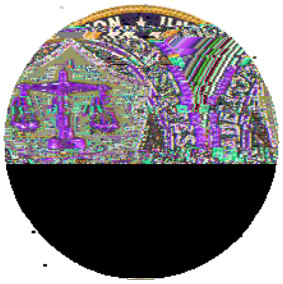

# Federal Trade Commission

**Remarks of Deborah Platt Majoras[1]**
**Chairman, Federal Trade Commission**
**Chamber of Commerce**
**Washington, DC**
**December 5, 2006**

**"Protecting Consumer Privacy in an Information Age"**

## I. Introduction

Good afternoon. I appreciate having the opportunity to talk to you about "The Future of Privacy." For more than a decade, protecting the privacy of American consumers has been a top priority at the Federal Trade Commission. Privacy, while always important, has become an issue of significant concern to consumers in an information age. The explosive growth of the Internet and the development of sophisticated computer systems and databases has made it easier than ever for companies to gather and use information about their customers. In addressing privacy concerns, however, it is important to keep in mind that these new information systems can have tremendous benefits for consumers, who can access customer service hotlines 24-hours-a-day, have easier access to credit, and enjoy many marketplace conveniences that they have come to expect. At the same time, if we do not protect sensitive information adequately, consumers can be harmed and lose confidence in the marketplace. The balance must be carefully struck: ask consumers if they care about privacy, and you will get a resounding "yes;" ask consumers if they

[1] The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any Commissioner.

greater damage may be the potential cost of consumers losing confidence in the marketplace in general, and in electronic commerce in particular. Such a loss in confidence is one we cannot afford.

So, what are we doing about it? Identity theft takes many forms and thus must be attacked on many fronts. Fully 50 percent of identity theft victims do not know the origin of the theft, while the other half typically can link their loss to a discrete event. Some identities have been stolen through low-tech methods, like stealing a wallet or "dumpster diving." Other thieves use technology, like hacking into an organization's computer system or using a credit card "skimming" device. And the method of theft used may determine the type of identity theft that results – the use of an existing account, which is most prevalent but potentially less harmful to

assistance, and more effective education are essential components in fighting identity theft. Recommendations already are being implemented. For example, members of the Task Force recently created a universal police report that makes it easier for identity theft victims to enter information about their experiences onto a common form, print the form, and submit it with their police report. It records the information in a format that can be entered into a common database for use by law enforcement. And the FTC is planning a Spring 2007 workshop to explore better methods for authenticating individuals.

In the next few days, we will post on the Web sites of the FTC, the Department of Justice, and other Task Force agencies a summary of possible recommendations to the President, with an invitation for interested parties to submit comments on those recommendations. Ultimately, we hope to deliver the strategic plan to the President early next year.

## III. Data Security

Today, I am going to focus on the first goal of our identity theft efforts, deterrence. Deterrence begins with data security – keeping sensitive information out of the hands of wrongdoers. Security problems take many forms and present many challenges, but have one commonality – data thieves will exploit any available vulnerabilities to obtain sensitive personal information. Information is today's currency, and thieves know its value. Data security is important for every kind of organization – whether a company, government agency, or university; whether a mom-and-pop shop or a multinational corporation; whether a high-tech company or a low-tech business. It also is critical to every individual, each of whom must learn to better safeguard personal data.

And, as you well know, data security can no longer be viewed solely as a domestic issue. Like so many of the consumer protection issues that the FTC tackles, privacy and data security have "gone global." It no longer makes sense simply to refer to personal information being "here" or "there." The security of personal information no longer depends on the server room "in the back" being under lock and key. With the click of a mouse it can go to, or be accessed

[3] A survey of more than 1,000 victims of data security breaches found that nearly 20% of those victims terminated their relationship with the breached company. Another 40% stated that they might terminate their relationship. The range of total costs to the business was $226,000 to $22 million, making the average cost of a breach $4.8 million. *See* Vontu, Inc.,

[6] "School District Sold Computers with Personal Information," MyrtleBeachOnline.com, November 27, 2006, available at http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/local/16109822.htm.

[7] One recent survey of U.S. small businesses, for example, found that over half of the companies had experienced a breach within the past 12 months, yet fully two-thirds of them

Trade Commission Act's proscription against unfair or deceptive practices in cases where a business made false or misleading claims about its security procedures, or where its failure to employ reasonable security procedures caused substantial consumer injury in the form of a data breach.[10]

Based on existing legal rules on data security, the FTC has developed and implemented a single, basic standard for data security: Companies should maintain reasonable and appropriate measures to protect sensitive consumer information. This "reasonableness" standard is explicitly required by the FTC's GLB Safeguards Rule[11] ("Safeguards Rule") and by the Fair Credit Reporting Act, and it has been applied by the Commission in bringing actions under Section 5 of the FTC Act.

The Safeguards Rule contemplates that reasonableness will depend on the sensitivity of the information at issue, the potential risks to that information, and the costs involved in avoiding those risks. Thus, a security plan should be adapted to the size and nature of the business, the nature of the information the business maintains, the security tools that are available, and the security risks the business is likely to face.[12] The Rule does not mandate specific technical requirements. This process-oriented approach recognizes that risks, technologies, and circumstances all change over time, and that a specific technical standard would soon be obsolete – and also might stifle innovation. Reasonableness does not mean perfection, of course; data security can be breached despite the best of security procedures. Thus, the fact that a company suffered a breach does not, in and of itself, establish that its practices were unreasonable, although it could be evidence of that fact. We believe this flexible

---

[10] 15 U.S.C. § 45.

[11] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, available at http://www.ftc.gov/ftc/legal.htm.

[12] For example, firms must prepare a written plan; designate an official with responsibility for the plan; identify, assess, and address foreseeable risks; monitor and evaluate the program for effectiveness; and adjust the plan as appropriate.

rule can serve as a model to guide all businesses in developing a data security program.

Of course, having a set of legal principles is not enough; they must be backed by vigorous enforcement. The FTC has brought 14 enforcement actions against businesses that have failed to provide reasonable data security. None of these cases has been a close call. They include cases against companies that threw files containing consumer home loan applications into an unsecured dumpster; stored sensitive information in multiple files when there was no longer a business need to keep the information; failed to implement simple, low-cost, and readily available defenses to well known Web-based hacker attacks; stored sensitive consumer information in unencrypted files that could be easily accessed using commonly known user IDs and passwords; and failed to use readily available security measures to prevent unauthorized wireless connections to their networks.

Probably the best-known FTC enforcement action involving a security breach was our action against Choicepoint. Choicepoint, a data broker, inadvertently sold information on more than 160,000 customers to data thieves who used that information to open up new accounts and commit identity theft. The FTC alleged that ChoicePoint failed to use reasonable procedures to screen prospective subscribers. For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. The Commission obtained $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in an FTC case – $5 million in consumer redress for identity theft victims, and signiBT/Thefo6Er tythe cor

data-security practices, our goal is not to rack up prosecutions. It is to motivate the private sector to create a culture of security throughout their operations. In conjunction with our law enforcement, the FTC has published guidance for the business community on reducing threats to computer security and on complying with the Safeguards Rule.[14] The FTC also has issued a publication on managing data compromises.[15] I encourage you to look at these materials and to familiarize yourself with other resources that are available.

### D. Public Sector Efforts to Improve Data Security

Your government, too, as a holder of extensive information on consumers, has more work to do to secure our data, and one important focus of the Identity Theft Task Force is ensuring that the federal government maintains high standards for data security.

As you probably know, all federal agencies, including the FTC, must comply with a comprehensive set of rules governing privacy and data security. The recent high-profile data security breaches at federal agencies, however, highlighted the fact that the federal government needs to do a better job. To that end, over the past six months, the Office of Management and Budget has directed every agency to implement new policy and procedural initiatives to better safeguard sensitive information. For example, each agency is required to encrypt all data on mobile computers and devices. And, drawing on the efforts of the Identity Theft Task Force, the government now has a plan for responding to data breaches that could pose a risk of identity theft.[16]

Social Security numbers often are the key to the most pernicious form of identity theft, when the thief opens new accounts in the consumer's name. Interim recommendations of the

---

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

[15] *See* Information Compromise and the Risk of Identity Theft: Guidance for Your Business, available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.pdf.

[16] *See* Memorandum from the Identity Theft Task Force, Identity Theft Related Data Security Breach Notification Guidance, September 19, 2006.

Task Force also included proposals to minimize or eliminate the unnecessary use of Social Security numbers. For example, the Task Force recommended that the Office of Personnel Management examine and reduce the collection and use of Social Security numbers in the human resources context. More broadly, the Task Force recommended that OPM issue guidance for agencies on ways to minimize or eliminate use of Social Security numbers by federal agencies, including on forms and systems, where they are unnecessary for an agency's operation or where an alternative, such as an employee number, can be used.

## IV. Consumer Resources

While there is no guarantee that consumers can avoid identity theft, they are by no means powerless. They can and must take certain steps to avoid being victimized. In 1998, the Identity Theft Assumption and Deterrence Act ("the Identity Theft Act") assigned the FTC a unique role in combating identity theft and coordinating government efforts.[17] While we cannot prosecute the crime because we have only civil jurisdiction, we take consumer complaints and implement the Identity Theft Data Clearinghouse, a centralized database of victim complaints used by 1,300 law enforcement agencies; assist victims and consumers who wish not to be victims by providing information and education; and educate businesses on sound security practices.

Educating consumers is essential in the fight against identity theft. The FTC recently launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend." The message for consumers is that they can:

DETER identity thieves by safeguarding their personal information;

DETECT suspicious activity by routinely monitoring their financial accounts, billing statements, and credit reports; and

And they should DEFEND against ID theft as soon as they suspect it. Quick action is

[17] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

essential.

One component of the campaign is a consumer education kit, which is aimed at helping organizations educate their employees, their customers, and their communities about how to minimize their risk. The kit includes a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video.

The Deter, Detect, Defend campaign has been very popular – we have distributed more than 1.5 million brochures and 30,000 kits. And we have formed many partnerships to help us broaden our reach. Recently, for example, the National Association of Realtors, which has 1.2 million members, partnered with the FTC to educate homebuyers. NAR is distributing consumer education brochures and DVDs to realtors across the country, through its more than 1,400 local and state associations. All of the materials are available in English and in Spanish. I hope you will visit www.ftc.gov/idtheft to check them out, and use them in your education efforts.

The FTC also sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[18] The website offers guidance for online safety and provides information on specific topics such as phishing, spyware, and spam. The site also features interactive quizzes, articles, and videos on a range of topics, as well as information about other resources that are available to help consumers navigate the world of cybersecurity. Since its unveiling in September 2005, OnGuardOnline has attracted approximately 2.5 million visitors. Recently, several social networking sites featured OnGuard Online as a prominent link and have driven a good deal of traffic to our Web site. And for the second year in a row, Boeing is featuring OnGuardOnline materials in its internal security training.

Indeed, the FTC has recently collaborated with the Chamber of Commerce on consumer education issues. As part of a "Get Net Safe" initiative to promote online security, the Chamber and Microsoft co-sponsored panel discussions in 12 cities addressing how to stay safe online.

---

[18] *See* www.onguardonline.gov.

The OnGuard Online campaign is a featured part of this initiative.

## V. Legislative Developments

As you know, Congress has been considering a variety of bills on data security. While none has been enacted to date, I expect that the new Congress will be revisiting this issue next year. I have testified several times on these issues, urging Congress to use caution in passing any new laws, so that in an effort to safeguard data we do not inhibit consumers' commercial transactions.

In our view, should Congress pass legislation, it should focus on imposing a reasonableness standard that would apply to all businesses that maintain sensitive consumer information. Most of the breach notification bills have included a "safeguards" requirement of this sort.

In addition, we have advised that Congress should consider a national data breach notification law that would require notice to consumers when their sensitive personal information has been breached in a way that creates a significant risk of identity theft.[19] Notice can help consumers prevent or mitigate harm resulting from a data breach by allowing them to take precautions. Notice alerts consumers whether they need to monitor their accounts more closely, close their accounts, or place fraud alerts on their credit reports. Notice also alerts consumer reporting agencies and law enforcement to the risk of fraud so that they can take appropriate actions to assist consumers in preventing identity theft.

In our view, however, notification makes sense only when it is useful to consumers, and not in situations involving remote or insignificant risks. Notifying consumers when risks are insignificant may cause them to spend time and money taking protective steps that are not necessary. Further, over time, excessive breach notification can overwhelm consumers, with the

---

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

result that they start ignoring such notification. Accordingly, breach notice legislation should include a risk-based trigger.

## VI. Technology Developments

Of course, it is not enough to actively confront the privacy risks of today. We also must seek to anticipate and understand the risks of tomorrow, and then develop sound policies to address these new risks. In an effort to better understand the implications of technology changes on privacy and consumer protection, last month the FTC convened public hearings, which we dubbed "Protecting Consumers in the Next Tech-ade."[20] During the "Tech-ade" hearings, we heard from more than 100 of the best and the brightest in the tech world about the new technologies on the horizon and their potential effect on consumers.

Panelists raised privacy and data security issues, including during the discussions of, among other things, a range of payment devices and systems, such as on-line banking, contact-less devices, mobile telephone payments, and smart cards.

One data security issue discussed at the Tech-ade hearings aptly illustrates the potential benefits and risks of new technologies. Panelists at Tech-ade presented information about advances s78 Pr0Ti.545w[ Dor-ade,ade,ade,ade,ade,ad4(e)-.6gies. Paneli about)Tpn',addPanech-.00ed at-accepl

[20] For further information about this event, see http://www.ftc.gov/bcp/workshops/techade/who.html.

[21] Authentication involves comparing information that an individual provides (such as a password or fingerprints) with stored information to determine whether there is a match.

their help desk to immediately prevent the hacker's ability to use the old password. In contrast, if a hacker gains access to a database and steals the employee's fingerprint records to engage in identity theft, the solution may not be quite so simple. In short, although biometrics may improve authentication, to improve data security overall it is critical that stored biometric data – a "honeypot" for identity thieves – be kept secure.