UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

IDENTITY THEFT

PREPARED STATEMENT OF CHARLES HARWOOD,

DIRECTOR, NORTHWEST REGION,
FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON LABOR, COMMERCE AND FINANCIAL INSTITUTIONS
WASHINGTON STATE SENATE

Olympia, Washington

January 29, 2001

Senator Prentice and members of the Committee, I am Charles Harwood, Director of the Northwest Region of the Federal Trade Commission ("FTC" or "Commission").(1) I appreciate the opportunity to present testimony on the important issue of identity theft, and to describe the Commission's efforts to help victims, alert industry and equip law enforcement to deal with this harrowing crime.(2)

In my remarks today, I will discuss the growing phenomenon of identity theft, the measures the Commission has taken to meet the goals of the federal Identity Theft and Assumption Deterrence Act of 1998 ("the Identity Theft Act") and what we see as major challenges for the future in combating identity theft.

Identity theft often seems unavoidable, undetectable and unstoppable. Public concern over identity theft is understandably enormous. This is in part because it seems to be widespread and in part because the consequences can be devastating. Consumers feel particularly vulnerable knowing that no matter how careful they are, they may nonetheless become identity theft victims.

The Identity Theft Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. As the Commission staff have strived to meet the responsibilities of the Identity Theft Act, we have learned much about the crime, its victims and its perpetrators.

I. The Federal Trade Commission's Role in Combating Identity Theft

A. The Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act of 1998 addresses identity theft in two significant ways. First, the Act strengthens the criminal laws governing identity theft. Specifically, the Act amends 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents") to make it a federal crime to: knowingly transfer [] or use [], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any

unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.(3)

The second way in which the Act addresses the problem of identity theft is by focusing on consumers as victims.(4) The Act directs that the Federal Trade Commission establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.(5)

B. The FTC's Response to Identity Theft

In enacting the Identity Theft Act, Congress recognized that coordinated efforts are essential to best serve the needs of identity theft victims, because these fraud victims often need assistance both from government agencies at the national and state or local level and from private businesses. Accordingly, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.(6)

In order to fulfill the purposes of the Act, the Commission has begun implementing a plan with three principal components:

(1) *Toll-free telephone hotline*. The Commission has established a toll-free telephone number, 1-877-ID THEFT (438-4338), that consumers can call to report identity theft. Consumers who call the hotline receive telephone counseling from specially trained personnel to help them resolve credit-related problems that may have resulted from the misuse of their identities. In addition, the hotline counselors enter information from consumers' complaints into the Identity Theft Data Clearinghouse (the "Clearinghouse") - a centralized database used to aid law enforcement and prevent identity theft.

The identity theft hotline has been in operation since November 1, 1999, and answered over 52,000 calls in its first fourteen months of operation. The hotline now answers an average of over 1500 calls per week. About forty percent of consumers who call the FTC identity theft hotline inquire about how to guard against identity theft. The counselors suggest steps consumers should take to minimize their risk. This information has been developed from the Commission's experience in advising consumers on how to avoid credit and charge card fraud and maintain financial privacy.

Around sixty percent of consumers who call the FTC identity theft hotline are victims of identity theft. The counselors give them specific information about preventing additional harm to their finances and credit histories. Consumers are instructed to contact each of the three national consumer reporting agencies to obtain copies of their credit reports and request that a fraud alert be placed on their credit reports.(7) The counselors also advise consumers to review carefully the information on their credit reports to detect any additional evidence of identity theft. Consumers are informed of their rights under the Fair Credit Reporting Act(8) and are given the procedures for correcting misinformation on their credit reports. Consumers also are advised to contact each of the creditors or service providers where the identity thief has established or accessed an account to close the account. The counselors further inform consumers of their rights under the Fair Credit Billing Act(9) and the Truth in Lending Act,(10) which, among other things, limit their responsibility for certain unauthorized charges to fifty dollars in most instances. Consumers who have been contacted by a debt collector concerning debts incurred by the identity thief are advised of their rights under the Fair Debt Collection Practices Act,(11) which proscribes debt collectors' practices.

The FTC counselors also advise consumers to notify their local police departments, both because local law enforcement may be in the best position to catch and prosecute identity thieves, and because a police report often helps consumers demonstrate to would-be creditors and debt collectors that they are genuine victims of identity theft.(12) Nearly 75% of the states have enacted identity theft laws and counselors, in appropriate circumstances, will refer consumers to other state and local authorities.

Last, if investigation and resolution of the identity theft falls under the jurisdiction of another federal agency that has a program in place to assist consumers, callers are referred to the relevant agencies. For example, consumers who complain that someone has been using their Social Security number for employment are advised to report this to the Social Security Administration's fraud hotline and to request a copy of their Social Security Statement to verify the accuracy of the earnings reported to their Social Security number.

(2) *Identity theft complaint database*. Detailed information from the complaints received on the FTC's identity theft hotline is entered into the FTC's Identity Theft Data Clearinghouse, which began operating in October 1999. As of the end of 2000, the Clearinghouse contained over 42,000 records, which are available to law enforcement agencies nationwide via the FTC's secure law enforcement website, *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 spot patterns of illegal activity. For example, law enforcement agencies may be able to more readily identify organized or large-scale identity theft rings. The Commission expects that the Clearinghouse will allow the many agencies involved in combating identity theft to share data, enabling these offices to work more effectively to track down identity thieves and assist consumers.(13)

In addition, the Clearinghouse facilitates the referral process mandated by the Identity Theft Act. Clearinghouse members can directly access the database from their desktops in order to support their investigations and identify emerging trends and patterns in identity theft in their geographic areas. The Commission also plans to disseminate complaint information through customized reports, extracting for our law enforcement partners the Clearinghouse complaints that meet the criteria they have designated. Finally, the Clearinghouse information provides policy makers with a sense of the extent of identity theft activity and the forms it is taking (*e.g.*, credit card vs. phone fraud, latest scams, etc.).

(3) *Consumer education*. The FTC's extensive multi-media campaign includes print materials, media mailings and interviews and a website, located at www.consumer.gov/idtheft.

The FTC's consumer education booklet, Identity Theft: When Bad Things Happen to Your Good Name, has been a tremendous success. The 22-page booklet covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. The FTC has distributed directly more than 156,000 copies of the booklet from February through December 2000. Another 115,000 copies have been printed and distributed by the Social Security Administration.

The identity theft website includes the booklet, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources.(14) The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Identity Theft Data Clearinghouse. The website had received more than 242,000 "page views" by end of last year and more than 4,400 complaints had been submitted electronically.

II. What the Clearinghouse Tells Us About Identity Theft

A. A Serious Problem

Many people have encountered, directly or indirectly through another person, some form of identity theft. For example, someone has used their name to open up a credit card account or used other identifying information -- Social Security number, mother's maiden name, or other personal information -- to commit fraud or engage in other unlawful activities. Other common forms of identity theft include taking over an existing credit card account and making unauthorized charges on it (typically, the identity thief forestalls discovery by the victims by contacting the credit card issuer and changing the billing address on the account); taking out loans in another person's name; writing fraudulent checks using another person's name and/or account number; and opening a telephone or wireless service

account in another person's name. In extreme cases, the identity thief may completely take over the victim's identity -- opening a bank account, obtaining multiple credit cards, buying a car, getting a home mortgage and even working under the victim's name.

Unavoidable. Although there are many steps consumers can take to minimize their risk of identity theft, there is no way to completely avoid it. One out of eight victims that call the Commission's identity theft hotline report that they have been victimized by someone they know -- either a family member, a neighbor or workplace acquaintance, someone employed by a financial institution they do business with, or in some other way known to them. Incidences of workplace identity theft appear to be increasing. Since November 1999, the Commission has received reports of hospitals, schools, and other employers whose personnel records had been compromised by an identity thief. Each such instance has the potential to result in hundreds of identity theft victims. In these cases, where someone has access to personal information because of their relationship to the victim, identity theft may be unavoidable.

The majority of victims do not know how their identifying information was compromised. The question these victims most commonly ask when they call the FTC's identity theft hotline is, "how could this have happened to me?" Unfortunately, there are a multitude of ways. For example, identity theft can arise from simple, low-tech practices such as stealing someone's mail or "dumpster diving" through the trash to collect credit card offers or obtain identifying information such as account numbers or Social Security numbers. There are also far more sophisticated practices being employed. In a practice known as "skimming," identity thieves use computers to read and store the information encoded on the magnetic strip of an ATM or credit card when that card is inserted through either a specialized card reader or a legitimate payment mechanism (*e.g.*, the card reader used to pay for gas at the pump in a gas station). Once stored, that information can be re-encoded onto any other card with a magnetic strip, instantly transforming a blank card into a machine-readable ATM or credit card identical to that of the victim.

The Internet has dramatically altered the potential occurrence and impact of identity theft. First, the Internet provides access to identifying information, through both illegal and legal means. The global publication of identifying details that previously were available only to a select few, increases the potential for misuse of that information. Second, the ability of the identity thief to purchase goods and services from innumerable e-merchants expands the potential harm to the victim through numerous purchases that are accomplished in a shorter period of time than if done in person. The explosion of financial services offered on-line, such as mortgages, credit cards, bank accounts and loans, provides a sense of anonymity to those potential identity thieves who would not risk committing identity theft in a face-to-face transaction.

Undetectable. In many instances, identity theft goes undetected by creditors, law enforcement and the victims for months or even years. One caller to the FTC's identity theft hotline reported that his wallet was stolen in 1992. This consumer was unaware that he was the victim of identity theft until seven years later, when, in the summer of 1999, he was arrested on an outstanding warrant for an offense committed by the identity thief in 1993. The consumer spent several nights in jail and was forced to post $15,000 bond. He was also shocked and dismayed to discover multiple outstanding criminal charges against him in several states as a result of the identity thief's activities. This example, while unusual, is not unique. The FTC has received numerous reports from consumers who were not aware that they had been victimized by an identity thief until four or more years after the first fraudulent transaction.

Unstoppable. For victims of identity theft, the costs can be significant and long-lasting. Where the identity thief has committed a crime in the victim's name, the harm is especially pernicious. In the worst cases, the negative consequences are never completely eradicated. For example, one consumer who called the FTC identity theft hotline reported that her income tax refund was withheld due to past child support she was believed to have owed. She found out that a child was born to a person using her name and Social Security number in a state she had never even visited. Another consumer reported that he is unable to renew his driver's license or register to vote because, due to crimes committed in his name by another person, he is considered to be on probation for federal law violations including possession of drugs with intent to distribute and fraud. More than one consumer has been denied employment when a background check or security clearance showed criminal records relating to an offense committed by someone using their names and Social Security numbers. Another consumer lost his job when, as part

of his promotion review, a background check indicated that he had a criminal record. Although the consumer went to court and obtained a declaration that he did not have a criminal record, he lost his job because the company that performed the background check said that it could not clear his record.

Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even where the individual consumer is not legally liable for these debts,(14) the consequences to the consumer are often considerable. A consumer's credit history is frequently scarred, and he or she typically must spend numerous hours over the course of months or even years contesting bills and correcting credit reporting errors. Creditors for the fraudulent accounts often continue to harass the consumer. In the interim, the consumer victim may be denied loans, mortgages and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts. Moreover, even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer.

B. Patterns and Practices: Specific Complaint Data(15)

The Identity Theft Data Clearinghouse provides law enforcement with the first opportunity to collect and consolidate identity theft complaints on a nationwide basis. The basic complaint data for 2000 shows that the most common forms of identity theft reported during the first fourteen months of operation were:

- *Credit Card Fraud* - Nationally, approximately 50% of the consumer victims reported credit card fraud -- i.e., a credit card account opened in their name or a "takeover" of their existing credit card account, while in Washington the percentage was approximately 44%;
- *Communications Services* - Nationally, approximately 25% reported that the identity thief opened up telephone, cellular, or other utility service in their name, while in Washington the percentage was approximately 28%;
- *Bank Fraud* - Nationally, approximately 16% reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written, while in Washington the percentage was approximate 23%;
- *Fraudulent Loans* - Nationally, approximately 9% reported that the identity thief obtained a loan, such as a car loan, in their name, while in Washington the percentage was approximately 7%; and
- *Government Documents* - Nationally and in Washington, approximately 8% reported that the identity thief had obtained or forged a government document such as a driver's license, filed a fraudulent document such as a tax return, or obtained government benefits in their name.

Not surprisingly, the states with the largest populations account for the largest numbers of complainants and suspects. California had over 4800 complainants, New York, Florida, and Texas each had over 1900, while Illinois had over 1300. Washington had about 700 complainants.

Nationally, about 71% of victims calling the identity theft hotline report their age; in Washington, the comparable number is 73%. Of those who provide this information, nationally and in Washington, 29% fall between 30 and 41 years of age. Approximately 21% are between age 41 and 50 nationally, and approximately 23% in Washington. Another 27% nationally and 26% in Washington are between 19 and 30. About 8% nationally and 7% in Washington reported their ages as 65 and over; and finally, about 2% nationally and in Washington are age 18 and under.

Consumers also report the harm to their reputation or daily life. The most common non-monetary harm reported by consumers is damage to their credit report through derogatory, inaccurate information. The negative credit information leads to the other problems most commonly reported by victims, including loan denials, bounced checks and rejection of credit cards. Identity theft victims also report repeated contacts by debt collectors for the bad debt

incurred by the identity thief. Many consumers report that they have to spend significant amounts of time resolving these problems.

Consumers also report problems with the institutions that provided the credit, goods, or services to the identity thief in the consumers' name. These institutions often attempt to collect the bad debt from the victim, or report the bad debt to a consumer reporting agency, even after the victim believes that he or she has shown that the debt is fraudulent. Consumers further complain that these institutions' inadequate or lax security procedures failed to prevent the identity theft in the first place; that customer service or fraud departments were not responsive; or that the companies refused to close or correct the unauthorized accounts after notification by the consumer.

IV. Next Steps

The Commission has made significant strides in assisting consumers and law enforcement to combat identity theft but recognizes that much remains to be done.

For instance, the Identity Theft Act authorizes the Commission to refer consumer identity theft complaints and information to the three major national consumer reporting agencies and other appropriate entities. The Commission has been working with the three major national consumer reporting agencies to develop a process to share key information from victims' complaints with them. The Commission also has been working with the consumer reporting agencies to develop a streamlined process that would decrease the amount of time spent by consumer victims correcting credit report errors. Paramount in this process would be the ability of a consumer to make a single call to report himself or herself as a victim of identity theft to the FTC or one of the three major national consumer reporting agencies and to have a fraud alert posted on the credit reports from each of the reporting agencies. Currently, a victim of identity theft must notify each of the three national consumer reporting agencies separately and then typically make additional calls to the FTC and to all creditors.

The Commission is also working with private industry and consumer advocates to develop a standardized fraud declaration for creditors. Currently, in order to clear up the fraudulent accounts or unauthorized charges incurred by the identity thief, a consumer must submit different affidavits and supporting documents to each creditor involved. The standard fraud affidavit would be a single form that would be accepted by multiple creditors, thereby significantly reducing the victim's burden in terms of time and copying costs.

Further, the Commission will soon begin sharing certain limited information from its Identity Theft Clearinghouse with banks, creditors and other businesses whose practices are frequently associated with identity theft complaints. The goal is to encourage and enable industry and individual companies to develop better fraud prevention practices and consumer assistance techniques. To that end, the Commission convened a workshop for industry, consumer groups, the public and law enforcement on identity theft victim assistance on October 23-24, 2000.(16) Shortly after the FTC workshop, the Social Security Administration Inspector General's Office, the Department of Justice and the U.S. Secret Service convened workshops on preventing, investigating and prosecuting identity theft.

V. Conclusion

The Identity Theft Data Clearinghouse demonstrates that identity theft is a serious and growing problem, but it also reveals ways to curb this growth. The Clearinghouse, the toll-free hotline counselors and the consumer education campaign have begun to address the serious problems associated with identity theft. Heightened awareness by consumers and businesses will also help reduce the occurrences of this fraud. The Commission looks forward to continued collaboration and cooperation between government agencies, law enforcement, policy makers and the private sector in these efforts.

Endnotes

1. This testimony represents the views of Northwest Regional Office and the staff of the Bureau of Consumer Protection of the Federal Trade Commission. They are not necessarily the views of the Federal Trade Commission or any Commissioner.

2. Pub. L. No. 105-318, 112 Stat. 3007 (1998)(codified at 18 U.S.C. § 1028).

3. 18 U.S.C. § 1028(a)(7). The statute further broadens "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code and telecommunication identifying information.

4. Because individual consumers' financial liability is often limited, where, for example, a credit card is stolen and misused, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. See S. Rep. No. 105-274, at 4 (1998).

5. Pub. L. No. 105-318 § 5, 112 Stat. 3010 (1998).

6. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Jeremy Martinez d/b/a Info World*, Amended Temporary Restraining Order, 00 Civ 12701 (C.D. Cal. Dec. 5, 2000) <http://www.ftc.gov/opa/2000/12/martinez.shtm> (granting temporary restraining order to prevent the illegal sale of the fake ID templates); *FTC v. J.K. Publications, Inc., et al*, 99 F. Supp.2d. 1176 (C.D. Cal. Apr. 10, 2000)(granting summary judgment for the FTC in case alleging that defendants obtained consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services), later proceedings at *FTC v. J.K. Publications, Inc., et al*, 99 Civ 00044 (C.D. Cal. Aug. 30, 2000)(final order awarding $37.5 million in redress); *FTC v. Rapp*, No. 99-WM-783 (D. Colo. filed Apr. 21, 1999) (alleging that defendants obtained private financial information under false pretenses)(Stipulated Consent Agreement and Final Order entered June 23, 2000). The practices the Commission expects to focus its law enforcement resources on are those where the injury is widespread and where civil remedies are likely to be effective.

7. These fraud alerts require that the consumer be contacted when new credit is requested in that consumer's name.

8. 15 U.S.C. §§ 1681 *et seq*.

9. 15 U.S.C. § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

10. 15 U.S.C. §§ 1601 *et seq*.

11. 15 U.S.C. §§ 1692 *et seq*.

12. In December 2000, the International Association of Chiefs of Police (IACP) adopted a resolution in support of writing reports on ID theft crime and referring victims to the FTC ID theft hotline.

13. The Commission has been working closely with other agencies to establish a coordinated effort to identify the factors that lead to identity theft, work to minimize those opportunities, enhance law enforcement and help consumers resolve identity theft problems. The first such event was the Commission's April 1999 meeting with representatives of approximately a dozen federal agencies as well as the National Association of Attorneys General to discuss the implementation of the consumer assistance provisions of the Identity Theft Act. FTC staff works with the Identity Theft Subcommittee of the Attorney General's Council on White Collar Crime to coordinate law enforcement strategies and

initiatives. FTC staff also coordinates with staff from the Social Security Administration's Inspector General's Office on the handling of social security number misuse complaints, a leading source of identity theft problems.

14. www.consumer.gov is a federal "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It currently has links to information from more than 170 federal agencies.

15. The Truth in Lending Act, 15 U.S.C. §§ 1601 et seq. and the Electronic Fund Transfer Act, 15 U.S.C. §§ 1693 *et seq*. limit consumers' liability for fraudulent transactions in connection with credit and debit cards, respectively.

16. Data used in this analysis are for November 1999 through December 2000. (See charts included with this testimony as attachments).

17. Transcripts of the workshop are posted on the FTC's identity theft Web site. (http://www.ftc.gov/bcp/workshops/idtheft/transcripts.shtm)