PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON

FINANCIAL IDENTITY THEFT

Before the

SUBCOMMITTEE ON
TELECOMMUNICATIONS, TRADE AND CONSUMER PROTECTION

and the

SUBCOMMITTEE ON
FINANCE AND HAZARDOUS MATERIALS

of the

COMMITTEE ON COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

April 22, 1999

Mr. Chairman Tauzin, Mr. Chairman Oxley, and members of the Subcommittees, I am Jodie Bernstein, 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 the important issue of financial identity theft.

In my remarks today, I will discuss the increasingly common problem of identity theft, the role of the FTC in addressing this problem under the recently enacted Identity Theft and Assumption Deterrence Act[(2)], and the steps the Commission is taking to aid consumers who become identity theft victims. I will also briefly address one of the notable ways in which identity theft can occur in the financial services industry -- "pretexting," *i.e.*, obtaining private financial information from banks and others under false pretenses.

I. Identity Theft: the Problem

Identity theft occurs when someone uses the identifying information of another person -- name, social security number, mother's maiden name, or other personal information -- to commit fraud or engage in other unlawful activities. For example, an identity thief may open up a new credit card account under someone else's name. When the identity thief fails to pay the bills, the bad debt is reported on the victim's credit report. 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 using personal information to access, and transfer money out of, another person's bank or brokerage account. In extreme cases, the identity thief may completely take over his or her victim's identity -- opening a bank account, getting multiple credit cards, buying a car, getting a home mortgage and even working under the victim's name.[(3)]

Identity theft almost always involves a financial services institution in some way -- as a lender, holder of a bank account, or credit card or debit card issuer -- because, as the bank robber Willie Sutton observed, that is where the money is. Identity theft involving financial services institutions, furthermore, is accomplished through a wide variety of means. Historically, identity thieves have been able to get the personal information they need to operate through simple, "low-tech" methods: intercepting orders of new checks in the mail, for example, or rifling through the trash to get discarded bank account statements or pre-approved credit card offers. Sometimes, identity thieves will try to trick others into giving up this information. As discussed in more detail below, one way in which identity thieves do this is by "pretexting," or calling on false pretenses, such as by telephoning banks and posing as the account holder. In other cases, the identity thief may contact the victim directly. In one recent scheme, fraud artists have reportedly been preying on consumers' fears about Year 2000 computer bugs; a caller, for example, represents that he or she is from the consumer's bank and tells the consumer that the caller needs certain information about the consumer's account (or needs to transfer money to a special account) in order to ensure the bank can comply with Year 2000 requirements.[(4)]

Other methods of identity theft may involve more sophisticated techniques. 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. In addition, the increased availability of information on the Internet can facilitate identity theft.[(5)]

For individuals who are victims of identity theft, the costs can be significant and long-lasting. 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,[(6)] 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 sometimes over the course of months or even years contesting bills and straightening out credit reporting errors. 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 are tainted and a new account is essential. 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.

Although comprehensive statistics on the prevalence of identity theft are not currently

available, the available data suggest that the incidence of identity theft has been increasing in recent years. The General Accounting Office, for example, reports that consumer inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department increased from 35,235 in 1992 to 522,922 in 1997,[(7)] and that the Social Security Administration's Office of the Inspector General conducted 1153 social security number misuse investigations in 1997 compared with 305 in 1996.[(8)]

II. The Federal Trade Commission's Authority

A. *Overview*

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTC Act"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(9)] With certain exceptions, the FTC Act provides the Commission with broad civil law enforcement authority over entities engaged in or whose business affects commerce,[(10)] and provides the authority to gather information about such entities.[(11)] The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices.[(12)]

Among the Commission's statutory mandates of particular relevance here are the Fair Credit Billing Act and Fair Credit Reporting Act, which provide important protections for consumers who may be trying to clear their credit records after having their identities stolen. The Fair Credit Billing Act, which amended the Truth in Lending Act, provides for the correction of billing errors on credit accounts and limits consumer liability for unauthorized credit card use.[(13)] The Fair Credit Reporting Act ("FCRA") regulates credit reporting agencies and places on them the responsibility for correcting inaccurate information in credit reports.[(14)] In addition, the FCRA limits the disclosure of consumer credit reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment or similar purposes) and under specified conditions (such as certifications from the user of the report).[(15)]

B. *The FTC's Activities With Respect to the Financial Services Industry and Financial Privacy*

The Commission has extensive experience in addressing consumer protection issues that arise in the financial services industry, involving, for example, the use of credit cards, lending practices, and debt collection.[(16)] The Commission also provides consultation to Congress and to the federal banking agencies about consumer protection issues involving financial services. The Commission periodically provides comments to the Federal Reserve Board regarding the Fair Credit Reporting Act, and the implementing regulations for the Truth in Lending Act, the Consumer Leasing Act, the Electronic Funds Transfer Act, and the Equal Credit Opportunity Act.[(17)]

In addition, The FTC has taken an active role in addressing a range of issues involving consumer privacy, including the privacy of personal financial information. Thus, for example, the Commission has recently reported to or testified before Congress and/or held public workshops on online privacy, individual reference services, pretexting, financial privacy, and the implications of electronic payment systems for individual privacy.

C. *The FTC's Role in Addressing Identity Theft*

As an outgrowth of its broader concern about financial privacy, the Commission has been involved in the issue of identity theft for some time. In 1996, the Commission convened two public meetings in an effort to learn more about identity theft, its growth consequences, and possible responses. At an open forum held in August 1996, consumers who had been victims of this type of fraud, representatives of local police organizations and other federal law enforcement agencies, members of the credit industry, and consumer and privacy advocates discussed the impact of identity theft on industry and on consumer victims. Subsequent press coverage helped to educate the public about the growth of consumer identity theft and the problems it creates. In November 1996, industry and consumer representatives reconvened in working groups to explore solutions and ways to bolster efforts to combat identity theft.

Having thereby developed a substantial base of knowledge about identity theft, the Commission testified before the Senate Judiciary Committee in May 1998 in support of the Identity Theft and Assumption Deterrence Act.

III. The Identity Theft and Assumption Deterrence Act of 1998

Last fall, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act" or "Act").[(18)] The Act 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.[(19)]

Previously, 18 U.S.C. § 1028 addressed only the fraudulent creation, use, or transfer of identification documents, and not theft or criminal use of the underlying personal information. Thus, the Act criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents. Furthermore, one who violates this prohibition and thereby obtains anything of value aggregating to $1000 or more during any one-year period, is subject to a fine and imprisonment of up 15 years.[(20)] These criminal provisions of the Act are enforced by the U.S. Department of Justice, working with investigatory agencies including the U.S. Secret Service, the Federal Bureau of Investigation, and the U.S. Postal Inspection Service.

The second way in which the Act addresses the problem of identity theft is by improving

assistance to victims.[21] In particular, the Act provides for a centralized complaint and consumer education service for victims of identity theft, and gives the responsibility of developing this service to the Federal Trade Commission. The Act directs that the 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.[22]

IV. Current Efforts: the FTC's Consumer Assistance Program

In enacting the Identity Theft Act, Congress recognized that coordinated efforts in this area are essential to best serve identity theft victims. Accordingly, the FTC's role under the Act is primarily one of managing information sharing among public and private entities in support of criminal law enforcement efforts,[23] and aiding victims by serving as a central, Federal source of information. In order to fulfill the purposes of the Act, the Commission has developed and begun implementing a plan that centers on three principal components[24]:

(1) *Toll-free telephone line*. The Commission plans to establish a toll-free telephone number that consumers can call to report identity theft and to receive information and referrals to help them to resolve the problems that may have resulted. The identity theft toll-free number will build on the success of the Commission's two-year-old Consumer Response Center, a general purpose hotline for consumer information and complaints.

(2) *Identity theft complaint database*. The Commission is developing a database to track the identity theft complaints received by the FTC and other public and private entities. This database will allow the Commission to monitor better the extent and nature of identity theft. Moreover, the Commission expects that the database will enable the many agencies involved in combating identity theft to share and manage data so as to more effectively track down identity thieves and assist consumers.[25] For example, criminal law enforcement agencies could take advantage of a central repository of complaints to spot patterns that might not otherwise be apparent from isolated reports. In addition, a consumer with a concern that his or her social security number has been misused would not -- and should not -- need to call all the many federal agencies that could possibly be involved to ensure that the complaint was directed to the appropriate people. Under the planned system, the consumer could make a single phone call to one central number (the FTC's or that of any other agency sharing data with the Commission), to report the offense, have it referred to the appropriate agency, and receive additional information and assistance.

(3) *Consumer Education Materials*. A number of public and private organizations have published or begun developing materials that provide information on particular aspects of identity theft. The FTC is coordinating with others, both within and outside the government, to develop unified, comprehensive consumer education materials for victims of identity theft, and those concerned with preventing identity theft, and to make this information widely available.

Commission staff has been working hard to implement these plans. Phone counselors in our

Consumer Response Center have been trained to handle identity theft complaints, and our general complaint database has been modified so as to permit entry of at least basic information about the identity theft complaints we already receive. In addition, we have recently issued a Consumer Alert that provides an overview of the steps consumers should take if they become victims of identity theft. We are also working with other government agencies to launch a web page in the near future devoted to identity theft information. The web page, which will include links to information from a number of government agencies, will be located on www.consumer.gov, the federal government's central site for consumer information.[(26)]

The Commission, in fact, has been working closely with other agencies in a number of ways in our effort to help consumers. For example, FTC staff has been working with the identity theft subcommittee of the Attorney General's Council on White Collar Crime to provide interim guidance to law enforcement field offices on how best to assist identity theft victims, and with the Social Security Administration's Inspector General to coordinate the handling of social security number misuse complaints. Most recently, Commission staff hosted a meeting on April 20, 1999, with representatives of approximately a dozen federal agencies as well as the National Association of Attorneys General. The meeting brought together individuals involved in diverse aspects of identity theft to discuss the implementation of the consumer assistance provisions of the Identity Theft Act. In particular, Commission staff sought input from others in the design of the identity theft complaint database, to ensure that the FTC captures the information most useful to other agencies in both assisting consumers and catching identity thieves. In addition, this meeting was the first step in the FTC's efforts to develop a single set of consumer education materials. The Commission expects that a number of agencies will be working jointly with the Commission on this project to ensure that consumers have the best information possible on preventing and recovering from identity theft.

V. Pretexting

Related to identity theft is a practice known in the information broker industry as "pretexting." Pretexting involves obtaining confidential consumer information under false pretenses, *e.g.*, by lying and pretending to be the consumer. This tactic appears to be gaining popularity in response to the booming market for comprehensive personal information relating to consumers. Today, many information brokers tout their ability to obtain sensitive financial information -- including current bank or brokerage account numbers and balances, which are not publicly available -- without the subject ever knowing.[(27)] Pretexting is the method they use to obtain this information.

Pretexting may harm consumers in two related ways. First, there may be a significant invasion of the consumer's privacy resulting from the disclosure of private financial information through pretexting. Second, pretexting also may increase the risk of identity theft, resulting in serious economic harm. For example, using account balances and numbers obtained from a pretexter, an identity thief could deplete a bank account or liquidate a stock portfolio. The Commission just voted to file a complaint in federal district court against alleged pretexters. I will be prepared to discuss it at the hearing and the Commission will

provide the Committee with a copy of its complaint and the concurring and dissenting statements of the Commissioners as soon as possible.

VI. Conclusion

Financial identity theft clearly continues to present a significant threat to consumers. The FTC looks forward to working with the Committee to find ways to prevent this crime and to assist its victims.

---

1. This written statement represents the views of the Federal Trade Commission. My oral presentation and response to questions are my own, and do not necessarily represent the views of the Commission or any Commissioner.

2. Pub. L. No. 105-318, 112 Stat. 3007 (1998).

3. In at least one case, an identity thief reportedly even died using the victim's name, and the victim had to get the death certificate corrected. Michael Higgins, *Identity Thieves*, ABA Journal, October 1998, at 42, 47.

4. Federal trade Commission, Y2K? Y2 Care: Protecting Your Finances from Year 2000 Scam Artists (Consumer Alert, March 1999).

5. *See, e.g.*, Federal Trade Commission, Individual Reference Services: A Report to Congress (December 1997) (examining computerized databases or "look-up services" that disseminate personally identifiable information on individuals, often through on-line access). With the FTC's encouragement, members of the individual reference services industry have adopted voluntary guidelines, effective December 31, 1998, limiting the availability of certain types of personal information.

6. The Fair Credit Billing 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.

7. Calls to this department included "precautionary" phone calls, as well as calls from actual fraud or identity theft victims.

8. U.S. General Accounting Office, Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (May 1998). The Social Security Administration attributed the increase in investigations, in part, to the hiring of additional investigators.

9. 15 U.S.C. § 45(a).

10. Certain entities such as banks, savings and loan associations, and common carriers as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

11. 15 U.S.C. § 46(a).

12. In addition to the credit laws discussed in the text, the Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the

provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

13. 15 U.S.C. §§ 1601 *et seq.*

14. 15 U.S.C. §§ 1681e, 1681i .

15. 15 U.S.C. § 1681-1681u.

16. For example, in 1992, Citicorp Credit Services, Inc., a subsidiary of Citicorp, agreed to settle charges that it aided and abetted a merchant engaged in unfair and deceptive activities. *Citicorp Credit Services, Inc.*, 116 F.T.C. 87 (1993). In 1993, the Shawmut Mortgage Company, an affiliate of Shawmut Bank Connecticut, N.A., and Shawmut Bank, agreed to pay almost one million dollars in consumer redress to settle allegations that it had discriminated based on race and national origin in mortgage lending. *United States v. Shawmut Mortgage Co.*, 3:93CV-2453AVC (D. Conn. Dec. 13, 1993). The Commission brought the *Shawmut* case jointly with the United States Department of Justice. In 1996, the J.C. Penney Company entered into a consent decree and paid a civil penalty to resolve allegations that the company failed to provide required notices of adverse actions to credit applicants. *United States v. J.C. Penney Co.*, CV964696 (E.D.N.Y. Oct. 8, 1996). In 1998, in conjunction with the law enforcement efforts of several state attorneys general, the Commission finalized a settlement agreement with Sears, Roebuck and Company that safeguards at least $100 million in consumer redress based on allegations that the company engaged in unfair and deceptive practices in its collection of credit card debts after the filing of consumer bankruptcy. *Sears, Roebuck and Co.*, C-3786, 1998 FTC LEXIS 21 (Feb. 27, 1998). The Commission also worked with state attorneys general in resolving allegations against other companies that involved practices in the collection of credit card debts after the debtors had filed for bankruptcy. *Montgomery Ward Corp.*, C-3839 (Dec. 11, 1998); *May Department Stores Co.*, File No. 972-3189, 1998 FTC LEXIS 117 (Nov. 2, 1998).

17. Commission staff participates in numerous task forces and groups concerned with, for example, fair lending, leasing, subprime lending, electronic commerce, and fraud on the Internet, all of which have an impact on the financial services industry.

18. Pub. L. No. 105-318, 112 Stat. 3007 (1998).

19. 18 U.S.C. § 1028(a)(7). The statute further defines "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.

20. If the $1000 threshold is not met, the maximum penalty is three years imprisonment. The maximum penalty is increased to 20 years imprisonment if the identity theft offense is committed to facilitate a drug trafficking crime or in connection with a crime of violence, and 25 years if the offense is committed to facilitate an act of international terrorism.

21. Because individual consumers' financial liability is often limited, 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).

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

23. Most identity theft cases are best addressed through criminal prosecution. 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. The practices the Commission expects to focus its law enforcement resources on are those where the effect is widespread and where civil remedies are likely to be effective. *See, e.g., FTC v. J.K. Publications, Inc., et al*, Docket No. CV 99-00044 ABC (AJWx) (C.D. Cal., filed January 5, 1999) (Alleging that defendants obtained consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services).

24. In the Identity Theft Act, Congress authorized the appropriation of such sums as may be necessary to carry out the FTC's obligations under the Act. Pub. L. No. 105-318 § 5(b), 112 Stat. 310 (1998). These plans are, of course, contingent on the actual appropriation of such funds. Should the volume of calls received from consumers approach the levels reported by Trans Union to the General Accounting Office, the appropriation required to respond to these calls may be substantial.

25. The Commission has successfully undertaken a similar effort with respect to telemarketing fraud. The FTC's Consumer Sentinel network is a bi-national database of telemarketing, direct mail, and Internet complaints used by law enforcement officials throughout the U.S. and Canada.

26. http://www.consumer.gov is a multi-agency effort, with technical maintenance provided by the FTC. It contains a wide array of consumer information and currently has links to information from 61 federal agencies.

27. *Id.* At last summer's hearings before the House Banking and Financial Services Committee, former and current information brokers described the recent explosion in the number -- from a handful to hundreds -- of information brokers offering confidential financial information, and noted that there are currently hundreds of Web pages available on the Internet advertising the ability of information brokers to obtain such information. *See Obtaining Confidential Financial Information by Pretexting: Hearings Before the House Comm. on Banking and Financial Services*, 105th Cong. (1998) (statements of Al Schweitzer, Robert Douglas).