including Ted Turner, Martha Stewart and Oprah Winfrey have been reported in the press as being victims of identity theft. Jenny Lynn Bader, *Paranoid Lately? You May Have Good Reason,* N.Y. Times, March 25, 2001, at 4, Section 4.

4. *See, e.g.,* Federal Trade Commission Act, 15 U.S.C. § 41 *et seq*. (prohibiting deceptive or unfair acts or practices, including violations of stated privacy policies); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (addressing the accuracy, dissemination, and integrity of consumer reports); Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 *et seq.* (including the Telemarketing Sales Rule, 16 C.F.R. Part 310) (prohibiting telemarketers from calling at odd hours, engaging in harassing patterns of calls, and failing to disclose the identity of the seller and purpose of the call); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.* (prohibiting the collection of personally identifiable information from young children without their parents' consent); Identify Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §1028 (directing the FTC to collect identity theft complaints, refer them to the appropriate credit bureaus and law enforcement agencies, and provide victim assistance); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (requiring financial institutions to provide notices to consumers and allowing consumers (with some exceptions) to choose whether their financial institutions may share their information with third parties).

5. Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority.

6. Pub. L. No. 105-318, 112 Stat. 3010 (1998) (Codified at 18 U.S.C. § 1028(a) note).

7. For example, we may refer consumers to the Social Security Administration or their state department of motor vehicles.

8. This statistic reflects the experience only of the consumers who contacted the FTC directly, and does not reflect data contributed by the Social Security Administration, Office of Inspector General ("SSA-OIG"). *See infra* at 4. While the SSA-OIG collects many of the same fields of data, they do not collect identical data. Unless otherwise noted, as in Section IV, the statistics used in this testimony include data from FTC and SSA-OIG.

9. The referral program complements the regular use of the database by all law enforcers from their desk top computers.

10. *See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

11. While this resolution is not binding, it sends an important message to the police around the country. The FTC has conveyed the same message in numerous law enforcement conferences across the country.

12. Ninety-eight percent of victims reported whether they had been able to file a police report. The statistics regarding filing police reports 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 such information. *See supra* at note 6.

13. Nearly all of the statistics in Section IV reflect the experience only of the consumers who contacted the FTC directly, and do not reflect data contributed by the SSA-OIG. As indicated at note 6 *supra*, this is because the SSA-OIG data do not contain the same fields as the FTC data. Again, these statistics cover calendar year 2001.

14. Recent Internet scams reportedly have emerged that try to trick consumers into revealing their information. For example, consumers report receiving emails from an entity purporting to be their Internet service provider, health insurer, or bank. The scammers request personal information, to confirm the consumer's identity or eligibility for a program. In reality, these are traps for unwary consumers. We are looking for such scams and will take appropriate action.

15. Jacob H. Fries*, Worker Accused of Selling Colleagues' ID's Online*, N.Y. Times, March 2, 2002, at B2.

16. Suspect identifying information is collected both by FTC and SSA-OIG. This statistic includes data contributed by the SSA-OIG to the Clearinghouse.

17. The Clearinghouse was established in November 1999. Because it is relatively new, the information in the database may be influenced by geographical differences in consumer awareness of the FTC's identity theft hotline and database.

18. 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. *See supra* at note 6.

19. The statistics regarding when victims discover the crime and what entities they have notified 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 such information. *See supra* at note 6.

20. Ninety-five percent of victims reported whether they had contacted any credit bureaus.

21. Sixty-three percent of victims reported whether they had notified any financial institutions.

22. 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.