PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Protecting Personal Consumer Information from Cyber Attacks and Data Breaches

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

March 26, 2014

I. INTRODUCTION

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, I am Edith Ramirez, Chairwoman of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security.

Under your leadership, Chairman Rockefeller, this Committee has led critical efforts in Congress to protect consumers' privacy and data security. Throughout your tenure, the Committee has focused on a wide range of privacy and security concerns facing consumers in this increasingly interconnected economy. From the recent examination of the data broker industry and its impact on consumers;[2] to protecting our children's privacy as technology changes;[3] to promoting consumers' choices about online privacy;[4] to proposing baseline data security requirements for industry,[5] you and members of the Committee have shared the same

---

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] *See* Office of Oversight & Investigations Majority Staff Report, Senate Commerce Committee, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Dec. 18, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a.

[3] *See, e.g.*, Press Release, *Rockefeller Says Modernized COPPA Rule Will Better Protect Children Online*, Dec. 19, 2012, *available at* http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=1a0ac4aa-bfbe-493e-a877-16035146562d&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d&MonthDisplay=12&YearDisplay=2012.

[4] *See, e.g.*, Hearing Before the Committee on Commerce, Science, and Transportation, U.S. Senate, *A Status Update on the Development of Voluntary Do-Not-Track Standards*, Apr. 24, 2013, *available at* http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=1cf8fb1a-fb0b-4bf1-958b-1ea3c443a73c&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=4&YearDisplay=2013.

[5] *See, e.g.*, Press Release, *The Data Security & Breach Notification Act*, Jan. 30, 2014, *available at* http://www.commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord_id=40e0ad58-866a-41ea-bf00-750c17e1ee3a.

goals as the Federal Trade Commission: to protect consumer privacy and promote data security in the private sector. The FTC thanks you for your leadership.

As this Committee is well aware, consumers' data is at risk. Recent publicly announced data breaches[6] remind us that hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harm to consumers as well as businesses. These threats affect more than payment card data; breaches reported in recent years have also compromised Social Security numbers, account passwords, health data, information about children, and other types of personal information.

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, identity theft, and other harm, along with a potential loss of consumer confidence in the marketplace. As one example, the Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012.[7]

As the nation's leading privacy enforcement agency, the Commission has undertaken substantial efforts for over a decade to promote data security and privacy in the private sector through civil law enforcement, education, and policy initiatives. The Commission is here today to reiterate its longstanding, bipartisan call for enactment of a strong federal data security and

---

[6] *See* Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. Times, Jan. 10, 2014, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html (discussing recently-announced breaches involving payment card information by Target and Neiman Marcus); Nicole Perlroth, *Michaels Stores Is Investigating Data Breach*, N.Y. Times, Jan. 25, 2014, *available at* http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html (announcement of potential security breach involving payment card information).

[7] *See* Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

breach notification law. Never has the need for legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress must act. This testimony provides an overview of the Commission's data security efforts, and restates the FTC's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

The Commission enforces several statutes and rules that impose obligations upon businesses to protect consumer data. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for non-bank financial institutions.[8] 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,[9] and imposes safe disposal obligations on entities that maintain consumer report information.[10] The Children's Online Privacy Protection Act (COPPA) requires reasonable security for children's information collected online.[11] Reasonableness is the foundation of the data security provisions of each of these laws.

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[12] A company acts deceptively if it makes materially misleading statements or omissions.[13] Using its deception authority, the Commission has settled

---

[8] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

[9] 15 U.S.C. § 1681e.

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

[11] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[12] 15 U.S.C. § 45(a).

[13] *See* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

more than 30 matters challenging companies' express and implied claims about the security they provide for consumers' personal data. Further, a company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[14] The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[15]

The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission's 50 settlements with businesses that it charged with failing to provide reasonable protections for consumers' personal information have halted harmful data security practices; required companies to accord strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.[16] And they have addressed the risks to a wide variety of consumer data, such as Social Security numbers, health data, data about children, credit card information, bank account information, usernames, and passwords, in a broad range of sectors and platforms.

In each of these cases, the Commission has examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. Through these settlements, the Commission has made clear that reasonable and appropriate security is a

---

[14] *See* Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement").

[15] Some of the Commission's data security settlements allege both deception and unfairness, as well as allegations under statutes such as the FCRA, GLB Act, and COPPA.

[16] *See* Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law.

In its most recent case, the FTC entered into a settlement with GMR Transcription Services, Inc., a company that provides audio file transcription services for its clients – which includes health care providers.[17] According to the complaint, GMR relies on service providers and independent typists to perform this work, and conducts its business primarily over the Internet by exchanging audio files and transcripts with customers and typists by loading them on a file server. As a result of GMR's alleged failure to implement reasonable and appropriate security measures or to ensure its service providers also implemented reasonable and appropriate security, at least 15,000 files containing sensitive personal information – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet. The Commission's order prohibits GMR from making misrepresentations about privacy and security, and requires the company to implement a comprehensive information security program and undergo independent audits for the next 20 years.

The FTC also recently announced a case against TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.[18] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening, by anyone with

---

[17] *GMR Transcription Servs., Inc.*, Matter No. 112-3120 (F.T.C. Dec. 16, 2013) (proposed consent order), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

[18] *TRENDnet, Inc.*, No. C-4426(F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next two years.

The FTC also has brought a number of cases alleging that unreasonable security practices allowed hackers to gain access to consumers' credit and debit card information, leading to many millions of dollars of fraud loss.[19] The Commission's settlement with TJX provides a good example of the FTC's examination of reasonableness in the data security context.[20] According to the complaint, TJX engaged in a number of practices that, taken together, failed to reasonably protect consumer information. Among other things, it (1) failed to implement measures to limit wireless access to its stores, allowing a hacker to connect wirelessly to its networks without authorization; (2) did not require network administrators to use strong passwords; (3) failed to use a firewall or otherwise limit access to the Internet on networks processing cardholder data; and (4) lacked procedures to detect and prevent unauthorized access, such as by updating antivirus software and responding on security warnings and intrusion alerts. As a result, a hacker obtained tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. As this matter illustrates, the FTC's approach to reasonableness is process-based rather than a checklist of

---

[19] *See, e.g.*, *Dave & Buster's, Inc.*, No. C-4291 (F.T.C. May 20, 2010) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; *DSW, Inc.*, No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; *BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

[20] *The TJX Cos., Inc.*, No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter.

specific technologies or tools. The Commission looks to see whether companies have a general framework in place to develop, implement, and maintain appropriate safeguards that is reasonable and appropriate in light of the sensitivity and volume of the data it holds, the size and complexity of its data operations, and the cost of available tools.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security. For example, the FTC hosts workshops on business practices and technologies affecting consumer data. The FTC is in the midst of hosting its Spring Privacy Series to examine the privacy implications of a number of new technologies in the marketplace.[21] The first seminar, held in February, included a panel of industry, technical experts, and privacy advocates and examined the privacy and security implications of mobile device tracking, where retailers and other companies rely on technology that can reveal information about consumers' visits to and movements within a location.[22]

In November, the FTC held a workshop on the phenomenon known as the "Internet of Things" – *i.e.*, Internet-connected refrigerators, thermostats, cars, and other products and services that can communicate with each other and/or consumers.[23] The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity in everyday devices, in areas as diverse as smart homes,

---

[21] Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues*, Dec. 2, 2013, *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

[22] *See* Spring Privacy Series, *Mobile Device Tracking*, Feb. 19, 2014, *available at* http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.

[23] FTC Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), *available at* http://www.ftc.gov/bcp/workshops/internet-of-things/.

connected health and fitness devices, and connected cars. Commission staff is developing a report on privacy and security issues raised at the workshop and in the public comments.

And last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[24] As the use of mobile technology increases at a rapid rate and consumers take advantage of the technology's benefits in large numbers, it is important to address threats that exist today as well as those that may emerge in the future. The forum brought together technology researchers, industry members and academics to explore the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from potential security threats.

C. Consumer Education and Business Guidance

The Commission is also committed to promoting better data security practices through consumer education and business guidance. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[25] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[26] average more than 2.2 million unique visits per year. Also, for consumers who may have been affected by the recent Target and other breaches, the FTC posted information online about steps they should take to protect themselves.[27]

---

[24] FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), *available at* http://www.ftc.gov/bcp/workshops/mobile-security/.

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

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

[27] *See* Nicole Vincent Fleming, *An Unfortunate Fact About Shopping*, FTC Consumer Blog, http://www.consumer.ftc.gov/blog/unfortunate-fact-about-shopping (Jan. 27, 2014); Nicole Vincent Fleming, *Are you affected by the recent Target hack?*, FTC Consumer Blog, https://www.consumer.ftc.gov/blog/are-you-affected-recent-target-hack. In addition to these materials posted in response to recent breaches, the FTC has long published a victim recovery guide and other resources to explain the immediate steps identity theft victims should take to address the crime; how to

The Commission directs its outreach to businesses as well to provide education about applicable legal requirements and reasonable security practices. For example, the FTC widely disseminates its business guide on data security,[28] along with an online tutorial based on the guide.[29] These resources are designed to provide a variety of businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. First, companies should know what consumer information they have and what personnel or third parties have, or could have, access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the information they collect and retain based on their legitimate business needs, so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing protections in certain key areas – physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should properly dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.

The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.[30] For example, because mobile applications ("apps") and devices often rely on consumer data, the FTC has developed specific security

---

obtain a free credit report and correct fraudulent information in credit reports; how to file a police report; and how to protect their personal information. *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[28] *See Protecting Personal Information: A Guide for Business, available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

[29] *See Protecting Personal Information: A Guide for Business (Interactive Tutorial), available at* http://business.ftc.gov/multimedia/videos/protecting-personal-information.

[30] *See generally* http://www.business.ftc.gov/privacy-and-security/data-security.

guidance for mobile app developers as they create, release, and monitor their apps.[31] The FTC also creates business educational materials on specific topics – such as the risks associated with peer-to-peer ("P2P") file-sharing programs and companies' obligations to protect consumer and employee information from these risks[32] and how to properly secure and dispose of information on digital copiers.[33]

III. DATA SECURITY LEGISLATION

The FTC supports federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[34] Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Where breaches occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data. For example, in the case of a breach of Social Security numbers, notifying

---

[31] *See Mobile App Developers: Start with Security* (Feb. 2013), *available at*http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[32] *See Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

[33] *See Copier Data Security: A Guide for Business* (Nov. 2010), *available at* http://business.ftc.gov/documents/bus43-copier-data-security.

[34] *See, e.g.*, Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf; Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf.

consumers will enable them to 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. And although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected.

Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking authority under the Administrative Procedure Act. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA.[35] To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits[36] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[37]

Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC in implementing the legislation to respond to changes in technology. For example, whereas a decade ago it would be incredibly difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. And, as the growing problem of child identity theft has brought to light in recent years, a child's Social Security number alone can be used in combination with another

---

[35] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(*l*).

[36] Non-profits are generally outside the FTC's jurisdiction. 15 U.S.C. §§ 44 & 45(a).

[37] A substantial number of reported breaches have involved non-profit universities and health systems. *See* Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities), *available at* http://www.privacyrights.org/data-breach/new.

person's information, such as name or date of birth, in order to commit identity theft.[38] Rulemaking authority would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumer data and we look forward to continuing to work with the Committee and Congress on this critical issue.

[38] FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft* (July 12, 2011), *available at* http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft.