PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Data Security

Before the

COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, & INSURANCE

UNITED STATES SENATE

Washington, D.C.

September 22, 2010

I. INTRODUCTION

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, I am Maneesha Mithal, Associate Direc

[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.

consumer data. The FTC enforces several laws and rules imposing data security requirements. 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. In addition, the Commission enforces the FTC Act'sl.t0000 TD(ssion er

[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).

[6] *See In re Rite Aid Corp.*, FTC File No. 072-3121 (July 27, 2010) (consent approved subject to public comment)*; In re Twitter, Inc.*, FTC File No. 092-3093 (June 24, 2010) (consent approved subject to public comment); *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 & Company*, FTC Docket No. C-4258 (June 12,

sl tf TD(ve)Ti11.2800 0.0000 Td(is)Ti15.7200 0.0000 To(ie)Ti8.6400 0.0000 TD dD(r i)Ti10.3200 0.0000hang

in actions against Microsoft,[8] Petco,[9] Tower Records,[10] Life is good,[11] and Premier Capital Lending,[12] the FTC challenged claims on the companies' websites that each had strong security procedures in place to protect consumer information. In these cases the FTC alleged that, contrary to their claims, the companies did not employ many of the most basic security measures.

Second, businesses should protect against well-known, common technology threats. In a number of cases, the Commission has alleged that companies failed to protect their customer information from a simple and well-known type of attack – an SQL injection – designed to install hacker tools on the companies' computer networks.[13] Most recently, the Commission announced its first data security case against socia

---

[8] *In re Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[9] *In re Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order).

[10] *In re MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order).

[11] *In re Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order).

[12] *In re Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order).

[13] *See, e.g., In re Genica Corp.*, FTC Docket No. C-4252 (Mar. 16, 2009) (consent order); *In re Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order).

[14] *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006) (stipulated order).

[15] *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Oct. 14, 2009) (stipulated order).

transaction, when the companies no longer had a business need for the information. The Commission further alleged that, as a result, when thieves gained access to the companies' systems, they were able to obtain hundreds of thousands – in some cases millions – of credit card numbers and security codes.

Finally, businesses should dispose of sensitive consumer information properly. The Commission's most recent data security case against Rite Aid illustrates this principle.[20] In that case, the Commission alleged that Rite Aid failed to implement reasonable and appropriate procedures for handling personal information about customers and job applicants, particularly with respect to its practices for disposing of such information. The FTC's action followed media reports that Rite Aid pharmacies across the country were throwing pharmacy labels and employment applications into open dumpsters. The FTC coordinated its investigation and settlement with the Department of Health and Human Services ("HHS"), which investigated Rite Aid's handling of health information under the Health Insurance Portability and Accountability Act. Under its settlement order with the FTC, Rite Aid agreed to establish a comprehensive information security program and obtain biennial audits of this program for the next 20 years. HHS announced a separate agreement with Rite Aid in which the company agreed to pay a $1 million fine.[21]

---

[20] *See In re Rite Aid Corp.*, FTC File No. 072-3121 (July 27, 2010) (consent approved subject to public comment).

[21] The FTC brought a similar case against CVS Caremark alleging that the company failed to properly dispose of sensitive customer and employee information. *See In re CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009) (consent order). The FTC also has brought cases involving mortgage companies' alleged improper disposal of sensitive customer financial information. *See FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 29, 2009) (stipulated order); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007) (stipulated order).

The Commission recog

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 its business guide on data security, along with an online tutorial based on the guide.[26] These resources provide

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

[30] *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).

[31] *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 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).

[32] This recommendation is consistent with prior Commission recommendations. *See* Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 109th Cong. (Jun. 16, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf; Prepared Statement of the F

consumers may never have anticipated when it was collected. Given the invisibility of these practices, consumers are unaware of and thus unable to control them. If information from data brokers is inaccurate – for example, if a data broker provides inaccurate information to a business for purposes of verifying a job applicant's identity – consumers can be harmed by the lack of access to, and ability to correct, that information. The Commission believes that S. 3742's provisions on access can help to alleviate these concerns.

At the same time, the Commission acknowledges that providing access can be costly, and that the right to suppress data rather than correct it may be sufficient in certain circumstances – if the data is used, for example, to make marketing decisions. The proposed rulemaking authority for the Commission will allow it to scale the legislative provisions on access, weighing its costs and benefits in particular circumstances.

Finally, the Commission supports the legislation's robust enforcement provisions, which would (1) give the FTC the authority to obtain civil penalties for violations[34] and (2) give state

---

[34] *See supra* at n. 32.; *see also* 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/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf. These recommendations also were made in an April 2007 report released by the President's Identity Theft Task Force, which was co-chaired by the Attorney General and the FTC Chairman, as well as in a report on Social Security numbers released in December 2008. *See* The President's Identity Theft Task Force Report, Sep. 2008, *available at* http://idtheft.gov/reports/IDTReport2008.pdf; 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.

pleased to work with this Committee to address these issues.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on the topic of data security. We