

**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

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

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

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 primer¹¹ and victim recovery guide¹² 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

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>.

¹⁸ *See generally* FTC Exploring Privacy web page,

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).

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](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](http://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](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.