Maureen K. Ohlhausen, FTC Commissioner
Remarks Before the Congressional Bipartisan Privacy Caucus
February 3, 2014

I would like to thank Representatives Barton and DeGette, the co-chairs of the Congressional Bipartisan Privacy Caucus, for inviting me to discuss the FTC's role in data security and the specific tools used by the agency to protect consumers' personal data. First, on behalf of all of the FTC Commissioners, I urge Congress to enact data security legislation that would enhance the FTC's enforcement of data security, provide greater clarity for consumers who suffer a breach of their data, and streamline and improve the steps companies must take to notify consumers when a breach occurs.[1]

As recent publicly announced data breaches, including those involving Target and Neiman Marcus[2] remind us, consumers' information is subject to a variety of risks. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to sensitive information, and potentially misuse it in ways that can cause serious harms to consumers as well as businesses. Such harms include identity theft, a pernicious crime that hurts both consumers and financial institutions. The Bureau of Justice Statistics estimates that in 2012, 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft, as defined to include any fraudulent and other misuse of an existing account.[3]

The FTC's Role in Data Security

As companies collect more personal information about their customers, they need to protect this information from theft and unauthorized access, which can hurt customers and harm the business's reputation. The FTC is concerned with how entities with consumer data safeguard it from unauthorized access by data hackers or by insiders. To address these data security issues the Commission uses a multipronged approach of enforcement, research, and education.

Law Enforcement

Congress has authorized the Commission to enforce several laws and rules that place obligations upon businesses that possess consumer data. The Commission's Safeguards Rule,

---

[1] The current FTC Commissioners are on record supporting federal data security legislation. Beyond that, the views I express today are my own and do not necessary reflect the views of my fellow Commissioners.

[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).

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

which implements the Gramm-Leach-Bliley Act, for example, provides data security requirements for non-bank financial institutions.[4] The Fair Credit Reporting Act 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 it imposes safe disposal obligations on entities that maintain consumer report information.[6] The Children's Online Privacy Protection Act requires reasonable security for children's information collected online.[7]

In addition, the Commission enforces the prohibition 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, that are likely to mislead reasonable consumers, the statements or omissions may 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. 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 under Section 5. The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.

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 business, and the cost of available tools to improve security and reduce vulnerabilities.[10] In each investigation, the Commission examines factors such as whether the risks at issue were well known or reasonably foreseeable, and the costs and benefits of implementing various protections based on the tools that are currently available and used in the marketplace.

---

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

[5] 15 U.S.C. § 1681e.

[6] *Id.* § 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.

[8] 15 U.S.C. § 45(a).

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

[10] 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 under the same standard.

Just a week ago, the Commission announced the 50th settlement in a data security case.[11] 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 security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that there is no such thing as perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law.

Let me give you one example of a recent case in this area to illustrate our enforcement in this area. The FTC recently announced a case against TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.[12] 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 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 reasonable security program, obtain outside audits, notify consumers about the security flaw and how to correct it, and provide affected customers with free technical support for the next two years.

Policy Initiatives

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" – a term coined to describe the proliferation of Internet-connected devices.[13] The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity 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 the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from security threats.[14]

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

---

[11] *In the Matter of GMR Transcription* Services, Inc., a corporation, and Ajay Prasad and Shreekant Srivastava (FTC file: 122 3095)

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

[13] 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/.

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

unique challenges facing children and seniors and worked with stakeholders to develop outreach messages and plans for these two communities.

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.[15] OnGuard Online and its Spanish-language counterpart Alerta en Línea[16] average more than 2.2 million unique visits per year.

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.[17] 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.

In fact, Congress is one of our most important partners in our effort to educate consumers and businesses on effective data security practices. Through our congressional outreach initiative, several hundred members of Congress link to our online information through their own websites. Additionally, we provide materials, and, as appropriate, staffing for local town hall meetings and consumer events hosted by a member of Congress.

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.[18] 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

---

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

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

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

[18] *See, e.g.*, Prepared Statement of the Federal Trade Commission, "Safeguarding Consumers' Financial Data," Before the Subcommittee on National Security and International Trade and Finance of the Senate Committee on Banking, Housing, and Urban Affairs, 113th Cong., February 3, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-safeguarding-consumers-financial-data/140203financialdatasecurity.pdf .

copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. 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.[19] To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for data security and breach notice violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits[20] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[21] Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology in implementing the legislation.

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.

---

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

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

[21] 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.