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

maintain.

In particular, a large database containing sensitive personal information can be a treasure trove for identity thieves.[3] When breached, the data in these systems can be used to impersonate consumers, take over their accounts, and cause substantial injury to consumers, businesses, and other institutions.[4] In recent years, there have been reports of a number of large-scale computer security breaches in which identity thieves and others gained access to the sensitive personal information of tens of thousands of consumers. Examples of publicly reported breaches include the theft of computer equipment containing detailed health insurance or financial information, security breaches that exposed credit card data, and the hacking of university databases. Breaches such as these create the potential for – and sometimes result in – mass-scale identity theft with millions of dollars in false charges.

Electronic systems and databases face diverse security threats. Sometimes, companies simply fail to properly safeguard consumers' information, leaving it vulnerable to hackers. Other breaches are caused by insiders, who exploit security weaknesses or use their position and access to the company's systems to steal data. In some instances, the breach can be as simple as the failure to dispose of sensitive documents properly. The adverse consequences of poor security can include not only identity theft and fraud, but also diminished computer operation, spam, "phishing" attacks, or even the takeover of computers to launch attacks on other commercial websites or on parts of the nation's critical information infrastructure.

III. PREVENTING BREACHES AND IDENTITY THEFT

Companies that process or store personal information about consumers – especially sensitive information such as a Social Security number or credit card information – have a

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 happen by encouraging businesses and consumers to make security part of their daily routines. We also provide advice to businesses and consumers in the event that a breach involving sensitive personal information does occur.

A. Reasonable Security Procedures

The Commission has considerable experience in understanding and addressing information security concerns. For example, in 1999, the Commission convened an Advisory Committee on Online Access and Security, in which a panel of experts examined the parameters of appropriate security for information collected online and provided a report with its findings.[5] The Commission also drafted and enforces its Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule"), which became effective in 2003.[6] This Rule requires "financial institutions" subject to the FTC's jurisdiction, which includes a broadly-defined group of non-bank entities, to develop and implement appropriate safeguards to protect customer information. In addition, the Commission played a leading role in developing and implementing the Organization for Economic Cooperation and Development's ("OECD") Security Guidelines.[7]

Through this work, as well as our more general education and enforcement initiatives, the Commission has come to recognize several principles that should govern any information security program. First, information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve. Second, a company's security procedures must be reasonable and

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

Companies should implement reasonable security procedures to prevent the compromise of sensitive personal information. In the event that a security breach does occur, however, there are several steps businesses should take to respond.[8]

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]

A. Education and Outreach

Education is an essential element of the Commission's information security efforts. Our educational initiatives include public workshops to highlight emerging issues, consumer and business education to help identify risks to personal information and promote a "Culture of Security," and business education to promote compliance with relevant laws. For example, last year we held a two-session workshop, "Technologies for Protecting Personal Information: The Consumer and Business Experiences," to educate businesses, consumers, and ourselves about the challenges and possible technological solutions to securing electronic data.[14] In order to secure systems that contain personal information, panelists advised that businesses adopt a comprehensive risk-management strategy that incorporates four critical elements: people, policy, process, and technology.[15] Panelists also discussed a variety of recent initiatives in which industry is applying these principles. For example, companies have worked to reduce security flaws in software code, ship products in a more secure configuration, add new security features to products, and provide better security support, such as providing warnings and security patches, to their already-deployed products when security flaws appear.[16] In addition, panelists explored identity management tools and authentication issues as part of a risk-management plan.[17]

Our information security campaign also includes extensive outreach to businesses and consumers through our website, educational alerts, speeches, and participation in joint cybersecurity initiatives with other government agencies and private groups. The Commission devotes a portion of its website to educating businesses and consumers about security, and these

security-related pages are some of the most popular on our site.[18] The site includes guidance for businesses to reduce risks to their computer systems,[19] and tips for consumers on selecting online security products.[20] Our recent outreach efforts have also included cooperative ventures with the Department of Homeland Security and such organizations as the National Cyber Security Partnership and the National Cyber Security Alliance Stay Safe Online.[21]

B. Law Enforcement

The Commission's enforcement tools in information security matters derive generally from Section 5 of the FTC Act[22] and the Commission's Safeguards Rule.

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[23] To date, the Commission's security cases have been based on its authority to prevent deceptive practices.[24] These cases involved companies that made alleged express or implied promises that they would take appropriate steps to protect sensitive information obtained from consumers, but did not do so.[25] The complaints and consent orders in these cases reflect the principles discussed in Section III.A., above, and provide guidance to industry about implementing reasonable security procedures. In particular, the orders require, among other things, that the companies establish and maintain a comprehensive information security program that includes the basic elements necessary to ensure reasonable and appropriate security.

The Commission also has responsibility for enforcing its Safeguards Rule. The Rule requires a wide variety of non-bank financial institutions to implement comprehensive protections for customer information.[26] The Commission has issued guidance on the Rule[27] and met with a variety of trade associations and companies to promote compliance. Currently, Commission staff is conducting non-public investigations of compliance with the Rule.

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 the issuance of a final rule by the end of the year. Once the rule is in effect, it will provide an additional tool for use in the Commission's law enforcement efforts.

C. International Cooperation

In an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information, and the Commission has joined others in the global community to educate and establish a culture of security. For example, we played a leading role in developing and implementing the OECD Security Guidelines, assisted in developing and promoting a website dedicated to the global dissemination of information about the Guidelines,[30] and play an ongoing role in information privacy and security work undertaken by the OECD and the Asian Pacific Economic Cooperation ("APEC") forum.[31]

D. Encouraging the Development and Deployment of Information Security Technologies

The Commission also encourages the development and deployment of information security technologies that may help protect consumers from spam and "phishing" attacks. In its June 2004 Report to Congress concerning a possible National Do Not Email Registry, the Commission identified domain-level authentication as a promising technological development that would enable ISPs and other domain holders to better filter spam, and that would provide law enforcement with a potent tool for locating and identifying spammers.[32] Domain-level

authentication could also serve as a useful tool in preventing "phishing" spam and spam containing viruses from reaching consumers' inboxes. The Report concluded that the Commission could play an active role in spurring the market's development, testing, evaluation, and deployment of domain-level authentication systems. As a first step, the Report explained that the Commission, with other relevant government agencies, would hold an Email Authentication Summit in the Fall of 2004. The Commission and the Department of Commerce's National Institute of Standards and Technology will be hosting the Summit on November 9-10, 2004.

E. Assisting Identity Theft Victims

Through our efforts to promote information security and educate consumers, we hope to prevent identity theft before it occurs. When identity theft does occur, however, we also have an extensive program to help consumers who have been victimized. The program has three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; (2) maintaining and promoting the Identity Theft Data Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and (3) outreach and education to consumers, law enforcement, and private industry.

Victims may call the FTC through a toll-free hotline, 1-877-ID THEFT (438-4338), to receive telephone counseling from specially trained personnel. The phone counselors provide general information about identity theft and help guide victims through the steps needed to resolve the problems that result from the misuse of their identities.

The FTC also maintains the federal government's identity theft website,

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.

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 other Commissioner.

2. The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act"). Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028). The Act did not confer on the FTC any additional law enforcement authority.

3. Social Security numbers in particular play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims.

4. For example, our 2003 Identity Theft Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf, showed that over 27 million individuals have been victims of identity theft, which may have occurred either offline or online, in the five years preceding the survey, including almost 10 million individuals in the year preceding the survey. The survey also showed that the average loss to businesses was $4800 per victim. Although in most cases, identity theft victims are not held liable for the fraudulent charges, they nonetheless suffer an average financial loss of $500, which reflects out-of-pocket expenses related to the efforts to dispute the frauds and repair their credit standing.

5. The Advisory Committee was comprised of forty e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates. Information about the Advisory Committee, including its charter, membership, meeting transcripts, and working papers, is available at http://www.ftc.gov/acoas/index.htm. The Advisory Committee submitted its Final Report to the Commission in May 2000. The Report recommended that companies undertake a security approach that is appropriate to the circumstances, and advised that a good security program includes: conducting a risk assessment; establishing and implementing a security system; managing policies and procedures based on the risk assessment; conducting periodic training for employees; conducting audits; conducting internal reviews; and conducting periodic reassessment of risk. *See Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security* (May 15, 2000), available at http://www.ftc.gov/acoas/papers/finalreport.htm.

6. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf. Pursuant to Section 501(b) of the Gramm-Leach-Bliley Act, the federal banking agencies have issued similar security guidelines that apply to the financial institutions they regulate. *See Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. Parts 30, app. B (OCC); 208, app. D-2 and 225, app. F (Board); 364, app. B (FDIC); 570, app. B (OTS).

7. In 2002, the OECD issued a set of nine voluntary principles for establishing a culture of security. The OECD principles are contained in a document entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." The principles address awareness, accountability, and action. They also recognize that security architecture and procedures should be appropriate for the kind of information collected and maintained and that good security is an ongoing process of assessing and addressing risks and vulnerabilities. *See* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

8. The FTC has developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, that provides advice on which law enforcement agency to contact, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, and information about contacting the FTC for assistance. The kit also provides FTC guidance regarding whether and how to notify consumers that there has been a breach. The information compromise kit is posted on our identity theft website, http://www.consumer.gov/idtheft and is also available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm.

9. Under certain state laws, companies may be required to notify consumers in the event of a breach. For example, the State of California requires consumer notification in the event of certain security breaches. The law, which went into effect July 1, 2003, requires a business or a State agency that maintains unencrypted computerized data that includes personal information to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is an individual's name plus one or more of the following: Social Security number, driver's license or state ID card number, or financial account numbers. *See* Cal. Civ. Code §§ 1798.29; 1798.82-1798.84.

10. The FTC's kit also includes a model letter for notifying individuals when that might be appropriate, such as when their names and Social Security numbers have been 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.

11. Prompt notification by businesses also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that individuals become victims, they can take action quickly to clear their records before any long-term damage is done.

12. The Federal Trade Commission maintains a database of identity theft complaints, and makes available and refers these complaints to criminal law enforcement agencies for investigation. Most identity theft cases are addressed best through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft, such as "pretexting" (tricking consumers or banks into revealing financial information) (*see, e.g.*, *FTC v. Corporate Marketing Solutions, Inc.*, Civ. No. 02-1256-PHX (RCB) (D. Ariz. Feb. 3, 2003) (final order)) or "phishing" (using spam email that looks like it comes from a legitimate website to deceive consumers into providing account or other

sensitive information) (*see, e.g.*, *FTC v. M.M.*, Civ. No. 04-2086 (E.D.N.Y. May 18, 2004) (final order)). 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).

13. Pub. L. No. 108-159 (2003).

14. The FTC staff released a short staff summary of the findings from the workshop, which is available at http://www.ftc.gov/bcp/workshops/technology/index.html.

15. *See* Staff Workshop Report: Technologies for Protecting Personal Information, at 2-3.

16. *Id.* at 4-5.

17. In particular, the National Academies of Science and the Center for Democracy and Technology discussed the strengths and weaknesses of certain identity systems, and the distinctions between identification, authentication, and authorization.

18. *See* http://www.ftc.gov/infosecurity.

19. *Security Check: Reducing Risks to Your Computer Systems*, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

20. *Detect, Protect, Disinfect: Consumers On Line Face Wide Choices in Security Products*, available at http://www.ftc.gov/bcp/conline/pubs/alerts/idsalrt.htm.

21. These include the consumer education website, www.staysafeonline.info.

22. 15 U.S.C. § 45.

23. 15 U.S.C. § 45(a)(1).

24. The Commission and the courts have defined a deceptive practice as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances. Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), *reprinted* in appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (setting forth the Commission's Deception Policy Statement). The Commission also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. 15 U.S.C. § 45(n). The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with "phishing." *See FTC v. Hill*, Civ. No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

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).