PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

On

IDENTITY THEFT: PREVENTION AND VICTIM ASSISTANCE

Before the
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE
of the
HOUSE FINANCIAL SERVICES COMMITTEE
Washington, D.C.
June 24, 2003

INTRODUCTION

Mr. Chairman, and members of the Subcommittee, 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 the impact of identity theft on consumers and the importance of information security in preventing identity theft.

The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. The FTC's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[2] The 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. The Commission also works extensively with industry on ways to improve victim assistance, including providing direct advice and assistance in cases when information has been compromised. The Commission can take enforcement action when companies fail to take adequate security precautions to protect consumers' personal information.

THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The Identity Theft Act strengthened the criminal laws governing identity theft[3] and focused on consumers as victims.[4] Congress also 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 businesses. As a result, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[5] Specifically, Congress directed the Commission to 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.[6] To fulfill the Act's mandate, the Commission has implemented a plan that focuses on three principal components: (1) A toll-free telephone hotline, (2) the Identity Theft Data Clearinghouse (the "Clearinghouse"), a centralized database used to aid law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

A. Assisting Identity Theft Victims

The most immediate way in which the FTC assists victims is by collecting complaints and providing advice on recovery through a telephone hotline and a dedicated website. On November 1, 1999, the Commission began collecting complaints from consumers via a toll-free telephone number, 1-877-ID THEFT (438-4338). Every year since has seen an increase in complaints. In 2002, hotline counselors added almost 219,000 consumer records to the Clearinghouse, up from more than 117,000 in 2001. Of the 219,000 records, almost 162,000 (74%) were complaints from identity theft victims, and almost 57,000 (26%) were general inquiries about identity theft. Despite this dramatic growth in reports of identity theft, the FTC is cautious in attributing it entirely to a commensurate growth in the prevalence of identity theft. The FTC believes that the increase is, at least in part, an indication of successful outreach in informing the public of its program and the availability of assistance.

Callers to the hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the

misuse of their identities. Victims are advised to: (1) place a fraud alert on their credit reports and review their credit reports for additional fraudulent accounts;[7] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the Fair Credit Reporting Act,[8] the Fair Credit Billing Act,[9] the Truth in Lending Act,[10] and the Fair Debt Collection Practices Act.[11] If the investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form, which allows victims to enter their identity theft information for input into the Clearinghouse. Victims also can read and download all of the resources necessary for reclaiming their credit record and good name. One resource in particular is the FTC's tremendously successful consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*. The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims, how to correct credit-related and other problems that may result from identity theft, tips for those having trouble getting a police report taken, and advice on ways to protect personal information. It also describes federal and state resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its release in February 2000.[12] Last year, the FTC released a Spanish language version of the Identity Theft booklet, *Robo de Identidad: Algo malo puede pasarle a su buen nombre.*

B. Outreach and Education

The Identity Theft Act also directed the FTC to provide information to consumers about identity theft. Recognizing that law enforcement and private industry play an important part in the ability of consumers both to minimize their risk and to recover from identity theft, the FTC expanded its mission of outreach and education to include these sectors.

(1) *Consumers*: The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

To increase identity theft awareness for the average consumer, the FTC recently developed a new primer on identity theft, *ID Theft: What's It All About?* This publication discusses the common methods of identity thieves, how consumers can best minimize their risk of being victimized, how to identify the signs of victimization, and the basic first steps for victims. Taken together with the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name*, the two publications help to fully educate consumers.

(2) *Law Enforcement*: Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described below (*see infra* Section II.C.), the staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General letting him or her know about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. The letter encourages the Attorney General to link to the consumer information and complaint form on the FTC's website and to let residents know about the hotline, stresses the importance of the Clearinghouse as a central database, and describes all of the educational materials that the Attorney General can distribute to residents. North Carolina took the lead in availing itself of the Commission's resources in putting together for its resident victims a package of assistance that includes the ID Theft Affidavit (*see* Section II.B.(3)(a)) and links to the FTC website, www.consumer.gov/idtheft. Through this initiative, the FTC hopes to make the most efficient use of federal resources by allowing states to take advantage of the work the FTC has already accomplished and at the same time continuing to expand the centralized database of victim complaints and increase its use by law enforcement nationwide. Other outreach initiatives include: (1) Participation in a "Roll Call" video produced by the Secret Service, which will be sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (2) redesigning of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations. The FTC will launch the new website this summer.

(3) *Industry*:

(a) *Victim Assistance*: Identity theft victims spend significant time and effort restoring their good name and financial records. As a result, the FTC devotes significant resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.[(13)] To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001 through April 2003, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been more than 356,000 hits to the Web version. The affidavit is available in both English and Spanish.

The three major credit reporting agencies ("CRAs") recently launched a new initiative, the "joint fraud alert." After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each CRA now shares that request with the other two CRAs, thereby eliminating the requirement that the victim contact each of the three major CRAs separately.

(b) *Information Security Breaches*: Additionally, the FTC is working with institutions that maintain personal information to identify ways to help keep that information safe from identity theft. Last year, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records. The FTC will soon publish a self-assessment guide to make businesses and organizations of all sizes more aware of how they manage personal information and to aid them in assessing their security protocols.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest[(14)] and Ford/Experian,[(15)] in which tens of thousands of consumers' files were compromised, the Commission advised how to notify those individuals and how to protect the data in the future. To provide better assistance in these types of cases, the FTC developed a kit, *Responding to a Theft of Customer or Employee Information*, that will be posted on the identity theft website in the coming weeks. The kit provides advice on which law enforcement agency to contact, depending on the type of compromise, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. The kit also includes a form letter for notifying the individuals whose information was taken. Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

The FTC particularly stresses the importance of notifying individuals as soon as possible when information has been taken that may put them at risk for identity theft. They can then begin to take steps to limit the potential damage to themselves. Individuals who place a fraud alert promptly have a good chance of preventing, or at least reducing, the likelihood that the release of their information will turn into actual misuse. Prompt notification also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that they should become victims, they can quickly take action to clear their records before any long-term damage is done. Besides providing *Responding to a Theft of Customer or Employee Information*, FTC staff can provide individual assistance and advice, including review of consumer information materials for the organization and coordination of searches of the Clearinghouse for complaints with the law enforcement officer working the case.

C. Identity Theft Data Clearinghouse

The final mandate for the FTC under the Identity Theft Act was to log the complaints from victims of identity theft and refer those complaints to appropriate entities such as law enforcement agencies. Before launching this complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement, including meeting with a host of law enforcement and regulatory agencies to obtain feedback on what the database should contain. Access to the Clearinghouse via the FTC's secure Web site became available in July of 2000. To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available.[(16)] FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. For instance, the Commission publishes charts showing the prevalence of identity theft by states and by

cities. Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse, 62 federal agencies and 574 state and local agencies have signed up for access to the database. Within those agencies, over 4,200 individual investigators have the ability to access the system from their desktop computers twenty-four hours a day, seven days a week. The Commission actively encourages even greater participation.

One of the goals of the Clearinghouse and the FTC's identity theft program is to provide support for identity theft prosecutions nationwide.[(17)] Last year, in an effort to further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice, the International Association of Chiefs of Police and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. Sessions were held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, and Phoenix. The Phoenix program was held May 22. More than 730 officers have attended these seminars, representing more than 170 different agencies. Additional training seminars will occur later this year in Seattle, New York, and Houston -- cities the FTC has identified as having high rates of identity theft. Also, the FTC is a member of an identity theft task force in Kansas City and is helping coordinate a training seminar there later this summer.

The FTC staff also helps develop case leads. Now in its second year, the Commission runs an identity theft case referral program in coordination with the United States Secret Service. The Secret Service has assigned a special agent on a full-time basis to the Commission to assist with identity theft issues and has provided the services of its Criminal Research Specialists.[(18)] Together, the FTC and Secret Service staff develop preliminary investigative reports by examining significant patterns of identity theft activity in the database and refining the data through the use of additional investigative resources. Thereupon, the staff refer the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers located throughout the country for further investigation and potential prosecution.

III. CONCLUSION

Identity theft places substantial costs on individuals and businesses. The Commission, through its education and enforcement capabilities, is committed to reducing these breaches as much as possible. The Commission will continue its efforts to assist criminal law enforcement with their investigations. Prosecuting perpetrators sends the message that identity theft is not cost-free. Finally, the Commission knows that as with any crime, identity theft can never be completely eradicated. Thus, the Commission's program to assist victims and work with the private sector on ways to facilitate the process for regaining victims' good names will always remain a priority.

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.

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 broadly 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.

4. 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).

5. 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. *See, e.g.,* FTC v. Assail, Inc., W03 CA 007 (W.D. Tex. Feb. 4, 2003) (order granting preliminary injunction) (defendants alleged

to have debited consumers' bank accounts without authorization for "upsells" related to bogus credit card package) and FTC v. Corporate Marketing Solutions, Inc., CIV - 02 1256 PHX RCB (D. Ariz Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam (Jan. 16, 2003) (*at* http://www.ftc.gov/opa/2003/01/idpfinal.htm).

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

7. At a consumer's request, the three major credit reporting agencies will place a fraud alert on the consumer's credit file that indicates to credit issuers that the consumer is to be contacted before new credit is issued in that consumer's name. *See* Section II.B.(3)(a) *infra* for a discussion of the credit reporting agencies new "joint fraud alert" initiative.

8. 15 U.S.C. § 1681 *et seq.*

9. *Id*. § 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. *Id*. § 1601 *et seq*.

11. *Id*. § 1692 *et seq*.

12. Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name*.

13. *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).

14. Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. Times, Jan. 12, 2003, § 1 (Late Edition), at 12.

15. Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA Times, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

16. Charts that summarize 2002 data from the Clearinghouse can be found at www.consumer.gov/idtheft and www.consumer.gov/sentinel.

17. The Commission testified last year in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. *See* Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002). S. 2541 has been reintroduced in the 108th Congress as S. 153.

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