PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

COMMERCE, TRADE & CONSUMER PROTECTION SUBCOMMITTEE

COMMITTEE ON ENERGY AND COMMERCE

U.S. HOUSE OF REPRESENTATIVES

on

CYBERSECURITY AND CONSUMER DATA: WHAT'S AT RISK FOR THE CONSUMER?

November 19, 2003

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 Federal Trade 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 at home; increasingly, more consumers are making purchases over the Internet and paying bills and banking online.

These interconnected information systems provide enormous benefits to consumers, businesses, and government alike. At the same time, however, these systems can create serious vulnerabilities that threaten the security of the information stored and maintained in these systems as well as the continued viability of the systems themselves. Every day, security breaches cause real and tangible harms to businesses, other institutions, and consumers.[2] These breaches and the harm they do shake consumer confidence in the companies and systems to which they have entrusted their personal information.

II. The Federal Trade Commission's Role

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 a combined approach that stresses the education of businesses, consumers, and government agencies about the fundamental importance of good security practices; law enforcement actions; and international cooperation. Our program encompasses efforts to ensure the security of computer networks, an understanding that we all have a role to play, as well as efforts to ensure that companies keep the promises they make to consumers about information security and privacy. In the information security matters, our enforcement tools derive from Section 5 of the FTC Act,[3] which prohibits unfair or deceptive acts or practices, and the Commission's Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule" or "Rule").[4] Our educational efforts include business education to promote compliance with the law, consumer and business education to help promote a "Culture of Security," international collaboration, public workshops to highlight emerging issues, and outreach to political leaders.

A. Section 5

The basic consumer protection statute enforced by the Commission is Section 5 of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."[5] The statute defines "unfair" practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[6] To date, the Commission's security cases have been based on deception,[7] which the Commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.[8]

The companies that have been subject to enforcement actions have made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. Their security measures, however, proved to be inadequate; their promises, therefore, deceptive.

Through the information security enforcement actions, the Commission has come to recognize several principles that govern any information security program.

1. Security procedures should be appropriate under the circumstances

First, a company's security procedures must be appropriate for the kind of information it collects and maintains. Different levels of sensitivity may dictate different types of security measures. It is highly problematic when a company inadvertently releases sensitive personal information due to inadequate security procedures.

The Commission's first information security case, Eli Lilly,[9] involved an alleged inadvertent disclosure of sensitive information despite the company's promises to maintain the security of that information. Specifically, Lilly put consumers' e-mail addresses in the "To" line of the e-mail that was sent to Prozac users who subscribed to a service on Lilly's website, essentially disclosing the identities of all of the Prozac user-subscribers.

Given the sensitivity of the information involved, this disclosure was a serious breach. Nevertheless, the Commission recognized that there is no such thing as "perfect" security and that breaches can occur even when a company has taken all reasonable precautions. Therefore, the Commission construed statements in Lilly's privacy policy as a promise to take steps "appropriate under the circumstances" to protect personal information. Similarly, the complaint alleged that the breach resulted from Lilly's "failure to maintain or implement internal measures

appropriate under the circumstances to protect sensitive consumer information."[10] The focus was on the reasonableness of the company's efforts.

According to the complaint in the Lilly matter, the company failed, among other things, to provide appropriate training and oversight for the employee who sent the e-mail and to implement appropriate checks on the process of using sensitive customer data. The order contains strong relief that should provide significant protections for consumers, as well as "instructions" to companies. First, it prohibits the misrepresentations about the use of, and protection for, personal information. Second, it requires Lilly 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, every year the company must have its program reviewed by a qualified person to ensure compliance.

2. Not All Security Breaches Are Violations of FTC Law

The second principle that arises from the Commission's enforcement in the information security area is that not all breaches of information security are violations of FTC law – the Commission is not simply saying "gotcha" for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen, as noted above, even when a company has taken every reasonable precaution. In such instances, the breach will 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.

When breaches occur, our staff reviews available information to determine whether the incident warrants further examination. If it does, the staff gathers information to enable us to

assess 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. 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."[12] 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.,[13] 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 data such as credit card numbers, and Web-based applications are often the "front door" to these databases. It is critical that online companies take reasonable steps to secure these aspects of their systems, especially when they have made promises about the security they provide for consumer information.

In Guess, the Commission alleged that the company broke such a promise concerning sensitive information collected through its website, www.guess.com. According to the Commission's complaint, by conducting a "web-based application" attack on the Guess website,

an attacker gained access to a database containing 191,000 credit card numbers. This particular type 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 under Section 5 of the FTC Act, the Commission also has responsibility for enforcing 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.[14] The Rule became effective on May 23 of this year, and the Commission expects that it will quickly become an important enforcement and guidance tool to ensure greater security for consumers' sensitive financial information. The Safeguards Rule 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 covered, the Rule requires a plan that accounts for 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 risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust 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. The Safeguards Rule requires businesses to consider all areas of their operation, but identifies three areas that are particularly important to information security: employee management and training; information systems; and management of system failures.

Prior to the Rule's effective date, the Commission issued guidance to businesses covered by the Safeguards Rule to help them understand the Rule's requirements.[15] 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. Now that the Rule is effective, the Commission is investigating 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 educational 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,[16] publication of business guidance regarding common vulnerabilities in computer systems,[17] 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 outreach effort is centered on the Commission's information security website.[18] The website registered more than 400,000 visits in its first year of deployment, making it one of the most popular FTC web pages. The site is now available in CD-ROM and PDF format and frequently updated with new information for consumers on cybersecurity issues. In addition, 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; distributed 160,000 postcards featuring Dewie and his information security message to approximately 400 college campuses nationwide; and coordinated the 2003 National Consumer Protection Week with a consortium of public- and private-sector organizations around the theme of information security.

Finally, the Commission's Office of Congressional Relations has conducted outreach through constituent service representatives in each of the 535 House and Senate member offices by mailing "Safe Computing" CDs. We would like to thank Chairman Stearns for his leadership on the issue of cybersecurity, and for encouraging his colleagues, in his July 18, 2003 "Dear Colleague" letter announcing the delivery of the FTC's safe Internet practices outreach kit, to educate their constituents on safe computing practices.

In addition, the Commission uses opportunities that arise in non-security cases to educate the public about security issues. For example, in early November, the Commission announced that a district court issued a temporary restraining order in an action against D Squared Solutions, and its principals.[19] The complaint alleged that the defendants operated a scam that barraged consumers' computers with repeated Windows Messenger Service pop up ads – most of which advertised software that consumers could purchase for about $25 to block future pop ups. Part of what made the defendants' conduct so egregious is that consumers continued to be

bombarded by pop-ups, even when they were off of the Internet and working in other applications such as word-processing or spreadsheet programs and that the defendants allegedly either sold or licensed their pop-up sending-software to other people allowing them to engage in the conduct. The defendants' website allegedly offered software that would allow buyers to send pop-ups to 135,000 Internet addresses per hour, along with a database of more than two billion unique addresses. Contrary to the defendants' representations, consumers, when educated about how the Windows operating systems works, can actually stop pop-up spam at no cost by changing the Windows default system.

In addition to bringing a law enforcement action to halt the defendants' conduct, the Commission issued an alert to consumers about the security issues raised in the case. The "Consumer Alert" provides instructions for consumers on how to disable the Windows Messenger Service in order to avoid other pop-up spam. The alert[20] also discusses the use of firewalls to block hackers from accessing consumers' computers.

Finally, the Commission continues, and will continue, to host workshops on information security issues when appropriate. Last summer, the Commission hosted two workshops focusing on the role technology plays in protecting personal information.[21] The first workshop focused on the technologies available to consumers to protect themselves. Panelists generally agreed that, to succeed in the marketplace, these technologies must be easy to use and built into the basic hardware and software consumers purchase.

The second workshop focused on the technologies available to businesses. We learned that businesses, like consumers, need technology that is easy to use and compatible with their other systems. Unfortunately, we also heard that too many technologies are sold before

undergoing adequate testing and quality control, frustrating progress in this area.

The Commission also held a workshop on unsolicited commercial e-mail ("spam") which was instructive about the security risks that spam poses. We learned that, in addition to other problems, spam can also serve as a vehicle for malicious and damaging code.

D. International Efforts

In addition to our cases and domestic efforts, the Commission has taken an active international role in promoting cybersecurity. We recognize that American society and societies around the world need to think about security in a new way. The Internet and associated technology have literally made us a global community. We are joining with our neighbors in the global community in this enormous effort to educate and establish a culture of security.

During the summer of 2002, the Organization for Economic Cooperation and Development ("OECD") issued a set of principles for establishing a culture of security – principles that can assist us all in minimizing our vulnerabilities. Commissioner Swindle has had the opportunity to work with this organization and to head the U.S. Delegation to the Experts Group on the post-September 11 review of existing OECD Security Guidelines and to the Working Party on Information Security and Privacy.

The OECD principles are contained in a document entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security."[22] The nine principles are an 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, including 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. They already have been the model for more sector-specific guidance by industry groups and associations.

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 governmental partners in Asia and in the EU also are working on cybersecurity initiatives.

Notwithstanding these global efforts, developing a "Culture of Security" is a daunting challenge. The FTC 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. The critical lesson in this information-based economy is that we are all in this together: government, private industry, and consumers, and we must all take appropriate steps to create a culture of security.

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. 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 brought Internet cases using the unfairness doctrine. See *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) (setting forth the commission's Deception Policy Statement.).

9. The Commission's final decision and order against Eli Lilly is available at www.ftc.gov/os/2002/05/elilillydo.htm. The complaint is available at www.ftc.gov/os/2002/05/elilillycmp.htm.

10. *Eli Lilly Complaint*, paragraph 7.

11. The Commission's final decision and order against Microsoft is available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf. The complaint is available at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

12. *Microsoft Complaint*, paragraph 7.

13. 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.

14. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

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

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

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

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

19. The Commission's press release announcing the case can be found at http://www.ftc.gov/opa/2003/11/dsquared.htm.

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

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

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