PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Protecting Consumer Information: Can Data Breaches Be Prevented?

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

February 5, 2014

I. INTRODUCTION

Chairman Terry, Ranking Member Schakowsky, and members of the Subcommittee, 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.

We live in an increasingly connected world, and information is the new currency. Businesses in this data-driven economy are collecting more personal information about consumers than ever before, and storing and transmitting across their own systems as well as the Internet. But, as recent publicly announced data breaches remind us,[2] these vast systems of data are susceptible to being compromised. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harms to consumers as well as businesses.

All of this takes place against the background of the threat of identity theft, a pernicious crime that harms both consumers and financial institutions. 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.[3]

As the nation's leading privacy enforcement agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has settled 50 law

---

[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* 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 (discussing Michaels Stores' announcement of potential security breach involving payment card information).

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

enforcement actions against businesses that we alleged failed to protect consumers' personal information appropriately. 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, along with a potential loss of consumer confidence in particular business sectors or entities, payment methods, or types of transactions. Accordingly, the Commission has undertaken substantial efforts for over a decade to promote data security in the private sector through civil law enforcement, education, policy initiatives, and recommendations to Congress to enact legislation in this area. The FTC has also worked with the Department of Justice and criminal investigative agencies, as well as state Attorneys General, to coordinate efforts and leverage government resources more effectively.

The Commission is here today to reiterate its longstanding bipartisan call for enactment of a strong federal data security and 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 needs to act. This testimony provides an overview of the Commission's efforts and restates the Commission's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several statutes and rules that impose obligations upon businesses that collect and maintain 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.[4] The Fair Credit

[4] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

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,[5] and imposes safe disposal obligations on entities that maintain consumer report information.[6] The Children's Online Privacy Protection Act ("COPPA") requires reasonable security for children's information collected online.[7]

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[8] If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5.[9] Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims that they provide reasonable security for consumers' personal data when, the Commission charged, the companies failed to employ available, cost-effective security measures to minimize or reduce data risks.

Further, if a company's 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, those practices can be found to be unfair and violate Section 5.[10] Congress expressly codified these criteria in Section 5.[11] The

---

[5] 15 U.S.C. § 1681e.

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

[7] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[8] 15 U.S.C. § 45(a).

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

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

[11] 15 U.S.C. § 5(n).

Commission has settled over 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[12]

In the data security context, the FTC conducts its investigations with a focus on reasonableness – a company's data security measures must be reasonable 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 examines such factors as whether the risks at issue were well known or reasonably foreseeable, the costs and benefits of implementing various protections, and the tools that are currently available and used in the marketplace. This same reasonableness requirement is the basis for sectoral laws that have data security requirements, including the GLB Act and the FCRA.

Since 2001, the Commission has used its authority under these laws to settle 50 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information.[13] The practices at issue were not merely isolated mistakes. In each of these cases, the Commission examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. And through these settlements, the Commission has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.

---

[12] Some of the Commission's data security settlements allege both deception and unfairness.

[13] *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.

In its most recent case, the FTC settled allegations that GMR Transcription Services, Inc., and its owners violated Section 5 of the FTC Act.[14] According to the complaint, GMR provides audio file transcription services for their clients, which include health care providers, and relies on service providers and independent typists to perform this work. GMR exchanged 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 resolving the case 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 its first data security settlement concerning the "Internet of Things" – *i.e.*, Internet-connected refrigerators, thermostats, cars, and many other products and devices which can communicate with each other and/or consumers. The TRENDnet settlement involved a video camera designed to allow consumers to monitor their homes remotely.[15] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were "secure." However, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet

[14] *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.

[15] *TRENDnet, Inc.*, No. 122-3090 (Sept. 4, 2013), *available at* http://www.ftc.gov/opa/2013/09/trendnet.shtm.

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.

Finally, the FTC has also 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.[16] For example, the Commission alleged that TJX's failure to use reasonable and appropriate security measures resulted in a hacker obtaining 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.[17] Banks also claimed that tens of millions of dollars in fraudulent charges were made, and cancelled and reissued millions of cards. Meanwhile, criminal law enforcement authorities investigated and prosecuted the hackers involved in this and other data breaches.[18] As this matter illustrates, the goals of FTC and federal criminal agencies are complementary: FTC actions send a message that businesses need to protect their customers' data on the front end, and actions by criminal agencies send a message to identity thieves that their efforts to victimize consumers will be punished.

---

[16] *See, e.g., Dave & Busters, Inc.*, No. C-4291 (F.T.C. May 20, 2010), *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), *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), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

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

[18] *See, e.g.*, Kim Zetter, *TJX Hacker Gets 20 Years in Prison*, Wired, Mar. 25, 2010, *available at* http://www.wired.com/threatlevel/2010/03/tjx-sentencing/.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security, including by hosting workshops on emerging business practices and technologies affecting consumer data. This testimony describes two such recent initiatives that addressed information security issues.

In November, the FTC held a workshop on the Internet of Things.[19] 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, health and fitness devices, and cars.

Last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[20] 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.

The Commission has also hosted programs on emerging forms of identity theft, such as child identity theft[21] and senior identity theft.[22] In these programs, the Commission discussed

---

[19] 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/.

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

[21] 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.

unique challenges facing children and seniors, and worked with stakeholders to develop outreach messages and plans for these two communities. Since the workshops took place, the Commission has continued to engage in such tailored outreach.

C. Consumer Education and Business Guidance

The Commission also promotes 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.[23] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[24] average more than 2.2 million unique visits per year.

As directed by Congress, the Commission maintains the nation's main repository of identity theft complaints, housed within our Consumer Sentinel consumer complaint database, and provides centralized resources for victims of identity theft.[25] Identity theft has been the top consumer complaint to the FTC for 13 consecutive years, and tax identity theft – which often begins by thieves obtaining Social Security numbers and other personal information from consumers in order to obtain their tax refund – has been an increasing share of the Commission's identity theft complaints.[26] To address these concerns, Commission staff have worked with members of Congress to host numerous town hall meetings on identity theft in order to educate their constituents. And, just last month, the FTC hosted 16 events across the country, along with

---

[22] FTC Workshop, *Senior Identity Theft: A Problem in This Day and Age* (May 7, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/05/senior-identity-theft-problem-day-and-age.

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

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

[25] 18 U.S.C. § 1028 note.

[26] In 2012, tax identity theft accounted for more than 43% of the identity theft complaints, making it the largest category of identity theft complaints by a substantial margin. *See* Press Release, *FTC Releases Top 10 Complaint Categories for 2012* (Feb. 26, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/02/ftc-releases-top-10-complaint-categories-2012.

a series of national webinars and Twitter chats as part of Tax Identity Theft Awareness Week.[27] The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims. 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.[28]

The Commission directs its outreach to businesses as well. The FTC widely disseminates a business guide on data security, [29] along with an online tutorial based on the guide.[30] 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 has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.[31] For example, because mobile applications ("apps") and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.[32] The FTC also creates

---

[27] Press Release, *FTC's Tax Identity Theft Awareness Week Offers Consumers Advice, Guidance* (Jan. 10, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/ftcs-tax-identity-theft-awareness-week-offers-consumers-advice.

[28] *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 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.

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

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

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

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

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[33] and how to properly secure and dispose of information on digital copiers.[34]

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.[35] 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 consumers will enable them to request that fraud alerts be placed in their credit files, obtain

---

[33] *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.

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

[35] *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.

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, rulemaking authority under the Administrative Procedure Act, and jurisdiction over non-profits. 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.[36] 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[37] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[38] Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology in implementing the legislation.

VI. 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 Congress on this critical issue.

---

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

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

[38] 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.