PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Small Business Cybersecurity: Federal Resources and Coordination

Before the

COMMITTEE ON SMALL BUSINESS

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

March 8, 2017

I. Introduction

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, I am Maureen Ohlhausen, Acting Chairman of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security and, in particular, its efforts to educate small businesses.

Reports of data breaches affecting millions of American consumers have become commonplace.[2] Data is an increasingly vital asset for every business, including small businesses, and as companies collect more personal information from consumers, the databases they create become more attractive targets for criminals. 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 and businesses.

Failing to take reasonable precautions to secure data from identity thieves and other malicious actors hurts consumers and legitimate businesses alike. Consumers face the risk of fraud, identity theft, and other harm.[3] In addition, data breaches can harm a business's financial interests and reputation as well as result in the loss of consumer confidence in the businesses to whom they entrust their data. In the case of small businesses, a data breach can be devastating.

---

[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, e.g.*,Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. Times, Dec. 14, 2016, *available at* https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0; Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. Times, Oct. 21, 2016, *available at* https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html (describing the Dyn DDoS attack that relied on hundreds of thousands of IoT devices); 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, 2014* (Sept. 2015), *available at* https://www.bjs.gov/content/pub/pdf/vit14.pdf (estimates that 17.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2014).

Although such incidents rarely make the headlines, the majority of attacks target small and mid-sized businesses, and, according to the National Cyber Security Alliance, some 60% of small businesses go out of business within six months of a breach.[4]

The Federal Trade Commission is a small, independent agency with a large role to play when it comes to data security. The Commission, a bipartisan body, has operated effectively for more than 100 years, with a unique dual mandate to protect consumers and maintain competition in broad sectors of the economy. As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector using the flexible tools Congress gave us. The Commission has undertaken substantial efforts throughout the 21st century to promote data security in the private sector through civil law enforcement, business outreach and consumer education, policy initiatives, and recommendations to Congress to enact legislation in this area. This testimony provides an overview of those efforts.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

The Commission enforces several statutes and rules that impose data security requirements on companies. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, sets forth data security requirements for

[4] *See* Gary Miller, *60% of Small Companies That Suffer a Cyber Attack Are Out of Business Within Six Months*, The Denver Post, Oct. 23, 2016, *available at* http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/; Oscar Marquez, *The Costs and Risks of a Security Breach for Small Businesses*, Security Magazine, July 26, 2016, *available at* http://www.securitymagazine.com/articles/87288-the-costs-and-risks-of-a-security-breach-for-small-businesses; Robert Strohmeyer , *Hackers Put a Bull's-Eye on Small Business*, PCWorld, Aug. 12, 2013, *available at* http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html.

financial institutions within the Commission's jurisdiction.[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 it 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 FTC Act, which prohibits unfair or deceptive acts or practices, such as businesses making false or misleading claims about their data security procedures, or failing to employ reasonable security measures and, as a result, causing or likely causing substantial consumer injury.[9]

Since 2001, the Commission has used its authority under these laws to take enforcement action and obtain settlements in approximately 60 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information.[10] In each of these cases, the practices at issue were not merely isolated mistakes. Instead, the Commission examined the company's practices as a whole and challenged alleged data security failures that were multiple and systemic. And through these actions and orders, the Commission has made clear that it does not require perfect security; that reasonable security is a continuous

---

[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). 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. 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] *See generally* http://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249.

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.

An example of this approach can be found in the FTC's recent settlement with AshleyMadison.com. In that case, the FTC alleged that the companies responsible for the site failed to protect 36 million users' personal information in relation to a massive data breach of their network – one of the largest data breaches that the FTC has investigated to date.[11] According to the FTC, although the defendants assured users their sensitive information was private and securely protected, the security of AshleyMadison.com was lax. According to the complaint, the defendants had no written information security policy, no reasonable access controls, inadequate security training of employees, no knowledge of whether third-party service providers were using reasonable security measures, and no measures to monitor the effectiveness of their system security. Intruders accessed the companies' networks several times between November 2014 and June 2015, but due to their lax data-security practices, the defendants allegedly did not discover the intrusions. Following a major data breach in July 2015, the hackers published sensitive information for more than 36 million AshleyMadison.com users. According to the complaint, this included information that the defendants had retained on users who had paid for an account deletion option that purportedly removed users' data from the site.

The FTC also brought a data security enforcement action last year against computer hardware maker ASUSTeK Computer, Inc. According to the complaint, ASUS marketed its routers as including numerous security features that the company claimed could "protect computers from any unauthorized access, hacking, and virus attacks" and "protect [the] local

[11] *FTC v. Ruby Corp. et al*., No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison.

network against attacks from hackers."[12] Despite these claims, the FTC's complaint alleged that ASUS failed to take reasonable steps to secure the software on its routers. The Commission charged that critical security flaws in ASUS' routers put the home networks of hundreds of thousands of consumers at risk. The FTC also alleged that the routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal data on the internet.

The Ashley Madison and ASUS settlements, along with the FTC's other data security settlements, are available on the FTC website, and descriptions of the proposed complaints and consent orders are published in the Federal Register before each settlement is made final. The settlements provide companies with insight into the practices that the FTC has alleged to be unreasonable.[13] By learning about alleged lapses that led to law enforcement action, companies can improve their practices to avoid fundamental security missteps.

Commission complaints are not the only enforcement-related source of information that may assist businesses. The FTC closes far more data security cases than it pursues to settlement or litigation. Staff is currently working to provide the public with more information about these closed matters, which will help further illustrate, through additional examples, how the Commission has consistently applied the principles contained in its longstanding existing public guidance materials, discussed below.

B. Business Guidance and Consumer Education

In addition to law enforcement, the FTC engages in extensive business and consumer education on data security. Our goal is to provide information to help businesses protect the data

[12] *ASUSTeK Computer Inc.*, No. C-4587 (July 28, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.
[13] *See generally* www.ftc.gov/datasecurity.

in their care and understand what practices may run afoul of the FTC Act. In fiscal year 2016, the FTC filled orders for more than 500,000 free printed publications for businesses on data security. We provide general business education about security issues, as well as specific guidance on emerging threats, such as ransomware, which is discussed below.

For general education, the FTC offers user-friendly guidance to help companies of all sizes improve their data security practices and comply with the FTC Act. For example, in November the FTC released an update to *Protecting Personal Information: A Guide for Business*.[14] The FTC first published this guide in 2007 and has updated it periodically ever since.

Last fall, the FTC released *Data Breach Response: A Guide for Business*, which outlines steps businesses should follow when they experience a data breach.[15] The Guide, and a related video, describe immediate steps companies should take, such as taking breached systems offline, securing physical areas to eliminate the risk of further harm from the breach, and notifying consumers. And the Guide includes a model data breach notification letter businesses can use to get started.

Also, in 2015, the FTC launched its *Start with Security* initiative, which includes a guide for businesses that summarizes the lessons learned from the FTC's data security cases,[16] as well as 11 short videos.[17] These materials discuss ten important security topics and give advice about

---

[14] *Protecting Personal Information: A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[15] *Data Breach Response: A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.
[16] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[17] *Start with Security: Free Resources for Any Business* (Feb. 19, 2016), *available at* https://www.ftc.gov/news-events/audio-video/business.

specific security practices for each. As part of this initiative, the FTC hosted events in San Francisco, Austin, Seattle, and Chicago, bringing business owners and app developers together with industry experts to discuss practical tips and strategies for implementing effective data security.[18] Last year, FTC staff presented our *Start with Security* materials on six cybersecurity webinars sponsored by the National Institute of Standards and Technology (NIST) and the SBA; thousands of small business owners attended these webinars. We also issued a publication directed toward businesses to educate them on how the NIST Cybersecurity Framework applies to FTC best practice.[19]

In addition to general data security guidance, the FTC also provides businesses with specific guidance on emerging threats. For example, most recently the FTC released a staff perspective and related blog post to help businesses prevent phishing scams.[20] These materials encourage businesses to use email authentication – a technical solution that businesses can use to protect their reputations and prevent phishing emails from getting through to their customers.[21] The FTC has also educated businesses about threats like ransomware – malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom. Following a workshop,[22] the FTC published a

---

[18] *See, e.g.*, FTC Event, Start with Security – Seattle (Feb. 9, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/02/start-security-seattle.
[19] FTC Business Blog, *The NIST Cybersecurity Framework and the FTC*, Aug. 31, 2016, *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.
[20] FTC Staff Perspective, *Businesses Can Help Stop Phishing and Protect Their Brands Using Email Authentication* (Mar. 2017), *available at* https://www.ftc.gov/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff; FTC Business Blog, *Want to stop phishers? Use email authentication*, Mar. 3, 2017, *available at* https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication.
[21] Email authentication is a collection of techniques that allow ISPs and others to verify the domain of the sender of an email. These techniques include Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain Message Authentication Reporting & Conformance (DMARC).
[22] *Fall Technology Series: Ransomware* (Sept. 7, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware.

blog post describing the nature of the ransomware threat, how to defend against ransomware, and essential steps to take if businesses become victims of ransomware.[23]

Further, the FTC develops guidance for companies in specific industries. For example, we developed *Careful Connections*, business guidance that includes a series of steps for companies to consider if they design and market Internet-connected products.[24] We have also developed specific security guidance for mobile app developers.[25]

In the coming months, the FTC plans to expand its outreach to small businesses around data security issues, with a focus on helping very small businesses identify risks and develop data security plans.

Very small businesses, including sole proprietors and companies with just a few employees, generally do not have full-time information technology or human resources staff. Some of the cybersecurity challenges they face are similar to those confronting consumers, such as securing their wireless networks or avoiding phishing scams. The FTC offers free resources and educational materials to help consumers protect themselves from the evolving threats they face while using technology. For example, the FTC has provided guidance for consumers on securing their home wireless networks, a critical security step for protecting devices and personal information from compromise.[26] These and other resources are accessible on the FTC's

---

[23] FTC Business Blog, *Ransomware – A Closer Look* (Nov. 10, 2016), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.
[24] *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.
[25] *Mobile App Developers: Start with Security* (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.
[26] FTC Consumer Blog, *Securing Your Wireless Networks*, Sept. 2015, *at* https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network.

consumer guidance website, consumer.ftc.gov.[27]

Finally, the FTC launched an improved version of IdentityTheft.gov[28] (robodeidentidad.gov in Spanish[29]) last year. It's a free, one-stop resource consumers can use to report and recover from identity theft. As part of the site, identity theft victims obtain personalized recovery plans based on their specific experience with identity theft, and get customized letters and forms to send to credit bureaus, debt collectors, and other businesses. More than 400,000 victims have used IdentityTheft.gov in the last year.

C. Policy Initiatives

Finally, the FTC pursues numerous policy initiatives to enhance data security. The FTC has hosted workshops and issued reports recommending best practices designed to improve data security and privacy and to highlight the privacy and security implications of new technologies and business practices. For example, last year the FTC hosted a three-part Fall Tech Series to examine new and evolving technologies that raise critical consumer protection issues, focusing on ransomware, drones, and smart TVs.[30]

The FTC works across the government, providing comments to other agencies as they engage in cybersecurity initiatives. For example, the FTC provided comments to NHTSA during the development of the Federal Automated Vehicle Policy.[31]

---

[27] *See generally* https://www.consumer.ftc.gov/.
[28] *See* https://identitytheft.gov/.
[29] *See* https://robodeidentidad.gov/.
[30] Press Release, *FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues* (Mar. 31, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.
[31] Comment of Jessica L. Rich, Director, Bureau of Consumer Protection, to the National Highway Traffic Safety Administration Supporting the Inclusion of Consumer Privacy and Cybersecurity Guidance in the Document "Federal Automated Vehicles Policy" (Nov. 2016), *available at* https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/11/comment-jessica-l-rich-director-bureau-consumer.

In addition, in January, the FTC announced an Internet of Things (IoT) security challenge.[32] The Commission is offering a cash prize of up to $25,000 for the best technical solution that helps consumers quickly identify security vulnerabilities in their IoT devices and pushes out updates to address those vulnerabilities. The FTC is particularly interested in tools that can prompt consumers to change default passwords to decrease the risk of their IoT devices being compromised. This important initiative will draw attention to IoT security problems and facilitate solutions that consumers and small businesses can use.

III. Legislation

The Commission continues to reiterate its longstanding, bipartisan call for comprehensive data security legislation that would (1) strengthen its existing data security authority and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[33] Reasonable 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 a database with Social Security numbers, notifying 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

[32] Press Release, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security.

[33] 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 common carriers, and the authority to issue implementing rules under the notice and comment rulemaking procedures of the Administrative Procedure Act, 5 U.S.C. § 553. The Court of Appeals for the Ninth Circuit recently held that the FTC could not bring a case against AT&T because the common carrier exception in Section 5 of the FTC Act precluded FTC enforcement of the Act against any company with the status of a common carrier, even if the case involved non-common-carrier activities. *See* FTC v. AT&T Mobility LLC, 835 F.3d 993 (9th Cir. 2016). The Commission has asked the court to rehear the case en banc, and its petition remains pending.

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.

IV. Conclusion

Thank you for the opportunity to provide the Commission's views on data security. The FTC is committed to keeping data secure without imposing unnecessary or undue costs on businesses, including small businesses. We look forward to continuing to work with the Committee and Congress on this critical issue.