PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT

Before the

HOUSE FINANCIAL SERVICES COMMITTEE

Washington, D.C.

April 3, 2003

I. INTRODUCTION

Mr. Chairman, and members of the Committee, 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 private 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.

---

[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) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[6] 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

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

[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*

[12] Charts that summarize 2002 data from the Clearinghouse can be found at

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 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 held sessions in Washington, D.C., 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]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).

[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.

[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*.d and 0l SecurdAe TD 0.12oighpr8.5 -15 34 636TD /05 Tc 097905 Tw 097905 0las a105sult223.i

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

III. THE FEDERAL TRADE COMMISSION'S ROLE IN INFORMATION SECURITY

In addition to providing assistance to victims of identity theft, the Commission also examines security precautions involving consumers' personal information to determine whether law enforcement may be appropriate. If so, the Commission has two valuable legal tools to work with: Section 5 of the FTC Act,[20] which prohibits unfair and deceptive acts or practices, and, starting in May of this year, the Commission's Gramm-Leach-Bliley Safeguards Rule (the "Safeguards Rule" or the "Rule").[21]

A. Law Enforcement Under Section 5

One of the mainstays of the Commission's privacy program is the enforcement of promises that companies make to consumers about privacy, and in particular, the precautions they take to ensure the security of consumers' personal information. The Commission currently enforces such promises both online and offline. The Commission is particularly concerned about breaches involving sensitive information because they put consumers at the greatest risk of identity theft and other harms.

Last August, the Commission announced a settlement with Microsoft regarding misleading claims made by the company about the information collected from consumers through its Passport services – Passport, Passport Wallet, and KidsPassport.[22] Passport is a service that collects information from consumers and then allows them to sign in at any participating site using a single name and password. Passport Wallet collects and stores consumers' credit card numbers, and billing and

---

[20] 15 U.S.C. § 45.

[21] 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[22] The Commission's final decision and order in the Microsoft case is available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf. The Commission's complaint is available at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

shipping addresses, so that consumers do not have to input this information every time they make a purchase from a site. Kids Passport was promoted as a way for parents to create accounts for their children that limited the information that could be collected from them.

The Commission's complaint alleged that Microsoft misrepresented the privacy afforded by these services, including the extent to which Microsoft kept the information secure. For example, in various online statements, Microsoft said that the Passport service "achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information." In fact, the Commission alleged that Microsoft failed to employ reasonable and appropriate measures to protect the personal information collected in connection with these services because it failed to: (1) implement procedures needed to prevent or detect unauthorized access; (2) monitor the system for potential vulnerabilities; and (3) perform appropriate security audits or investigations.

The Commission's order against Microsoft contains strong relief that will provide significant protections for consumer information. First, it prohibits any misrepresentations about the use of and protection for personal information. Second, it requires Microsoft to implement a comprehensive information security program similar to the program required under the FTC's Gramm-Leach-Bliley Safeguards Rule, which is discussed below. Finally, to provide additional assurances that the information security program complies with the consent order, Microsoft must have its program certified as meeting or exceeding the standards in the order by an independent professional every two years. The provisions of the order will expire after 20 years.

The order in the Lilly case prohibits the misrepresentations and, as in Microsoft, requires Lilly to implement a comprehensive information security program.

It is important to note that the Commission is not simply saying "gotcha" for security breaches. While a breach may indicate a problem with a company's security, breaches can happen even when a company takes all reasonable precautions. In such instances, the breach does not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances. That is the approach the Commission took in these cases and in its Gramm-Leach-Bliley Safeguards Rule, and the approach it will continue to take.

B. GLB Safeguards Rule

Last May, the Commission finalized its Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. On May 23, 2003, the Rule becomes effective and the Commission expects that it will quickly become an important tool to ensure greater security for consumers' sensitive financial information. Whereas Section 5 authority derives from misstatements particular companies make about security, the Rule requires a wide variety of financial institutions to implement comprehensive protections for customer information – many of them for the first time. The Rule could go far towards reducing risks to this information, including identity theft.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. Due to the wide variety of different entities covered, the Rule requires a plan that takes into account each entity's particular circumstances –

its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these

[24] *Financial Institutions and Customer Data: Complying with the Safeguards Rule*, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[25] Additional information about the workshop is available at http://www.ftc.gov/bcp/workshops/security/index.html.

[26] Additional information about the workshop is available at http://www.ftc.gov/bcp/workshops/technology/index.html.

manage the consumer information they maintain and ensure that it is secure. Despite the widespread availability of these products, however, it is unclear just how much consumers and businesses are using them and whether they are meeting consumer and business needs in this area. The Commission's workshops will foster a wide-ranging discussion on these issues, with the goal of gaining a better understanding of whether technology is being used effectively to protect personal information.

IV. CONCLUSION

Large scale security breaches place 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.