

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

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 - 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 fling 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. In the card reader

271.15 T1-12(de)4(r)3.io2(m)-2(a)-1623r-20(y)6(m)-0(ne)4(t)-2(i)-2(c)4()-10(s)-1(t)-2(r)3(i)23r-20(y)

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, and that the Social Security Administration's Office of the Inspector General conducted 1153 social security number misuse investigations in 1997 compared to 100 in 1992. (b) (6)

is

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 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 to 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 improv

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⁾

Consumer Response Center have been trained to handle identity theft complaints, a 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

provide the Committee with a copy of its complaint and the concurring and dissenting

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., *J.K. Publications, Inc., et al*, Docket No. CV 990044 ABC (AJWx) (C.D. Cal., filed January 5, 1999) (Alleging that defendant 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. 105-58 § 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's 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