PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

on

PROTECTING INFORMATION SECURITY AND PREVENTING IDENTITY THEFT

September 22, 2004

I. INTRODUCTION

Mr. Chairman, and members of the subcommittee, I am Commissioner Orson Swindle.[1] I appreciate the opportunity to appear before you today to discuss the Commission's role in promoting information security and combating identity theft.

The Federal Trade Commission has a broad mandate to protect consumers from unfair and deceptive practices. As part of its mission, the Commission has given a special emphasis to efforts to protect the privacy and security of consumer information. These efforts include educating companies about the importance of using reasonable and appropriate procedures to safeguard consumers' personal information, supplemented by law enforcement in appropriate cases when companies fail to take such steps. In addition, as the federal government's central repository for identity theft complaints, the Commission plays a significant role in referring complaints about identity theft to appropriate law enforcement authorities, providing victim assistance and consumer education, and working with businesses to mitigate harm in the event of a security breach.[2]

II. THE BENEFITS AND RISKS OF ELECTRONICALLY-STORED CONSUMER DATA

Electronic information systems provide enormous benefits to consumers, businesses, and government alike. We rely on them for the orderly operation of our financial systems and power supplies, the efficient processing of our transactions, twenty-four hour access to information, and many other conveniences and cost savings. In order to provide these benefits, these computer-driven systems store voluminous data on consumers – ranging from sensitive medical and financial records to catalog purchases. If not adequately protected, these systems and databases can be extremely vulnerable, thus threatening the security of the information they store and

responsibility to safeguard that data. The Commission actively attempts to educate businesses and consumers about information security risks and the precautions they must take to protect or minimize risks to personal information. Our emphasis is on preventing breaches before they

appropriate in light of the circumstances. Such circumstances include the company's size and complexity, the nature and scope of its activities, and the sensitivity of the consumer information it handles. Third, the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. Finally, a company's practices may be unreasonable even without a known breach of security. Indeed, because the primary purpose of information security is to prevent breaches before they happen, companies cannot simply wait for a breach to occur before they take action.

Implementation of these principles requires businesses to develop a security plan and make security monitoring and oversight part of their regular operations – literally, a part of their culture. Information security planning should include: identifying internal and external risks to the security, confidentiality, and integrity of consumers' personal information; designing and implementing safeguards to control these risks; periodically monitoring and testing the safeguards to be sure they are working effectively; adjusting security plans according to the results of testing or changes in circumstances; and overseeing the information handling practices of service providers who have access to the personal information. As discussed below, these basic steps are required by the Commission's Safeguards Rule and the Commission's orders in cases involving information security.

B. Managing a Data Compromise

For example, if the security breach could result in harm to a person or business, companies should report the situation to the appropriate law enforcement agency. Companies should also consider whether the data compromise may affect other businesses, and if so, should notify them. In particular, if a breach affects information that a company stores or maintains on behalf of another business, notification to the other business would be appropriate.

In addition, companies should evaluate whether to notify consumers that there has been a breach.[9] For example, consumer notification may not be necessary if the information is not sensitive or there is no evidence of unauthorized access. If information that creates a risk of identity theft has been stolen, however, the FTC suggests notifying individuals of the incident as soon as possible so they can take steps to limit the potential damage.[10] For example, if an individual's Social Security number is compromised, that individual, by placing a fraud alert on his credit file, will have a good chance of preventing, or at least reducing, the likelihood of identity theft or the misuse of this information.[11]

IV. THE FEDERAL TRADE COMMISSION'S INITIATIVES

The Commission seeks to highlight the importance of information security using several approaches, including educating consumers and businesses, targeted law enforcement actions, international cooperation, and encouraging the private sector to develop and deploy information security technologies. Pursuant to its mandate under the Identity Theft Act, the Commission also facilitates information sharing among public and private entities to combat and help prevent identity theft.[12] Further, the Commission is currently working on a number of rulemakings implementing provisions of the Fair and Accurate Credit Transactions of 2003 ("FACT Act") that contain new and important measures to help reduce identity theft and facilitate identity theft

victims' recovery.[13]

Finally, an effective security program includes measures to ensure proper disposal of sensitive consumer information once it is no longer needed. Pursuant to the recently enacted FACT Act,[28] the Commission issued a proposed rule designed to reduce the risk of fraud or identity theft by ensuring that consumer reports, or information derived from consumer reports, are appropriately redacted or destroyed before being discarded.[29] The Commission anticipates

www.consumer.gov/idtheft, which includes publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources. Consumers may file identity theft complaints on our secure online complaint form. These complaints are entered into the Identity Theft Data Clearinghouse and are used by law enforcement agencies to support their investigations.

The Commission also is currently working on a number of rulemakings implementing provisions of the FACT Act that provide new and important measures to facilitate identity theft victims' recovery. These include a national fraud alert system, which will eliminate the need for victims to contact each of the major credit reporting agencies separately,[33] and identity theft blocking, which will prevent fraudulent account information from being reported on consumer reports.[34] When fully implemented, these initiatives should help to reduce the incidence of identity theft, and help victims recover when the problem does occur. In addition, the Commission is consulting with the Treasury Department on its study, required by the FACT Act, of how the use of biometrics and similar authentication technologies to identify parties to a transaction might reduce the incidence of identity theft.[35]

V. CONCLUSION

Through a variety of education and enforcement initiatives, the FTC is working to ensure that all companies entrusted with personal information take reasonable steps to secure that information and minimize the risk that it may be misused. The agency has been and will continue to be vigilant in promoting a culture of security. We are educating consumers and businesses about the risks to personal information and the role they must play in enhancing security. We also will continue to assist victims of identity theft. In addition, the Commission

will continue to take action against companies that violate information security laws.

25. *See MTS, Inc. d/b/a Tower Records/Books/Video*, FTC Dkt. No. C-4110 (June 2, 2004); *Guess?, Inc.*, FTC Dkt. No. C-4091 (August 5, 2003); *Microsoft Corp.*, FTC Dkt. No. C-4069 (Dec. 24, 2002); *Eli Lilly, Inc.*, FTC Dkt. No. C-4047 (May 10, 2002). The complaints and decisions and orders in these cases are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

26. The Rule requires covered financial institutions within the Commission's jurisdiction to develop a written information security plan to protect customer information that is reasonable in light of a company's 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 include certain basic elements, including: (1) designating one or more employees to coordinate the safeguards; (2) identifying and assessing the risks to customer information in each relevant area of the company's operation, and evaluating the effectiveness of the current safeguards for controlling these risks; (3) designing and implementing a safeguards program, and regularly monitoring and testing it; (4) hiring appropriate service providers and contracting with them to implement safeguards; and (5) evaluating and adjusting the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

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

28. The FACT Act amends the Fair Credit Reporting Act in a number of ways, including the addition of a number of provisions intended to combat consumer fraud and related crimes, including identity theft.

29. *See* Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21,388 (2004) (to be codified at 16 C.F.R. Part 682), available at http://www.regulations.gov/fredpdfs/04-08904.pdf. To help prevent identity theft, the FACT Act also directs the Commission to issue a "red flags" rule. *See* Pub. L. No. 108-396, § 157 (2003). The rule will help creditors analyze identity theft patterns and practices so that they can take appropriate action to prevent this crime.

30. *See* http://www.oecd.org/sti/cultureofsecurity.

31. The APEC Electronic Commerce Steering Group ("ECSG") promotes awareness and responsibility for cybersecurity among small and medium-sized businesses that interact with consumers. Commission staff participated in APEC workshop and business education efforts this past year and will remain actively engaged in this work for the foreseeable future.

32. The Commission's National Do Not Email Registry Report is available at: http://www.ftc.gov/reports/dneregistry/report.pdf.

33. Pub. L. No. 108-396, § 112 (2003).

34. Pub. L. No. 108-396, § 152 (2003).

35. Pub. L. No. 108-396, § 157 (2003).