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

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

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

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

what consumer information they have and what personnel or third parties have, or could have, access to it. Understanding how information

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/unfornfornfTf-Tc(.)TjET/Cs6 cs 0 0 1 -7e

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 risks[30] 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 TJX[33] and

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.