PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT

Before the

COMMITTEE ON THE JUDICIARY

COUNCIL OF THE DISTRICT OF COLUMBIA

Washington, D.C.

April 3, 2003

I. INTRODUCTION

Madam Chair, and members of the Committee, I am Betsy Broder, Assistant Director of the Division of Planning and Information in 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 what our statistics tell us about identity theft in the District of Columbia.

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 private industry on ways to improve victim assistance, including providing direct advice and assistance in cases where information has been compromised. The Commission can take enforcement action when companies fail to take adequate security precautions to protect consumers' personal information.

---

[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).

II. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The Identity Theft Act strengthened the criminal laws governing ID 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 private businesses. Accordingly, 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]18 U.S.C. § 1028(a)(7). The statute broadened "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. R&R Consultants, Inc., 01-CV-1537 TJM (N.D.N.Y. Apr. 25, 2002) (final order) (FTC v. Assail, Inc., W03 CA 007 (W.D.Tx 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), 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 (January 16, 2003) (*at* http://www.ftc.gov/opa/2003/01/idpfinal.htm).

(3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[6] In order to fulfill the purposes of the Act, the Commission has implemented a plan that centers 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. Toll-free Telephone Hotline

On November 1, 1999, the Commission established a toll-free telephone number, 1-877-ID THEFT (438-4338), for consumers to report identity theft and to receive information about identity theft. In 2002, hotline counselors added almost 219,000 consumer reports to the Clearinghouse, up from more than 117,000 in 2001. Of the 219,000 reports, almost 162,000 (74%) were complaints from actual victims of identity theft, and almost 57,000 (26%) were inquiries about identity theft generally. Despite this dramatic growth in reports, 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 to provide them with general information about identity theft or to help them through the steps they need to take to resolve the problems resulting from the misuse of their identities. Victims are advised to: (1) contact each of the three national consumer reporting agencies to obtain copies of their credit reports and request that

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

a fraud alert be placed on their credit reports;[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 debts; 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 are trained to 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 are also referred to those agencies.

B. Identity Theft Data Clearinghouse

The Identity Theft Act directed the FTC 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

---

[7] These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name. *See* Section II.C.(3) *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*.

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.[12] 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. (See attachment.) 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, 75 federal agencies and 549 state and local agencies have signed up for access to the database. Within those agencies, over 4500 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.[13] To further expand the use of the Clearinghouse among law

---

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

[13]The Commission testified last year in support of S. 2541, the Identity Theft Penalty

(continued...)

enforcement, 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. Last year, the FTC began this program with a widely-attended session here in Washington, D.C., followed by programs in Des Moines, Chicago, San Francisco, Las Vegas, and Dallas. More than 600 officers have attended these seminars, representing more than 130 different agencies. This year, the FTC tentatively plans to hold similar training seminars in Phoenix, Seattle, New York, and Houston -- cities the FTC has identified as having high rates of identity theft.

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, which 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.[14] 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 located throughout the country for further investigation and potential prosecution.

---

[13](...continued)
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).

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

C. Outreach and Education

The final mandate for the FTC under the Identity Theft Act was to provide information to consumers about identity theft. Recognizing that the roles of law enforcement and private industry play an important part in the ability of consumers to both 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, multi-media campaign includes print materials, media mailings, and interviews, as well as the identity theft website, located at www.consumer.gov/idtheft, which includes the publications, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources.[15] The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Clearinghouse.

The FTC's comprehensive consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*, has been a tremendous success. The 26-page booklet, now in its fourth edition, 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

[15] www.consumer.gov is a multi-agency "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from more than 170 federal agencies.

as a result of identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its release in February 2000.[16] 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.*

(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 above, the staff recently joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General, as well as the Corporation Counsel for the District of Columbia, 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.C.(3)), links to the FTC website, and its own booklet containing information from *Identity Theft: When Bad Things Happen to Your Good Name.* Through this initiative, the FTC hopes to make the most efficient use of federal resources by allowing other jurisdictions 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

[16]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.*

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) the redesign 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 Web site shortly.

(3) *Private Industry*

a. Victim Assistance

Because identity theft victims spend significant time and effort restoring their good name and financial records, the FTC devotes significant resources to conducting outreach with the private sector on ways in which victim assistance procedures can be improved. One such initiative arose from the burdensome requirement for victims to complete a different fraud affidavit for each different creditor when the identity thief opened or used an account in the victim's name.[17] To reduce that burden, the FTC worked 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 with whom identity thieves had opened accounts. From its release in August 2001 through February 2003, the FTC has distributed more than 264,000 print copies of the ID Theft Affidavit. There have also been more than 351,000 hits to the Web version. The affidavit is available in both English and Spanish.

Another initiative is the development of a "joint fraud alert" among the three major credit reporting agencies ("CRAs"). This initiative will allow the CRAs to share among themselves requests

---

[17]*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).

from identity theft victims that fraud alerts be placed on their consumer reports and copies of their reports be sent to them, thereby eliminating the victim's need to contact each of the three major CRAs separately. A pilot program is expected to begin in early this month.

b. Information and 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 April, the FTC invited representatives from financial institutions, credit issuers, universities and retailers to a one day informal roundtable discussion of ways to prevent access to personal information in employee and customer records. The FTC will soon publish a self-audit guide to make businesses and organizations of all sizes more aware of how they are managing 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 who have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest[18] and Ford/Experian,[19] in which massive numbers of individuals' personal information was taken, the Commission provided advice on notifying those individuals and what steps they should take to protect themselves. From these experiences, the FTC developed a business record theft response kit that will be posted shortly on the identity theft Web site. The kit includes the steps to take in responding to an information compromise and a form letter for notifying the individuals whose information was taken. The kit provides advice on the type of law enforcement agency to

---

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

[19]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.

contact, depending on the type of compromise, business contact information for the three major credit reporting agencies, suggestions for setting up an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. 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 as soon as possible the individuals whose information has been taken as soon as possible so that they can 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 theft of their information will turn into the actual misuse of their information. Prompt notification also alerts them to review their credit reports and to keep 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. In addition to providing the business record theft response kit, 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.

III. ID THEFT IN THE DISTRICT OF COLUMBIA

The FTC's ID Theft Data Clearinghouse offers a view into the impact of identity theft on individuals, and its prevalence in a specific area. In calendar year 2002, the FTC received complaints from 704 District residents who discovered that their identities were stolen. (*See,* Identity Theft Figures and Trends, January 1, 2002 - December 31, 2002, attached.) Although in aggregate, this represents a small number of victims, it does position the District as the jurisdiction with the highest *per capita* rate of

ID theft (*per* 100,000 residents) in the nation.[20] Of these DC victims, 44% had their identity used to open new credit accounts or takeover existing accounts. Nineteen percent had utility service, including cell phone accounts, opened in their name. Bank fraud, including accessing a checking or savings account, affected 20% of the DC complainants, and 10% of the victims had government documents or benefits fraudulently obtained in their name. Finally, 7% experienced loan fraud, and 18% suffered other, miscellaneous types of fraud including use of another's name in the criminal justice system, to obtain medical services or rent a home.[21] These trends generally track the national trends.

DC residents primarily reached the FTC through our hotline (73%), while others filed their complaints online (16%) with the remaining complaints entering the system via the Social Security Administration's sharing of data (11%).

Our data also reflect how law enforcement has responded to victims of ID theft. Thirty-nine percent of the DC victims contacted the police department following the discovery of the identity theft. (Attachment, Fig. 5). The Metro Police Department wrote police reports for 24% of the victims. This compares to 45% of consumers nationwide who contacted police, and 36% who obtained a police report.[22] Police reports are significant, because the police report establishes the victim's good faith

---

[20] The high *per capita* ranking of the District reflects several anomalies. Frequent local media coverage in the District has resulted in an unusually high rate of knowledge among DC residents of the FTC's complaint handling program. Also, the District, which is wholly urban, is treated as a state for statistical purposes, resulting in a higher concentration of identity theft cases.

[21] Percentages add to more than 100% because approximately 23% of the victims report experiencing more than one type of identity theft.

[22] The low rate of police reports is likely related to the fact the District currently has no criminal sanctions for identity theft. If the Council were to adopt such laws, consideration should be given to

(continued...)

status as a victim, rather than someone seeking to evade legitimate debts. Also, consumer reporting agencies have voluntarily instituted a program to block the fraudulent trade lines on an IDT victim's credit report upon submission of the report.

IV. CONCLUSION

The Commission is committed to continuing its efforts in training and sharing data with criminal law enforcement agencies. Prosecuting perpetrators sends the message that identity theft is not cost-free. The Commission knows, however, 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.

---

[22](...continued)
increasing the resources devoted to the detection and prosecution of ID theft.