PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

COMMITTEE ON SMALL BUSINESS

U.S. HOUSE OF REPRESENTATIVES

hearing on

THE STATE OF SMALL BUSINESS SECURITY IN A CYBER ECONOMY

March 16, 2006

I. Introduction

Mr. Chairman and members of the Subcommittee, I am Lydia Parnes, 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 small 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.

For more than a decade, one of the FTC's top priorities has been protecting the privacy of American consumers. The Commission is committed to vigorous consumer and business education efforts, aggressive law enforcement, and global cooperation to safeguard the security of consumers' personal information. To date, the agency has brought 12 data security cases, six spyware and adware cases, more than a dozen financial pretexting cases, and over 80 spam cases. More cases in all of these critical areas are being developed.

Maintaining the security of computer-driven information systems is essential in the information age. A secure information infrastructure is required for the operation of everything from traffic lights to credit and financial systems, communications networks, and emergency medical service. The explosive growth of the Internet and the development of sophisticated computer systems and databases have made it easier than ever for companies large and small to gather and use information about their customers. Small businesses that once were limited to customers walking past store fronts on Main Street USA now can reach consumers across the globe. Transactions that once were conducted face-to-face now are conducted entirely online.

---

[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.

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. Security breaches can 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 small businesses.

II. The Federal Trade Commission's Role

The Federal Trade Commission is the federal government's principal consumer protection agency. Congress directed the Commission, under the FTC Act, to take law enforcement action against "unfair or deceptive acts or practices" in almost all sectors of the economy and to promote vigorous competition in the marketplace.[3] With the exception of certain industries and activities, the FTC Act provides the Commission with broad investigative and enforcement authority over entities

---

[2] *See, e.g., United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006)(FTC alleged that at least 800 cases of identity theft arose out of information compromise); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006)(FTC alleged that data security breach compromised more than 1.4 million credit and debit cards, resulting in fraudulent charges on some of these accounts). *See also* Federal Trade Commission – Identity Theft Survey Report (Sept. 2003) *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf. This 2003 FTC survey estimated that nearly 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated $48 billion in losses, and costing consumers an additional $5 billion in out-of-pocket losses. The survey looked at the two major categories of identity theft: (1) the misuse of existing accounts; and (2) the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims, in both the time and money spent resolving the problems.

[3] 15 U.S.C. § 45.

engaged in, or whose business affects, commerce.[4] The FTC Act also authorizes the Commission to conduct studies and collect information, and, in the public interest, to publish reports on the information it obtains.

The Federal Trade Commission's approach to information security is similar to the approaches taken in its other consumer protection efforts: it 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,[5] which prohibits unfair or deceptive acts or practices, the Commission's Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule"),[6] and the Fair Credit Reporting Act ("FCRA").[7] In addition, in an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information. An online presence can allow a small business to reach customers anywhere on the globe. And businesses routinely contract for services with providers in other countries. In fact, a company's web servers may be located on a different continent from its other operations.

---

[4] In addition to the FTC Act, the Commission also has responsibility under approximately 50 additional statutes governing specific industries and practices.

[5] 15 U.S.C. § 45.

[6] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[7] 15 U.S.C. §§ 1681-1681x.

A. Workshops, Education, and Outreach

1. Security Challenges and Possible Solutions

In 2003, the Commission held a workshop that explored the challenges consumers and businesses face in securing their computers.[8] Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop also examined the role of technology in meeting these challenges.[9]

Workshop participants included industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups. The panelists identified a range of challenges facing consumers, industry, and policy makers. For example, many computer users do not buy the privacy tools now on the market or, if they do, they often use these tools improperly – for example, failing to appropriately configure their firewalls, using easily-guessed passwords, or using anti-virus software and operating systems without properly updating them.

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

---

[8] In May 2002, the Commission also held a workshop on Consumer Information Security. For more information, including transcripts of the workshop, *see* http://www.ftc.gov/bcp/workshops/security/index.html. For links to subsequent Commission workshops on spam, email authentication, Radio Frequency Identification, spyware, and peer-to-peer file-sharing, *see* http://www.ftc.gov/ftc/workshops.htm.

[9] The workshop agenda and transcripts are available at www.ftc.gov/bcp/workshops/technology. The Staff Report is available at http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf.

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* to ensure that policies are implemented; and (4) deploy *technology* effectively and securely.

2. FTC's Information Security Campaign

In addition to holding workshops, the FTC for several years has engaged in a broad outreach campaign to educate businesses and consumers about information security and the precautions they can take to protect or minimize risks to personal information. These efforts have included publication and widespread dissemination of detailed information for consumers and small businesses; publication of business guidance regarding common vulnerabilities in computer systems,[10] and responding to information compromises;[11] and speeches and presentations. 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.

Last September, the FTC unveiled an innovative multimedia campaign to educate consumers about basic computer security practices. This cybersecurity campaign, called OnGuard Online, is built around seven tips about online safety that will remain relevant even as technology evolves, as well as modules with information on specific topics such as phishing, spyware, and spam.[12] It

---

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

[11] *See* Information Compromise and the Risk of Identity Theft: Guidance for Your Business, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf.

[12] *See* http://www.OnGuardOnline.gov. The seven tips are described in detail in the FTC publication, Stop Think Click: Seven Practices for Safer Computing *available at*

includes articles, videos, and engaging interactive quizzes – in English and in Spanish.[13] In addition, it provides information about where to get help, ensuring that consumers know that they are not alone as they travel through cyberspace.

The FTC created OnGuard Online with consumers in mind, but it is a valuable tool for small businesses as well. According to the Small Business Administration, the majority of U.S. firms have fewer than five employees. In many ways, computer users in small businesses are similar to home users. They use similar applications to participate in e-commerce, send email, build spreadsheets, and create presentations. Moreover, as in the typical household, often there is no information technology professional on site. It is critical that small businesses educate their employees about good computer security practices. OnGuard Online can help them do that.

OnGuard Online is branded independently of the FTC. The FTC encourages other organizations to make the information their own and to disseminate it to reach the most people. OnGuardOnline.gov has attracted over 750,000 unique users in less than six months, and the agency has distributed over 800,000 brochures and bookmarks. In addition, numerous firms and government agencies – including many small businesses[14] – are now using the OnGuard Online materials in their own internal security training programs.

---

http://onguardonline.gov/stopthinkclick.html. The seven practices for safer computing are: (1) Protect your personal information; (2) Know who you're dealing with; (3) Use anti-virus software and a firewall, and update both regularly; (4) Be sure to set up your operating system and Web browser software properly, and update them regularly; (5) Protect your passwords; (6) Back up important files; and (7) Learn who to contact if something goes wrong online.

[13] *See* http://www.AlertaEnLinea.gov.

[14] The FTC has received emails to its OnGuardOnline@ftc.gov email account from businesses that are using OnGuard Online materials in internal security training. For example, a community bank manager from New York wrote, "We feel [OnGuardOnline.gov] would be a great training tool for all of our bank employees."

The Commission's Office of Congressional Relations also has 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 100 members now host links to FTC online resources, with many devoting entire sections of their Web sites to consumer protection issues, including identity theft and information security. In the past two years, the FTC staff has also participated in more than 40 town-hall meetings about consumer protection and information security issues. Further, the agency 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.

3. One Education Issue: "Phishing"

One specific OnGuard Online component educates computer users about phishing.[15] Phishing is a common high-tech scam that uses spam to deceive computer users into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive personal information. These spam messages often pretend to be from businesses with whom the potential victims deal – for example, their Internet service provider, online payment service, or bank. The fraudsters tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and then direct them to a "look-alike" Web site of the legitimate business, further tricking computer users into thinking they are responding to a bona fide request. Unknowingly, computer users submit their financial information – not to the businesses, but to the scammers – who

---

[15] *See* http://onguardonline.gov/phishing.html. For other examples of anti-phishing educational materials, *see* FTC's consumer alert: "How Not to Get Hooked by a 'Phishing' Scam," *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf.

use it to order goods and services and obtain credit.

Consumer education is a key to solving the phishing problem. Identifying individual phishers is extremely difficult; but if computer users are educated not to email financial information in response to a pop-up solicitation or email inquiry, they can protect themselves. Small businesses also can play an important role in educating their employees and customers about the importance of protecting their personal information.[16] Companies should not email their customers asking for personal information. And they should let their customers know that they will never send such a request.

B. The FTC's Efforts to Combat Spyware

Spyware is another serious threat to the security of consumer and small business data. In 2004, the FTC sponsored a public workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software," and in March 2005, the Commission released a staff report based on the information received in connection with the workshop.[17] The staff report documents how spyware causes problems for businesses. Companies incur costs as they seek to block and remove spyware from the computers of their employees. Employees are less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware

---

[16] *See* Jon Swartz, *Phishing Scams Aim to Bilk Smaller Prey,* USA Today, March 13, 2006 at 1B (noting that phishing scams increasingly are targeting regional credit unions and local banks).

[17] The agency received almost 800 comments in connection with the workshop, and 34 representatives from the computer and software industries, trade associations, consumer advocacy groups and various governmental entities participated as panelists. The workshop agenda, transcript, panelist presentations, and public comments received by the Commission are available at http://www.ftc.gov/bcp/workshops/spyware/index.htm. The FTC Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software, released March 2005, is available at http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

that captures the keystrokes of employees could also be used to obtain trade secrets, consumer data, and other confidential information from businesses.

One of the principal conclusions of the FTC staff's report was that active enforcement of existing consumer protection laws can help prevent the spread of spyware. Using the FTC Act's grant of broad authority to challenge unfair or deceptive acts and practices, the Commission launched an aggressive law enforcement program to fight spyware. To date, the FTC has filed six cases addressing spyware and adware and more cases are under investigation.[18]

The staff report emphasized that better technology needs to be developed to protect computer users from spyware. Fortunately, substantial efforts are currently underway to address spyware. In response to market forces, industry is developing and deploying new technologies to assist computer users. Consumers and businesses are becoming more aware of the risks of spyware, and they are responding by installing anti-spyware products and other measures. In addition, industry is helping protect consumer privacy by developing privacy-enhancing technologies.

C. Business Data Security Practices

Regardless of how well consumers secure their own information and computer systems, their personal information may still be vulnerable if the businesses with which they interact fail to implement safeguards. Therefore, in addition to its education and outreach efforts, the Commission also has sought to encourage better cybersecurity practices by bringing law enforcement actions

---

[18] *See FTC v. Enternet Media*, No. 05-7777 CAS (C.D. Cal. filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com, Inc.*, Docket No. C-4147 (filed Sept. 12, 2005); *FTC v. Trustsoft, Inc.*, No. H 05 1905 (S.D. Tex. May 31, 2005); *FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wash. Mar. 8, 2005); *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

against companies that fail to implement reasonable procedures to protect sensitive consumer information.

1. 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."[19] To date, the Commission has filed five data security cases based on deception, 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.[20] In each of these cases, the Commission alleged that the companies made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers.[21] Their security measures, however, were grossly inadequate and their promises therefore deceptive.

More recently, the Commission has used its authority under the FTC Act's unfairness standard[22] to bring cases in the area of data security. In four cases, the Commission has alleged that

---

[19] 15 U.S.C. § 45(a)(1).

[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] *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[22] The FTC Act defines "unfair" practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably outweighed by countervailing

the failure to take reasonable security measures to protect sensitive customer data was an unfair practice in violation of the FTC Act.[23]

One of the FTC's most recent law enforcement actions arose from ChoicePoint's high-profile breach that occurred last year.[24] According to the complaint, ChoicePoint's failures allegedly allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. The FTC alleged that at least 800 cases of identity theft arose out of these incidents. The Commission obtained $10 million in civil penalties for Fair Credit Reporting Act violations (the highest civil penalty ever levied in a consumer protection case), $5 million in consumer redress for identity theft victims, and significant injunctive provisions that require ChoicePoint to implement a variety of new data security measures. This settlement is an important victory for consumers and also an important lesson for industry.

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

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.

Second, in the information security area, not all breaches of information security are violations

---

benefits to consumers or competition." 15 U.S.C. § 45(n).

[23] *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006); *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006)*; In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

[24] *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006).

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 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.

Third, 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. Companies have a legal obligation to take reasonable steps to guard against threats before a compromise occurs.

Finally, 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

[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).

enforcement and guidance tool to ensure greater security for consumers' sensitive financial information.

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. To date, the Commission has brought three cases enforcing the security requirements of the Safeguards Rule. [27]

Safeguarding customer information makes good business sense. In testimony on data security,

---

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

[27] *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005)*; Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (April 12, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005).

the Commission has recommended that Congress consider whether all companies that hold sensitive consumer data should be required to take reasonable measures to ensure its security.[28] When a small business shows that it cares about the security of customers' personal information, it increases those customers' confidence in the company. Developing a plan is a good business practice for any company that handles consumer information such as names, addresses, account numbers, or Social Security numbers.

3. The Disposal Rule

When a business disposes of information, it should do so in a secure manner. This is particularly true when handling or disposing of credit reports and similar consumer reports. Pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),[29] the Commission recently issued the Disposal of Consumer Report Information and Record Rule ("Disposal Rule").[30] The Disposal Rule is designed to prevent unauthorized access to sensitive consumer report information by requiring all users of the reports to dispose of them properly – and not, for example, leave them lying in a dumpster available to identity thieves. Like the Safeguards Rule, the Disposal Rule contains a flexible standard – "reasonable measures to protect against unauthorized access" to the information being disposed of. However, the rule also cites some specific examples of "reasonable

---

[28] *See* Prepared Statement of the Federal Trade Commission before the Committee on Commerce, Science, and Transportation of the United States Senate, on Data Breaches and Identity Theft (June 16, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[29] On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was enacted. Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified at 15 U.S.C. § 1681 *et seq.*). Many of the provisions amend the Fair Credit Reporting Act. 15 U.S.C. § 1681 *et seq.*

[30] 16 C.F.R. Part 382. *See* www.ftc.gov/os/2004/11/041118disposalfrn.pdf.

measures," including burning, pulverizing, and shredding papers, and destroying or erasing electronic media, so that they cannot practicably be read or reconstructed. In order to help businesses comply with the Rule, the FTC released a business alert on the Disposal Rule in June 2005, when the Rule took effect.[31] Even when companies are not required to comply with the Safeguards Rule and the Disposal Rule, their principles provide valuable guidance for protecting sensitive consumer information.

D. International Efforts

The Internet and associated technology have created a global community. Thus, in addition to its law enforcement and education efforts, the Commission has taken an active international role in promoting cybersecurity. The Commission is joining with its neighbors in the global community in this important effort to educate and establish a culture of security.

Last June, the FTC submitted a report to Congress recommending legislation called the US SAFE WEB Act – Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers across Borders.[32] The proposed legislation would enable the FTC to share key information with foreign partners, assisting international law enforcers in pursuing security breaches in their countries that impact U.S. consumers. The legislation also would help the FTC fight deceptive spam and spyware by allowing the agency to investigate more fully messages transmitted through facilities outside the United States.

---

[31] *See* http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.pdf.

[32] FTC, The US SAFE WEB ACT: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress (June 2005), *available at* http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf. Senator Gordon Smith introduced S. 1608, the "US SAFE WEB Act," on July 29, 2005. The bill was unanimously reported out of the Senate Committee on Commerce, Science, and Transportation on December 15, 2005.

E. Hearings on Global Marketing and Technology

In 1995, the FTC held hearings for government policymakers to consider the risks presented by rapidly evolving technologies such as the Internet and to formulate policies to address these risks. This February, the agency announced that in November 2006, a decade after the original hearings, the FTC once again will bring together experts from the business, government, and technology sectors, as well as consumer advocates, academicians, and law enforcement officials to explore the ways in which technological convergence and the globalization of commerce impact consumer protection. The new hearings will examine changes that have occurred in marketing and technology over the past decade, and garner experts' views on coming challenges and opportunities for consumers, businesses, and government. The FTC hopes to receive significant input from the small business community as it plans for, and holds, those hearings.

III. Conclusion

Consumers and businesses must be vigilant about data security in the global information-based economy. The Commission is committed to continuing its work promoting security awareness and sound information practices through education, enforcement, and international cooperation.