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

INFORMATION SECURITY – CHALLENGES FOR CONSUMERS AND BUSINESSES

June 16, 2004

I. Introduction

Mr. Chairman and members of the subcommittee, I am Howard Beales, Director of the Federal Trade Commission's Bureau of Consumer Protection.[1] I appreciate the opportunity to appear before you today to discuss the challenges consumers and businesses face in protecting their computer systems – and the information contained in them – as well as the Commission's role in promoting a culture of security.

Today, maintaining the security of our computer-driven information systems is essential. A secure information infrastructure is required for the operation of everything from our traffic lights to our credit and financial systems, nuclear and electrical power supplies, and emergency medical service. Consumers rely on and use computers at work and at home; increasingly, 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 them, 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] Securing these systems against an ever-changing array of threats is challenging, particularly for consumers and small businesses.

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 its other consumer protection efforts. The Commission has sought to address concerns about computer

security through a combined approach that includes educating consumers and businesses about emerging threats and the fundamental importance of good security practices; targeted law enforcement actions; and international cooperation. The Commission's educational efforts 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. In information security matters, the Commission's 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] In addition, in an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information.

A. Workshops, Education, and Outreach

1. Security Challenges and Possible Solutions

One of the Commission's most successful strategies in this area is to hold public workshops designed to educate the agency and the public about

behavior, and representatives from consumer and privacy groups. The panelists identified a range of challenges facing consumers, industry, and policy makers. For example, many consumers do not buy the privacy tools now on the market because they are often available only as expensive, hard-to-use system add-ons. Consumers also use these tools improperly – for example, failing to configure their firewalls appropriately, using easily-guessed passwords, or using anti-virus software and operating systems without properly updating them.

accountability and limited IT training budgets for the protection of consumer information.

Panelists discussed a variety of ways to address these challenges. To help consumers understand the importance of information security and use privacy tools more effectively, panelists discussed the value of an educational campaign similar to the ones launched to increase seatbelt use or discourage smoking. Such a campaign may take time to produce changes in consumer behavior, but could ultimately teach consumers to take a more proactive role in protecting their computers and their personal information. Panelists also urged technology vendors to make security support and updates easier and more automatic for consumers, especially for legacy systems that remain in widespread use and are highly vulnerable to intrusion. Many panelists also agreed that privacy-enhancing technologies, in order to be most effective, should be more tightly integrated or "baked in" to systems so that even novice users can easily enjoy their protections.

To help businesses develop better ways to protect their systems, panelists urged the adoption of a comprehensive risk-management strategy that incorporates four critical elements: (1) people, (2) policy, (3) process, and (4) technology. Panelists discussed how each of these elements plays a role in security problems and solutions. For example, companies must (1) train their *people* about the threats to information systems and the steps they should take to address them; (2) develop and communicate *policies* regarding the appropriate use of information and computer systems; (3) put in place *processes*

The Commission's information security website[12] has registered more than 620,000 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; 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.

The Commission's Office of Congressional Relations has also conducted outreach through constituent service representatives in each of the 535 House and Senate member offices by providing "Safe Computing" CDs to encourage incorporation of safe computing information into mailings, newsletter articles, and other communication channels. More than 40 members now host links to FTC online resources, with many devoting entire sections of their websites to consumer protection, including identity theft and information security. In the past two years, the FTC staff have also participated in more than 20 town-hall meetings about consumer protection and information security issues. Further, the agency also has participated in consumer education events on Capitol Hill, including joining the Congressional Internet Caucus Advisory Committee on a series of workshops related to information security.

In addition, the FTC is working with the Department of Homeland Security (DHS) and such organizations as the National Cyber Security Partnership and the National Cyber Security Alliance Stay Safe Online[13] to promote its educational campaign more broadly. The National Cyber Security

Partnership created five task forces to examine (1) home user awareness; (2) corporate governance; (3) cyber security early warning; (4) software development; and (5) technical standards and common criteria. This Spring, the awareness task force issued a report recommending a number of concrete proposals to increase consumer awareness. The

information to keep their accounts active, and then direct them to a "look-alike" Web site of the legitimate business, further tricking consumers into thinking they are responding to a bona fide request. Unknowingly, consumers submit their financial information – not to the businesses, but to the scammers – who use it to order goods and services and obtain credit.

4. Spyware

Finally, just this April, the Commission hosted a workshop to explore issues associated with "spyware" – software that is loaded on personal computers without users' consent.[17] The discussion at the workshop clarified that some of this software can cause privacy, security, and functionality problems for consumers. In particular, spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. It also may facilitate identity theft by surreptitiously planting a keystroke logger that records the characters typed on a user's personal computer, including passwords, credit card numbers, and other personal information. Spyware may create security risks if it exposes communication channels to hackers. It also may affect the operation of personal computers, causing crashes, browser hijacking, home page resetting, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

The Commission's workshop also clarified how spyware can cause problems for businesses, too. Companies may incur costs as they seek to block and remove spyware from the computers of their employees. Employees will be less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could also be used to obtain trade secrets and other confidential information from businesses.

Commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.[20] In four separate cases, brought against Eli Lilly,[21]

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 threats before a compromise occurs.

- ***Good Security is an Ongoing Process of Assessing 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.

2. GLB Safeguards Rule

In addition to 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.[25] 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 non-bank 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 significantly reduce risks to this information, including identity theft.

The Rule requires covered 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 gives each company the flexibility to develop a plan that takes into account 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 Commission has issued guidance on the Rule[26] and met with a variety of trade associations and companies to promote compliance. Currently, Commission staff is conducting non-public investigations of covered entities.

Finally, pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),[27] the Commission recently issued a proposed rule designed to enhance the security of consumer report information.[28] The proposed rule is designed to prevent unauthorized disclosure of consumer information and to reduce the risk of fraud or identity theft by ensuring that records containing sensitive financial or personal information are appropriately redacted or destroyed before being discarded. The Commission anticipates the issuance of a final rule by the end of the year.

C. International Efforts

In addition to its law enforcement and education efforts, the Commission has taken an active international role in promoting cybersecurity. The Commission recognizes 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. The Commission is 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 voluntary principles for establishing a culture of security – principles that can assist us all in minimizing 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."[29] 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, 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 will remain 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.

Finally, in January of this year, the FTC partnered with 36 agencies from 26 countries around the world to launch "Operation Secure Your Server," an international effort to reduce the flow of

unsolicited commercial e-mail by urging organizations to close "open relays" and "open proxies."[30] As part of the initiative, the participating agencies identified tens of thousands of owners or operators of potentially open relay or open proxy servers around the world. The agencies sent letters urging these owners or operators to protect themselves from becoming unwitting sources of spam and providing guidance on inexpensive steps to take to secure their servers.[31]

III. Conclusion

Security presents challenges for everyone in our global information-based economy, but particularly for consumers and small businesses. The Commission is committed to continuing its work promoting security awareness and sound information practices through education, enforcement, and international cooperation.

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. For example, the Commission's 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. In May 2002, the Commission also held a workshop on Consumer Information Security. For

The partnership was created as part of the December 2003 National Cyber Security Summit held in Santa Clara, California.

14. *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.

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

16. *See*, e.g., http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm. Working closely with the FBI and Department of Justice, the Commission has also brought enforcement actions challenging unfair and deceptive practices in connection with "phishing." *See* cases cited *infra* note 19.

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

18. 15 U.S.C. § 45 (a) (1).

19. 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. 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.

20. 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.).

21. Final Decision and Order at www.ftc.gov/os/2002/05/elilillydo.htm; Complaint at www.ftc.gov/os/2002/05/elilillycmp.htm.

22. Final Decision and Order at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf; Complaint at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

23. Final Decision and Order at http://www.ftc.gov/os/2003/06/guessagree.htm; Complaint at http://www.ftc.gov/os/2003/06/guesscmp.htm.

24. Final Decision and Order at http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf; Complaint at http://www.ftc.gov/os/caselist/0323209/040602comp0323209.pdf.

25. 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).

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

27. The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), Pub. L. No. 108-159 (2003). In general, the FACT Act amends the Fair Credit Reporting Act to enhance the accuracy of consumer reports and to allow consumers to exercise greater control regarding the type and