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 Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on data security and to provide the Commission's thoughts on legislation in this area.[1]

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. 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. The Commission's testimony begins by describing these initiatives. It also sets forth the Commission's support of the proposed data security legislation introduced by Chairman Pryor and Chairman Rockefeller along with certain recommendations on the legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security through law enforcement, the Commission brings enforcement actions against businesses that fail to implement reasonable security measures to protect

[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.[4] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices[5] 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.

Since 2001, the Commission has used its authority under these laws to bring 29 cases against businesses that allegedly failed to protect consumers' personal information appropriately.[6] These cases illustrate several general principles.

---

[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,

First, businesses that make claims about data security should be sure that they are accurate. The Commission has brought several cases against companies that allegedly misrepresented their own security procedures. A recent example is our action against LifeLock, in which the Commission challenged the company's claims that it took stringent security measures to protect consumer data and that it encrypted such data.[7] The FTC charged that Lifelock's data was in fact not encrypted and that its data system was vulnerable and could have been exploited by identity thieves or others seeking access to customer information. Similarly,

---

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 Mortgage*, 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., 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 Mortgage 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 Mortgage 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] *FTC v. LifeLock, Inc.,* No. 2:10-cv-00530-NVW (D. Ariz. Mar. 15. 2010) (stipulated order).

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 social networking company Twitter, alleging that it failed to implement simple measures to counteract basic technology threats. For example, the Commission alleged that the company failed to require strong administrative passwords and to suspend passwords after a reasonable number of log-in attempts, and further alleged that this failure resulted in a hacker being able to use a simple automated password-guessing tool to gain administrative control of Twitter.

---

[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).

Third, businesses must know with whom they are sharing customers' sensitive information. One of the Commission's most well-known security cases involved ChoicePoint, a data broker that sold 160,000 consumer files to identity thieves posing as clients. In its complaint, the Commission alleged that ChoicePoint lacked reasonable procedures to verify the legitimacy of its customers.[14] In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for alleged violations of the FCRA and $5 million in consumer redress for identity theft victims. The company also agreed to undertake substantial new data security measures. Last year, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay monetary relief in the amount of $275,000.[15]

Fourth, businesses should not retain sensitive consumer information that they do not need. In cases against BJ's Warehouse,[16] DSW Shoe Warehouse,[17] and CardSystems Solutions,[18] for example, the Commission alleged that the companies stored unencrypted, full magnetic stripe information on payment cards[19] unnecessarily – long after the time of the

---

[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).

[16] *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sep. 20, 2005) (consent order).

[17] *In re DSW, Inc*., FTC Docket No. C-4157 (Mar. 7, 2006) (consent order).

[18] *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sep. 5, 2006) (consent order).

[19] Magnetic stripe information is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process.

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).

Some of the Commission's data security actions described above involve unfair or deceptive practices under the FTC Act, while others involve the GLB Act and related Safeguards Rule or the FCRA. Although the Commission brings its cases under different laws, all of its cases stand for the principle that companies must maintain reasonable and appropriate measures to protect sensitive consumer information.[22]

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.[23] 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 attracted nearly 12 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[24] and victim recovery guide[25] are widely available

---

[22] The Commission recognizes that what is "reasonable" under these laws will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. The principle recognizes that there cannot be "perfect" security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. At the same time, companies that put consumer data at risk can be liable even in the absence of a known breach.

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

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

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

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 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.

---

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

The Commission also has released articles for businesses relating to basic data security issues for a non-legal audience,[27] which have been reprinted in newsletters for 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, earlier this 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. 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*.[28]

C. Policy

The Commission's efforts to promote data security also include policy initiatives. Over the past several months, the FTC has convened three public roundtables to explore consumer privacy.[29] Panelists at the roundtables repeatedly noted the importance of data security in protecting 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

---

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

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

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

enables companies to collect and store vast amounts of data at little cost.[30] In addition, participants noted that the falling cost of data storage enables companies to retain data for long periods of time, again at little cost. Even if old data is not valuable to a particular company, it could be highly valuable to an identity thief. This is one of the reasons why businesses should promptly and securely dispose of data for which they no longer have a business need.[31]

The Commission staff expect to issue a report later this year seeking comment on these and other topics. Among other things, the report will encourage companies to incorporate sound data security and data retention practices into their business models in a reasonable and cost-effective way.

III. LEGISLATIVE RECOMMENDATIONS

The Commission appreciates the opportunity to comment on the proposed legislation introduced by Chairman Pryor and Chairman Rockefeller. The Commission supports the goal of improving the security of consumer data. The proposed legislation contains several important

---

[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).

components.

First, it would require a broad array of companies to implement reasonable security policies and procedures, including both commercial and nonprofit entities. Problems with data security and breaches affect businesses and nonprofit organizations alike. Requiring reasonable security policies and procedures of this broad array of entities is a goal that the Commission strongly supports, as illustrated by its robust data security enforcement program described above.

Second, it would require covered companies to notify consumers when there is a security breach. The Commission believes that notification in appropriate circumstances can be beneficial.[32] Indeed, various states have already passed data breach notification laws which require companies to notify affected consumers in the event of a data breach. These laws have further increased public awareness of data security issues and related harms, as well as data security issues at specific companies.[33] Breach notification at the federal level would extend notification nationwide and accomplish similar goals.

Third, the Commission learned from its privacy roundtables that data brokers often gather consumer data from a variety of sources, combine it, and use it for purposes that

---

[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 Federal Trade Commission Before the S. Comm. on Commerce, Trade, and Consumer Protection, 111th Cong. (May 5, 2009), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.

[33] *See, e.g.,* 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; Federal Trade Commission Report, *Security in Numbers: SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf.

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.

attorneys general concurrent enforcement authority.[35]

The Commission has three main recommendations for the legislation at this time. First, it recommends that the provision requiring notification in the event of an information security breach not be limited to entities that possess data in *electronic* form, because the breach of sensitive data stored in paper format can be just as harmful to consumers.[36] Second, as the proposed legislation is currently drafted, its requirements do not apply to telecommunications common carriers, many of which maintain significant quantities of highly personal information. The Commission believes that the legislation should cover these entities and that the Commission should have authority to enforce the legislation as to them. Third, the bill requires the Commission to establish a process for small businesses to request a waiver from having to provide free credit reports or credit monitoring to consumers following a breach. The Commission believes that such a business-by-business waiver process would be resource intensive for both the Commission and small businesses. Instead, the Commission suggests that the bill grant it rulemaking authority to determine circumstances under which the provision of free credit reports or credit monitoring may not be warranted.[37] The Commission would be

---

[35] *See* The President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan," (Apr. 2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[36] According to one survey, a significant number of breaches involve paper documents. *See* Ponemon Institute, *Security of Paper Documents in the Workplace* (Oct. 2008), *available at* http://www.ponemon.org/data-security. In addition, the Commission has brought several data security cases involving improper disposal of paper documents, including the Rite Aid case discussed above. The facts of these cases illustrate how breaches of sensitive data stored in paper format may create a serious potential for consumer harm.

[37] The Commission notes that, as drafted, S. 3742 would preempt state law. In light of this, the Commission encourages this Committee to closely examine relevant state law, such as state data breach notification laws, to ensure that any federal legislation in this area continues to provide consumers with a high level of protection.

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 remain committed to promoting data security and look forward to continuing to work with you on this important issue.