

**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 issues related to information security. One such workshop, held in two sessions during May and June 2003, specifically explored the issues before this subcommittee today – namely, the challenges consumers and businesses face in securing their computers.⁵ Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop also examined the role of technology in meeting these challenges.⁶ What the agency learned from that workshop is

summarized in a recently released Staff Report, available on the FTC website.⁷

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 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. Moreover, many consumers are largely unaware of the consequences of poorly protected systems and personal information. These consequences can range from identity theft to converting personal computers to “zombie drones” that spew out spam, to the use of a consumer’s system in an attack on a commercial Web site or on part of the nation’s critical infrastructure. Some consumers also have difficulty understanding businesses’ privacy policies.

In addition, a number of panelists cited the shortcomings of existing technological tools used by both consumers and businesses, such as secure socket layer (SSL) encryption and virtual private networks. Many agreed that SSL should be implemented more widely; however, they cautioned that SSL may give users a false sense about the security of their data at its ultimate destination, as it only encrypts data in transit and does not assure that information will be stored securely or used as stated in a privacy policy. Some also cited the security risks posed by the connection of unsecure machines to virtual private networks, which allow employees away from their offices to connect to their employer's systems. If an employee's machine is not properly configured, attackers could use it to access the virtual private network and enter the employer's

system.

Finally, panelists criticized the rapid introduction of technology, hardware, and software without adequate testing and quality assurance. They also noted the general trend toward poor 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* to ensure that policies are implemented; and (4)

deploy *technology* effectively and securely. Panelists also discussed a variety of recent initiatives, in both the public and private sectors, that have applied these principles. For example, companies have worked to reduce security flaws in code, ship products in a more secure configuration, add new security features to products, and provide better security support, such as patching and warnings, to their already-deployed products. The Department of Homeland Security has also successfully deployed its new National Cyber Alert System to warn businesses and consumers quickly about urgent security threats, and provide information on effective security policy and processes.

Panelists also discussed the extent to which benchmarks and standards can help provide guidance to industry on the effective management of security issues and, in particular, how to develop effective security programs. For example, the Center for Internet Security (CIS)⁸ has produced benchmarks for a variety of technologies, including operating systems, routers, and databases, which provide detailed guidance on how to configure technologies for increased security. Business have used these benchmarks to develop minimum security requirements for merchants authorized to accept certain payment cards and to set configuration requirements in connection with large technology purchases.

2. FTC's Information Security Campaign

In addition to holding workshops, the FTC has for several years 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 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;⁹

publication of business guidance regarding common vulnerabilities in computer systems¹⁰ and responding to information compromises;¹¹ 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 website¹² 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 Online¹³ 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 recommendations included: a comprehensive cyber security awareness campaign to reach consumers through a three-year national advertising campaign based 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.

Finally, the Commission uses opportunities that arise in non-security cases to educate the public about security issues. For example, when the Commission filed a case challenging an alleged practice that bombarded consumers’ computers with repeated Windows Messenger Service pop-up ads,¹⁴ the agency also issued a consumer alert providing instructions on how to disable the Windows Messenger Service to avoid other pop-up spam. The alert¹⁵ also discusses the use of firewalls to block hackers from accessing consumers’ computers.

3. “Phishing”

The Commission has also issued a number of alerts to consumers about “phishing.”¹⁶ Phishing is an increasingly common high-tech scam that uses spam to deceive consumers 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 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.

Fortunately, substantial efforts are currently underway to address spyware. In response to market forces, industry is developing and deploying new technologies to assist consumers. Consumers and businesses are becoming more aware of the risks of spyware, and they are responding by installing anti-spyware products and other measures. Industry representatives have indicated that they will explore best practices and consumer education on issues related to spyware. Government and industry-sponsored education programs, as well as industry self-regulation, could be instrumental in making users more aware of the risks of spyware, thereby assisting them in taking actions to protect themselves. All of these efforts are very encouraging. We are also actively investigating particular instances of questionable practices, and will take law enforcement actions as appropriate.

B. Law Enforcement

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 has also protected consumers by pursuing law enforcement actions in appropriate cases.

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.”¹⁸ To date, the Commission’s security cases have been based on deception,¹⁹ 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 four separate cases, brought against Eli Lilly,²¹ Microsoft,²² Guess,²³ and Tower Records,²⁴ the Commission alleged that the companies 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 were, therefore, deceptive.

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

§ *Security Procedures Should Be Appropriate Under the Circumstances*

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.

§ ***Not All Security Breaches Are Violations of FTC Law***

In the information security area, 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 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.

§ ***Law Violations Without a Known Breach of Security***

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 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 Rule²⁶ 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.

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 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 more information, including transcripts of the workshop, *see* <http://www.ftc.gov/bcp/workshops/security/index.html>.
6. The workshop agenda and transcripts are available at www.ftc.gov/bcp/workshops/technology.
7. The Staff Report is available at <http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf>.
8. The Center for Internet Security is a non-profit organization whose mission is to help organizations around the world effectively manage the risks related to information security. CIS manages a consensus process in which members identify security threats of greatest concern, then participate in development of practical methods to reduce the threats. CIS also provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances. *See* <http://www.cisecurity.org>.
9. *See* <http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html>.
10. *See* <http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm>.
11. *See* <http://www.ftc.gov/bcp/conline/pubs/buspubs/idthbizkit.htm>.

-
12. See <http://www.ftc.gov/infosecurity>.
13. The National Cyber Security Partnership is a 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.
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/online/pubs/alerts/popalrt.html>.
16. See, e.g., <http://www.ftc.gov/bcp/online/pubs/alerts/phishregalrt.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.gov/bcp/online/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 amount of marketing solicitations they receive. The Act also contains a number of provisions intended to combat consumer fraud and related crimes, including identity theft.
28. *See* Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21,388 (2004) (to be codified at 16 C.F.R. Part 682); available at <http://www.regulations.gov/fredpdfs/04-08904.pdf>.
29. *See* <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.
30. *See* <http://www.ftc.gov/secureyourserver>.
31. A sample letter is available at http://www.ftc.gov/bcp/online/edcams/spam/secureyourserver/letter_english.htm.