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.

June 15, 2011

[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 other Commissioner.

[2] In addition to these data security cases, in the last fifteen years, the FTC has brought numerous cases to protect consumer privacy including 64 cases against companies for improperly calling consumers on the Do Not Call registry; 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA"); 96 spam cases; 15 spyware cases; and 16

bipartisan support for legislation that would require companies to implement reasonable data security policies and procedures and, in the appropriate circumstances, provide notification to consumers when there is a security breach.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several laws and rules that impose obligations on 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,[3] and 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, 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 data security claims 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

---

[3] 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.

[4] 15 U.S.C. §§ 1681e, 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[5] 15 U.S.C. § 45(a).

appropriately.[6] As noted above, just today, the Commission announced that it had given final approval to consent orders in data security cases involving Ceridian Corporation and Lookout

[6] *See Lookout Servs.,Inc.*, File No. 1023076 (June 15, 2011) (consent order); *Ceridian Corp.*, File No. 1023160 (June 15, 2011) (consent order); *SettlementOne Credit Corp.,* File No. 082 3208, *ACRAnet, Inc.*, File No. 092 3088, and *Fajilan & Assocs., Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment); *Rite Aid Corp.*, File No. 072-3121 (July 27, 2010) (consent order)*; Twitter, Inc.*, 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); *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); *CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009) (consent order); *Genica Corp.*, FTC Docket No. C-4252 (Mar. 16, 2009) (consent order); *Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order); *Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *Goal Fin'l., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *DSW, Inc*., FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *Nationwide Mortg. Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[7] *Ceridian Corp.*, File No. 1023160 (June 15, 2011) (consent order).

numbers – of approximately 28,000 employees of Ceridian's small business customers.

Lookout Services 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. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

In addition, earlier this year, the Commission brought actions against three credit report resellers, alleging violations of the FCRA, the FTC Act, and the Safeguards Rule.[9] Due to their lack of information security policies and procedures, the respondents allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access

---

[8] *Lookout Servs., Inc.*, File No. 1023076 (June 15, 2011) (consent order).

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

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 consumers' personal information.

B. Education

The Commission also promotes better data security practices through extensive 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[11] 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. For example, the FTC's identity theft primer[12] and victim recovery guide[13] 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

---

[10] *See* http://www.onguardonline.gov.

[11] *See* http://www.alertaenlinea.gov.

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

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

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 er/s onsta

[14] *See* www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt06.pdf.

[15] *See* http://www.ftc.gov/infosecurity.

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

companies' obligations to protect consumer and employee information from these risks[17] and how to properly secure and dispose of information on digital copiers.[18]

C. Policy

The Commission also undertakes wide-ranging policy initiatives to promote data security. This testimony describes two such initiatives – the recent Privacy Roundtables and accompanying preliminary staff report as well as an 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.[19] 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.[20]

Based on these roundtable discussions, staff issued a preliminary privacy report in

---

[17] *See Peer-to-Peer File Sharing: A Guide for Business, available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[18] *See* http://business.ftc.gov/documents/bus43-copier-data-security.

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

[20] *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).

December 2010,[21] which proposed and solicited comment on a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy protection. The proposed framework incorporates the principles of privacy by design, simplified privacy choices for consumers, and improved 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 only information for which they have a legitimate business need. 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 are a critical component of sound data security. 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] *See 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 Appendices D and E, respectively.

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 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 mortgages. Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks employment or applies for a loan.

To address these challenges, Commission staff, along with the Department of Justice's

---

[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.

[23] *See* http://www.ftc.gov/bcp/workshops/stolenfutures.

[24] *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* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; and President's

harm.[25] For example, in the case of a breach of Social Security numbers, notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. The Commission appreciates that the discussion draft accomplishes these goals.

The Commission further appreciates the discussion draft's inclusion of several specific elements. First, the discussion draft provides the agency with rulemaking authority in several areas, and authorizes it to use the standard notice and comment procedures required by the Administrative Procedure Act in lieu of the current rulemaking procedures prescribed by Section 18 of the FTC Act (often referred to as "Magnuson-Moss" rulemaking). The Commission supports this provision, as effective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner. Second, the Commission supports the inclusion of a provision authorizing the agency to obtain civil penalties for violations.[26] Civil

---

[25] Indeed, various states have already passed data breach notification laws that require companies to notify affected consumers in the event of a data breach. These laws have increased public awareness of data security issues and related harms, as well as data security issues at specific companies. *See, e.g.*, Federal Trade Commission Report, *Security in Numbers: SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, *Security Breach Notification Laws: Views from Chief Security Officers* (Dec. 2007), *available at* http://www.law.berkeley.edu/files/cso_study.pdf. Breach notification at the federal level would extend notification nationwide and accomplish similar goals.

[26] *See, e.g.*, Prepared Statement of the Federal Trade Commission Before Subcomm. on Consumer Protection, Product Safety & Insurance of the S. Comm. on Commerce, Science & Transportation, 111th Cong. (Sep. 22, 2010), *available at* http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf; Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007) *available at* http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007), *available at* http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCo

penalties are particularly important in areas such as data security, where the Commission's traditional equitable remedies – including consumer restitution and disgorgement – may be impractical or not optimally effective. Third, the Commission continues to support legislative provisions that would authorize the Commission to sue non-profit entities for data security violations, and appreciates the draft proposal's inclusion of such provisions.[27] Finally, the Commission notes that the recent Commission staff report takes the same position as the discussion draft that data minimization is an important component of data security.

The Commission is ready to work with this Committee as it develops and considers data security legislation.

IV. CONCLUSION

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

---

mpetitionProgramsTestimonySenate04102007.pdf; *see also* FTC Report, *Recommendations on Social Security Number Use in the Private Sector* (Dec. 2008), *available at* http://www.ftc.gov/opa/2008/12/ssnreport.shtm.

[27] The Commission has authority to sue sham non-profits under existing law. *See, e.g.*, http://www.ftc.gov/opa/2009/05/charityfraud.shtm.