PREPARED STATEMENT OF

I. Introduction

Chairman Chabot, Ranking Member

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

network against attacks from hackers.[12] Despite these claims, the FTC 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 0.915 0 Td6ag

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

consumers. And the Guide includes a model data breach notification letter businesses can use to get started.

Also, in 2015, the FTC launched it

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, *W(lo)-1.7j 0.003 Tf8 Tc 0.001 Tw [s-3.7(*

blog post

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. When 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),

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 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.