PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Data Security

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

May 4, 2011

I. INTRODUCTION

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, I am David C. Vladeck, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on data security.[1]

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has brought more than 30 law enforcement actions against businesses that allegedly failed to protect consumers' personal information appropriately, including two new cases yesterday. Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, and policy initiatives. And in July, the Commission will be hosting a forum to explore the issue of identity theft targeting children. This testimony provides an overview of the Commission's efforts and reiterates the Commission's unanimous, bipartisan support for legislation that would require companies to implement reasonable security policies and procedures and, in the appropriate circumstances, provide notification to consumers when there is a security breach.

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several laws and rules that impose obligations upon businesses that possess consumer data. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for financial institutions.[2] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[3] and imposes safe disposal obligations on entities that maintain consumer report information.[4] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.[5]

Since 2001, the Commission has used its authority under these laws to bring 34 cases against businesses that allegedly failed to protect consumers' personal information

---

[2] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[3] 15 U.S.C. § 1681e.

[4] *Id*. at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[5] 15 U.S.C. § 45(a).

appropriately.[6] Just yesterday, the Commission announced two new data security cases. The first involves Ceridian Corporation, a large payroll processing company that maintains highly-sensitive payroll information.[7] In December 2009, as a result of Ceridian's alleged failures to adequately protect its data, an intruder was able to hack into Ceridian's payroll processing

---

[6] *See Lookout Servs., Inc.*, FTC File No. 1023076 (May 3, 2011) (consent order approved for public comment); *Ceridian Corp.*, FTC File No. 1023160 (May 3, 2011) (consent order approved for public comment); *SettlementOne Credit Corp.*, FTC File No. 082 3208, *ACRAnet, Inc.*, FTC File No. 092 3088, and *Fajilan & Assocs., Inc.*, FTC File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment); *In re Rite Aid Corp.*, FTC File No. 072-3121 (July 27, 2010) (consent order)*; In re Twitter, Inc.*, FTC File No. 092-3093 (June 24, 2010) (consent order); *Dave & Buster's, Inc.*, FTC Docket No. C-4291 (May 20, 2010) (consent order); *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. Mar. 15. 2010) (stipulated order); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009) (stipulated order); *In re James B. Nutter & Co.*, FTC Docket No. C-4258 (June 12, 2009) (consent order); *United States v. Rental Research Servs.*, No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 29, 2009) (stipulated order); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008) (stipulated order); *United States v. American United Mortg.*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007) (stipulated order); *In re CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009) (consent order); *In re Genica Corp.*, FTC Docket No. C-4252 (Mar. 16, 2009) (consent order); *In re Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *In re The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *In re Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order); *In re Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In re Goal Fin'l., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *In re Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *In re Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *In re DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *In re Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *In re Nationwide Mortg. Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *In re Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In re Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *In re MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In re Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In re Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[7] *Ceridian Corp.*, File No. 1023160 (May 3, 2011) (consent order approved for public comment).

system and compromise the personal information – including Social Security numbers and financial account numbers – of approximately 28,000 employees of Ceridian's small business customers.

The second case the Commission announced today involves Lookout Services, a company that offers a web-application to assist employers in meeting federal requirements to verify their employees' eligibility to work in the United States.[8] Within this application, Lookout maintains highly-sensitive information provided by employees, including Social Security numbers, dates of birth, passport numbers, alien registration numbers, driver's license numbers, and military identification numbers. In October and December of 2009, due to the company's alleged weak authentication practices and web application vulnerabilities, an employee of a Lookout customer obtained unauthorized access to the entire Lookout customer database.

In both cases, the Commission alleged that the companies did not maintain reasonable safeguards for the highly-sensitive information they maintained. Specifically, the Commission alleged that, among other things, both companies failed to adequately assess the vulnerability of their web applications and networks to commonly known or reasonably foreseeable attacks, such as – in the case of Ceridian – "Structured Query Language" ("SQL") injection attacks and – in the case of Lookout – "predictable resource location," which enables users to easily predict patterns and manipulate the uniform resource locators ("URL") to gain access to secure web pages. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

---

[8] *Lookout Servs., Inc.*, File No. 1023076 (May 3, 2011) (consent order approved for public comment).

Similarly, earlier this year, the Commission brought actions against three credit report resellers, alleging violations of the FCRA, FTC Act, and the Safeguards Rule.[9] Due to their lack of information security policies and procedures, the respondents in these cases allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access sensitive consumer reports through an online portal. This failure enabled hackers to access more than 1,800 credit reports without authorization. As with *Ceridian* and *Lookout*, the settlements require each company, among other things, to have comprehensive information security programs in place to protect the security, confidentiality, and integrity of consumers' personal information.

B. Education

The Commission also promotes better data security practices through extensive use of consumer and business education. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[10] OnGuard Online was developed in partnership with other government agencies and the technology sector. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have recorded more than 14 million unique visits.

In addition, the Commission has engaged in wide-ranging efforts to educate consumers about identity theft, one of the harms that could result if their data is not adequately protected.

---

[9] *SettlementOne Credit Corp.*, File No. 082 3208; *ACRAnet, Inc.*, File No. 092 3088; *Fajilan and Associates, Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment).

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

For example, the FTC's identity theft primer[11] and victim recovery guide[12] are widely available in print and online. Since 2000, the Commission has distributed more than 10 million copies of the two publications and recorded over 5 million visits to the Web versions. In addition, in February 2008, the U.S. Postal Service – in cooperation with the FTC – sent copies of the Commission's identity theft consumer education materials to more than 146 million residences and businesses in the United States. Moreover, the Commission maintains a telephone hotline and dedicated website to assist identity theft victims and collect their complaints, through which approximately 20,000 consumers contact the FTC every week.

The Commission recognizes that its consumer education efforts can be even more effective if it partners with local businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. For example, the Commission has launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups. The Commission has developed a second consumer education toolkit with everything an organization needs to host a "Protect Your Identity Day." Since the campaign launch in 2006, the FTC has distributed nearly 110,000 consumer education kits and over 100,000 Protect Your Identity Day kits.

The Commission directs its outreach to businesses as well. The FTC widely disseminates

---

[11] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[12] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

its business guide on data security, along with an online tutorial based on the guide.[13] These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. The Commission also has released articles directed towards a non-legal audience regarding basic data security issues for businesses,[14] which have been reprinted in newsletters of local Chambers of Commerce and other business organizations.

The FTC also creates business educational materials on specific topics, often to address emerging issues. For example, last year, the Commission sent letters notifying several dozen public and private entities – including businesses, schools, and local governments – that customer information from their computers had been made available on peer-to-peer ("P2P") file-sharing networks.[15] The purpose of this campaign was to educate businesses and other entities about the risks associated with P2P file-sharing programs and their obligations to protect consumer and employee information from these risks. As part of this initiative, the Commission developed a new business education brochure – *Peer-to-Peer File Sharing: A Guide for Business*.[16] More recently, we issued a guide to businesses about how to properly secure and dispose of information on digital copiers, after news reports called attention to the vast amounts of consumer data remaining on such copiers being prepared for re-sale.[17]

---

[13] *See* www.ftc.gov/infosecurity.

[14] *See* http://business.ftc.gov/privacy-and-security.

[15] *See* FTC Press Release, *Widespread Data Breaches Uncovered by FTC Probe* (Feb. 22. 2010), *available at* www.ftc.gov/opa/2010/02/p2palert.shtm.

[16] *See* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[17] *See* http://www.cbsnews.com/video/watch/?id=6412572n.

C. Policy

The Commission's efforts to promote data security also include policy initiatives. This testimony describes two such initiatives – the recent Privacy Roundtables and the accompanying preliminary staff report as well as the upcoming forum on child identity theft.

1. Privacy Roundtables and Preliminary Staff Report

In December 2009, February 2010, and March 2010, the FTC convened three public roundtables to explore issues surrounding consumer privacy.[18] Panelists at the roundtables repeatedly noted the importance of data security as an important component of protecting consumers' privacy. Many participants stated that companies should incorporate data security into their everyday business practices, particularly in today's technological age. For example, participants noted the increasing importance of data security in a world where cloud computing enables companies to collect and store vast amounts of data at little cost.[19]

Based on these roundtable discussions, staff issued a preliminary privacy report in December 2010,[20] which proposed and solicited comment on a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy

---

[18] *See generally* FTC Exploring Privacy web page, www.ftc.gov/bcp/workshops/privacyroundtables.

[19] *See, e.g.*, Privacy Roundtable, Transcript of January 28, 2010, at 182, Remarks of Harriet Pearson, IBM (noting the importance of data security as an issue for new computing models, including cloud computing).

[20] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively.

protection. The proposed framework incorporates the principles of privacy by design, simplifying the presentation of privacy choices for consumers, and improving transparency of privacy practices for consumers. In the context of data security, the principle of "privacy by design" is especially important. Indeed, consumers should not be expected to understand and evaluate the technical details of a company's data security plan; rather, reasonable security should be incorporated into the company's business practices.

As the staff report notes, privacy by design includes several substantive components related to data security. First, companies that maintain information about consumers should employ reasonable safeguards – including physical, technical, and administrative safeguards – to protect that information. The level of security required depends on the sensitivity of the data, the size and nature of a company's business operations, and the types of risks a company faces. Second, companies should collect information only if they have a legitimate business need for it. Because the collection and maintenance of large amounts of data increases the risk of unauthorized access to the data and the potential harm that could result, reasonable data collection practices help support sound data security practices. Third, businesses should retain data only as long as necessary to fulfill the business purposes for which it was collected and should promptly and securely dispose of data for which they no longer have a business need.[21]

---

[21] *See, e.g.*, Privacy Roundtable, Transcript of January 28, 2010, at 310, Remarks of Lee Tien, Electronic Frontier Foundation ("And having the opposite of data retention, data deletion as a policy, as a practice is something that, you know, really doesn't require any fancy new tools. It is just something that people could do, would be very cheap, and would mitigate a lot of privacy problems."); Privacy Roundtable, Transcript of March 17, 2010, at 216, Remarks of Pam Dixon (supporting clear and specific data retention and use guidelines). The Commission has long supported this principle in its data security cases. Indeed, at least three of the Commission's data security cases – against DSW Shoe Warehouse, BJ's Wholesale Club, and Card Systems – involved allegations that companies violated data security laws by retaining magnetic stripe information from customer credit cards much longer than they had a business

While old data may not be valuable to a particular company, it can be highly valuable to an identity thief.

In addition to these substantive principles, the staff report recommends that companies implement and enforce privacy procedures – including appropriate data security – throughout their organizations. This includes assigning personnel to oversee such issues, training employees, and assessing and addressing risks to privacy and security.

2. Child Identity Theft Forum

Along with periodically conducting policy reviews of privacy and security issues generally, the Commission also hosts workshops to study and publicize more specific issues. One such issue that has been in the news recently is identity theft targeting children.[22] For a variety of reasons – including poor safeguards for protecting children's data – identity thieves can get access to children's Social Security numbers. These criminals may deliberately use a child's Social Security number, or fabricate a Social Security number that coincidentally has been assigned to a child, in order to obtain employment, apply for government benefits, open new accounts, or apply for car loans, or even mortgages. Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks

---

need to do so. Moreover, in disposing of certain sensitive information, such as credit reports, companies must do so securely. *See* FTC Disposal of Consumer Report Information and Records Rule, 16 C.F.R. § 682 (2005).

[22] *See e.g.*, Richard Power, Carnegie Mellon Cylab, Child Identity Theft, New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers (2011), *available at* http://www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html; Children's Advocacy Institute, The Fleecing of Foster Children: How We Confiscate Their Assets and Undermine Their Financial Security (2011), *available at* http://www.caichildlaw.org/Misc/Fleecing_Report_Final_HR.pdf.

employment, or applies for student and car loans.

To address the challenges raised by child identity theft, Commission staff, along with the Department of Justice's Office of Victims of Crime, will host a forum on July 12, 2011. Participants will include educators, child advocates, representatives of various governmental agencies, and the private sector. The forum will include a discussion on how to improve the security of children's data in various contexts, including within the education system as well as the foster care system, where children may be particularly susceptible to identity theft. The goal of the forum is to develop ways to effectively advise parents on how to avoid child identity theft, how to protect children's personal data, and how to help parents and young adults who were victimized as children recover from the crime.

III. DATA SECURITY LEGISLATION

Finally, the Commission reiterates its support for federal legislation that would (1) impose data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[23] Companies' implementation of reasonable security is important for protecting consumers' data from identity theft and other harm. And if a breach occurs, prompt notification to consumers in appropriate circumstances can mitigate any such harm. For example, in the case of a breach of Social Security numbers, notified consumers can request that fraud alerts be placed in their credit

[23] *See e.g.*, Prepared Statement of the Federal Trade Commission, "Protecting Social Security Numbers From Identity Theft," Before the Subcommittee on Social Security of the House Committee on Ways and Means, 112th Cong., April 13, 2011, *available at* http://ftc.gov/os/testimony/110411ssn-idtheft.pdf (citing the Commission's support for data security and breach notification standards); FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* www.ftc.gov/os/2008/12/P075414ssnreport.pdf; and President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on the topic of data security. We remain committed to promoting data security and look forward to continuing to work with you on this important issue.