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 OUR NATION'S CYBERSPACE

April 21, 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 protecting information security and its importance to both consumers and businesses.

Today, maintaining the security of our computer-driven information systems is essential to every aspect of our lives. A secure information infrastructure is required for the operation of everything from our traffic lights to our credit and financial systems, including our nuclear and electrical power supplies and our emergency medical service. We are all, therefore, directly or indirectly linked together by this infrastructure. Consumers rely on and use computers at work and

The Federal Trade Commission has a broad mandate to protect consumers and the Commission's approach to information security is similar to the approaches taken in our other consumer protection efforts. As such, the Commission has sought to address concerns about the security of our nation's computer systems through

the reasonableness of the company's procedures in light of the circumstances surrounding the breach. This allows the Commission to determine whether the breach resulted from the failure to have procedures in place that are reasonable in light of the sensitivity of the information. In many instances, we have concluded that FTC action is not warranted. When we find a failure to implement reasonable procedures, however, we act.

3. Law Violations Without a Known Breach of Security

The Commission's case against Microsoft[11] illustrates a third principle – that there can be law violations without a known breach of security. Because appropriate information security practices are necessary to protect consumers' privacy, companies cannot simply wait for a breach to occur before they take action. Particularly when explicit promises are made, companies have a legal obligation to take reasonable steps to guard against reasonably anticipated vulnerabilities.

Like Eli Lilly, Microsoft promised consumers that it would keep their information secure. Unlike Lilly, there was no specific security breach that triggered action by the Commission.[12] The Commission's complaint alleged that there were significant security problems that, left uncorrected, could jeopardize the privacy of millions of consumers. In particular, the complaint alleged that Microsoft did not employ "sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained through Passport and Passport Wallet."[13] The complaint further alleged that Microsoft failed to have systems in place to prevent unauthorized access; detect unauthorized access; monitor for potential vulnerabilities; and record and retain systems information sufficient to perform security audits and investigations. Again, sensitive information was at issue – financial information including credit card numbers.

Like the Commission's order against Eli Lilly, the Microsoft order prohibits any misrepresentations about the use of, and protection for, personal information and requires Microsoft to implement a comprehensive information security program. In addition, Microsoft must have an independent professional certify, every two years, that the company's information security program meets or exceeds the standards in the order and is operating effectively.

4. Good Security is an Ongoing Process of Assessing Risks and Vulnerabilities

The Commission's third case, against Guess, Inc.,[14] highlighted a fourth principle – that good security is an ongoing process of assessing and addressing risks and vulnerabilities. The risks companies and consumers confront change over time. Hackers and thieves will adapt to whatever measures are in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make adjustments to reduce these risks.

The Guess case highlighted this crucial aspect of information security in the context of web-based applications and the databases associated with them. Databases frequently house sensitive

of attack was well known in the industry and appeared on a variety of lists of known vulnerabilities. The complaint alleged that, despite specific claims that it provided security for the information collected from consumers through its website, Guess did not: employ commonly known, relatively low-cost methods to block web-application attacks; adopt policies and procedures to identify these and other vulnerabilities; or test its website and databases for known application vulnerabilities, which would have disclosed that the website and associated databases were at risk of attack. Essentially, the Commission alleged that the company had no system in place to test for known application vulnerabilities or to detect or to block attacks once they occurred.

In addition, the complaint alleged that Guess misrepresented that the personal information it obtained from consumers through www.guess.com was stored in an unreadable, encrypted format at all times; but, in fact, after launching the attack, the attacker could read the personal information, including credit card numbers, stored on www.guess.com in clear, unencrypted text.

As in its prior security cases, the Commission's emphasis in Guess was on reasonableness. When the information is sensitive, the vulnerabilities well known, and the fixes inexpensive and relatively easy to implement, it is unreasonable simply to ignore the problem. As in the prior orders, the Commission's order against Guess prohibits the misrepresentations, requires Guess to implement a comprehensive information security program, and, like Microsoft, requires an independent audit every two years.

B. GLB Safeguards Rule

In addition to our enforcement authority unde

technical, and procedural safeguards to protect customer information.[15] The Safeguards Rule is an important enforcement and guidance tool to ensure greater security for consumers' sensitive financial information. It requires a wide variety of financial institutions to implement comprehensive protections for customer information - many of them for the first time. If fully implemented by companies, as required, the Rule could go a long way to reduce 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 entities

the Safeguards Rule to help them understand the Rule's requirements.[16] Commission staff also met, and continues to meet, with a variety of trade associations and companies to alert them to the Rule's requirements and to gain a better understanding of how the Rule is affecting particular industry segments. Since the Rule's effective date, the Commission has continued these efforts and has also conducted investigations of compliance by covered entities.

C. Education and workshops

In addition to our law enforcement efforts and conducting outreach under the Commission's Safeguards Rule, the Commission has engaged in a broad outreach campaign to educate businesses and consumers about the importance of information security and the precautions they can take to protect or minimize risks to personal information. These efforts have included creation of an information security "mascot," Dewie the e-Turtle, who hosts a portion of the FTC website devoted to educating businesses and consumers about security,[17] publication of business guidance regarding common vulnerabilities in computer systems[18] and responding to information compromises,[19] speeches by Commissioners and staff about the importance of this issue, and outreach to the international community. Many offices in the Commission, including the Commission's Bureau of Consumer Protection, the Office of Public Affairs, and the Office of Congressional Relations, have participated in this effort to educate consumers and businesses.

The Commission's information security website[20] has registered more than 600,000 visits since its deployment in August 2002, making it one of the most popular FTC web pages. The site has been made available in CD-ROM and exists in PDF format. The site itself is frequently updated with new information for consumers on cybersecurity issues. Further, the Commission's Office of Consumer and Business Education has produced a video news release, which has been seen by an

estimated 1.5 million consumers;

"spyware" – software that is loaded on personal computers without users' consent.[25] Among the issues discussed were the privacy and security concerns raised by such software programs and the steps that consumers can take to protect themselves. The workshop consisted of six panels. The first three panels dealt with defining and understanding spyware, security risks, and potential privacy risks with such software. The last three panels addressed possible responses from a variety of constituencies. For example, one panel moderated by Commissioner Mozelle Thompson examined efforts by industry to develop responses to the problems associated with spyware. Other panels dealt with potential technological and governmental responses to the issue.

D. International Efforts

excellent, common-sense starting point for formulating a workable approach to security. They address awareness, accountability, and action. They also reflect the principles that guide the FTC in its analysis of security-related cases, recognizing 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. These principles can be incorporated at all levels of use among consumers, government policy makers, and industry. The OECD Guidelines already have been the model for more sector-specific guidance by industry groups and associations.

Through the efforts discussed above, the FTC has played a leading role in implementing the OECD Security Guidelines. The FTC also participated in the October 2003 OECD Global Forum on Information Systems and Networks in Oslo, Norway, which began the actual implementation process. In addition, the OECD has launched a website, www.oecd.org/sti/cultureofsecurity, dedicated to the global dissemination of information about the OECD Security Guidelines, and the FTC has played a prominent role in the development and promotion of the site.

Besides the OECD, the Commission also is involved in information privacy and cybersecurity work undertaken by the Asian Pacific Economic Cooperation ("APEC") forum. APEC's Council of Ministers endorsed the OECD Security Guidelines in 2002. Promoting information system and network security is one of its chief priorities. 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 is actively engaged in this work for the foreseeable future.

Along with the OECD and APEC, in December 2002, the United Nations General Assembly unanimously adopted a resolution calling for the creation of a global culture of cybersecurity. Other UN groups, international organizations, and bilateral groups with whom the Commission has dialogues, including the TransAtlantic Business and Consumer Dialogues, the Global Business Dialogue on Electronic Commerce, and bilateral govern

on the Stay Safe Online "Top 10" cybersecurity tips; a partnership with the United States Internet Service Providers Association (USISPA) to educate home users about cyber security issues; and distribution of a Cyber Security Tool Kit to provide home users with easy-to-follow instructions on implementing the "Top 10" cyber tips.

Notwithstanding these efforts, developing a "Culture of Security" is a daunting challenge. The FTC, DHS, the Departments of Commerce, Justice, and State, and other government agencies have a role to play, but the government cannot do this alone, nor should it try. The Commission is working with consumer groups, business, trade associations, and educators to instill this new way of thinking. We are encouraging our global partners to do the same and to share what is learned.

III. Conclusion

The Commission, through law enforcement and consumer and business education, is committed to reducing the harm that occurs through information security breaches. Maintaining good security practices is a critical step in preventing these breaches and the resulting harms, which can range from major nuisance to major destruction. It is important to recognize one critical aspect of the global information-based economy: we are all in this together – government, private industry, and consumers -- and we must all take appropriate steps to create a culture of security.

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. For example, our recently released 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 last five years, including almost 10 million individuals in the last year alone. The survey also showed that the average loss to businesses was $4800 per victim. Although various laws limit consumers' liability for identity theft, their average loss was still $500 – and much higher in certain circumstances.

3. 15 U.S.C. § 45.

4. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

5. 15 U.S.C. § 45 (a) (1).

6. 15 U.S.C. § 45(n).

7. Where appropriate, the Commission has also alleged unfairness in its Internet cases. *See FTC v. Zachary Keith Hill*, Civ. No. H 03-5537 (filed S.D. Tex. December 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.

8. 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) (s(it TDd34 25 75AeCom)7.9(m)7.9(i)-1.2(ssio's. DecpationPolicy Sstatem)7.9(en.n).)]TJ0 -2.1
/www.ftc.gov/os/2002/05elbililydot.htm

14. The Commission's final decision and order against Guess, Inc. is available at http://www.ftc.gov/os/2003/06/guessagree.htm. The complaint is available at http://www.ftc.gov/os/2003/06/guesscmp.htm.

15. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

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

17. *See* http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html.

18. *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

19. *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtbizkit.htm.

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

21. *See FTC v. D Squared Solutions,* Civ. No. AMD 03 CV3108 (filed N.D. Md. Nov. 6, 2003). Pleadings are available at http://www.ftc.gov/os/caselist/0323223.htm.

22. The alert can be found at http://www.ftc.gov/bcp/conline/pubs/alerts/popalrt.html.

23. *See,* e.g., http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm. The Commission has also brought enforcement actions challenging unfair and deceptive practices in connection with "phishing." *See* cases cited *supra* note 7.

24. Additional information about the workshops are available at http://www.ftc.gov/bcp/workshops/technology/indes.html.

25. *See* http://www.ftc.gov/bcp/workshops/spyware/index.htm.

26. *See* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

27. *See* http://www.ftc.gov/secureyourserver.

28. A sample letter is available at http://www.ftc.gov/bcp/conline/edcams/spam/secureyourserver/letter_english.htm.

29. The National Cyber Security Partnership is an industry-led group of interested security experts from the public and private sectors and trade associations, including the U.S. Chamber of Commerce, the Information Technology Association of America, TechNet, and the Business Software Alliance. The partnership was created as part of the December 2003 National Cyber Security Summit held in Santa Clara, California.