

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION
on
Safeguarding Consumers' Financial Data
Before the
COMMITTEE ON BANKING, HOUSING, & URBAN AFFAIRS
SUBCOMMITTEE ON NATIONAL SECURITY
& INTERNATIONAL TRADE & FINANCE
UNITED STATES SENATE
Washington, D.C.
February 3, 2014

I. INTRODUCTION

Chairman Warner, Ranking Member Kirk, and members of the Subcommittee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s testimony on data security.

As recent publicly announced data breaches remind us,² consumers’ information is subject to a variety of risks. 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. And in this increasingly interconnected economy, 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 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

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 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> (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>.

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, and policy initiatives.

This testimony offers an overview of the Commission's recent efforts in the enforcement, education, and policy areas. It then describes the FTC's cooperation with federal and state agencies on issues of privacy and data security. Finally, while the testimony does not offer views on any particular legislation, the Commission reiterates its bipartisan support for Congress to enact data security 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.⁴

⁴ The Commission has long supported data security and breach notification legislation. *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>.

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.⁵ 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,⁶ and imposes safe disposal obligations on entities that maintain consumer report information.⁷ The Children’s Online Privacy Protection Act (COPPA) requires reasonable security for children’s information collected online.⁸

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.⁹ 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 5.¹⁰ 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. 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

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

⁶ 15 U.S.C. § 1681e.

⁷ *Id.* at § 1681w. The FTC’s implementing rule is at 16 C.F.R. Part 682.

⁸ 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 (“COPPA Rule”).

⁹ 15 U.S.C. § 45(a).

¹⁰ *See* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.¹¹ The Commission has settled more than 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 and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.¹³ In each investigation, 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.

Since 2001, the Commission has used its authority to settle 50 cases against businesses that it charged with failing to provide reasonable protections for consumers' personal information.¹⁴ 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 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.

¹¹ See Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement").

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

¹³ In many of the FTC's data security cases based on deception, the company has made an express or implied claim that its information security practices are reasonable, which is analyzed through the same lens.

¹⁴ 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 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.¹⁵ 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.¹⁶ The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from baby monitoring to home security. 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 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

¹⁵ *In the Matter of GMR Transcription Servs., Inc., et al.*, Matter No. 112-3120 (Dec. 16, 2013), available at <http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it>.

¹⁶ *In the Matter of TRENDnet, Inc.*, Matter No. 122-3090 (Sept. 4, 2013), available at <http://www.ftc.gov/opa/2013/09/trendnet.shtm>.

software updates to correct them, and provide affected customers with free technical support for the next two years.

Finally, one of the best-known FTC data security cases is the 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including Social Security numbers in some instances) concerning more than 160,000 consumers to data thieves posing as ChoicePoint clients.¹⁷ In many instances, the thieves used that information to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of the consumers' information and ignored obvious security red flags. For example, the FTC alleged that the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for violations of the FCRA and \$5 million in consumer redress for identity theft victims, and agreed to undertake comprehensive data security measures.¹⁸

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security. For example, through its reports, the FTC has encouraged companies to provide reasonable security for consumer data by following certain key principles.¹⁹ First, companies should know

¹⁷ *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/09/choicepoint-inc>.

¹⁸ In 2009, 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. *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. 2009) (settlement entered on Oct. 14, 2009).

¹⁹ FTC Report, *Protecting Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

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.²⁰

The FTC also hosts workshops on business practices and technologies affecting consumer data. For example, 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.²¹ 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, connected health and fitness devices, and connected cars. Also, last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.²² The forum brought together technology researchers, industry members and academics to explore the security of existing and

²⁰ *Id.* at 24-32.

²¹ 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/>.

²² FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), available at <http://www.ftc.gov/bcp/workshops/mobile-security/>.

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 and senior identity theft. In these programs, the Commission discussed unique challenges facing children and seniors, and worked with stakeholders to develop outreach 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 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.²³ OnGuard Online and its Spanish-language counterpart, Alerta en Línea,²⁴ average more than 2.2 million unique visits per year. Also, as part of its efforts to educate consumers about identity theft, Commission staff have worked with members of Congress to host numerous town hall meetings on identity theft in order to educate their constituents. And, 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.²⁵

²³ See <http://www.onguardonline.gov>.

²⁴ See <http://www.alertaenlinea.gov>.

²⁵ 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>.

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security,²⁶ along with an online tutorial based on the guide.²⁷ 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.

The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.²⁸ 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.²⁹ 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 risks³⁰ and how to properly secure and dispose of information on digital copiers.³¹

III. COOPERATION WITH STATE AND FEDERAL AGENCIES

The Commission has a long history of working closely with federal and state agencies, as well as the private sector, to further its mission of promoting privacy and data security. State, federal, and private sector entities each have served a unique role in data security: states have

²⁶ See *Protecting Personal Information: A Guide for Business*, available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>.

²⁷ See *Protecting Personal Information: A Guide for Business (Interactive Tutorial)*, available at <http://business.ftc.gov/multimedia/videos/protecting-personal-information>.

²⁸ See generally <http://www.business.ftc.gov/privacy-and-security/data-security>.

²⁹ See *Mobile App Developers: Start with Security* (Feb. 2013), available at <http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security>.

³⁰ 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>.

³¹ See *Copier Data Security: A Guide for Business* (Nov. 2010), available at <http://business.ftc.gov/documents/bus43-copier-data-security>.

innovated by passing data breach notification laws; federal banking agencies have protected consumers' security in the banking sector; the FTC has protected the security of consumers' information in retail, technology, and other sectors; federal criminal law enforcement agencies have prosecuted identity thieves; credit reporting agencies have provided credit monitoring services to consumers in the event of a breach; and trade associations sponsor educational seminars and publish guidance to help their members understand their legal obligations.

In terms of cooperation with states, the FTC works closely with state Attorneys General to ensure that we coordinate our investigations and leverage our resources most effectively. For example, in one of the largest FTC-state coordinated settlements on record, LifeLock, Inc. agreed to pay \$11 million to the FTC and \$1 million to 35 state Attorneys General to settle charges that the company used false claims to promote its identity theft protection services.³² As part of the settlement, LifeLock and its principals are barred from making deceptive claims and required to take more stringent measures to safeguard the personal information they collect from customers. The FTC also coordinated with the state AGs on cases such as TJX³³ and ChoicePoint.³⁴

³² *FTC v. LifeLock, Inc., et al.*, No. 2:10-cv-00530-NVW (D. Ariz.) (filed Mar. 9, 2010), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/11/lifelock-inc-corporation>.

³³ *In the Matter of The TJX Cos., Inc.*, 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>; see also Press Release, *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisent for Failing to Provide Adequate Security for Consumers' Data* (Mar. 27, 2008), available at <http://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx> (citing the Commission's coordination with 39 state Attorneys General).

³⁴ *United States v. ChoicePoint, Inc.*, *supra* note 17; see also Press Release, *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress* (Jan. 26, 2006), available at <http://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million> (mentioning the FTC's cooperation with the Department of Justice and Securities and Exchange Commission).

In terms of federal enforcement cooperation, the FTC has worked with criminal law enforcement agencies such as the Federal Bureau of Investigation and Secret Service. The goals of FTC and federal criminal law enforcement agencies are complementary: FTC actions send a message that businesses need to protect their customers' data on the front end, and criminal law enforcement actions send a message to identity thieves, fraudsters, and other criminals that their efforts to victimize consumers will be punished.

The FTC also works closely with state and federal agencies to educate consumers and businesses on issues involving data security and privacy. For example, 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.³⁵ Just last month, the FTC hosted 16 events across the country, along with a series of national webinars and Twitter chats as part of Tax Identity Theft Awareness Week.³⁶ The events, which included representatives of the Internal Revenue Service, the American Association of Retired Persons, and local U.S. Attorney's offices, 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.

³⁵ 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>.

³⁶ 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>.

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 Congress on this critical issue.