PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Data Breach on the Rise: Protecting Personal Information From Harm

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

Washington, D.C.

April 2 , 2014

I. INTRODUCTION

Chairman Carper, Ranking Member Coburn, and members of the Committee, I am Edith Ramirez, Chairwoman of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security, and I thank you for your leadership, Chairman Carper, on this important issue.

Consumers' data is at risk. Recent publicly announced data breaches[2] remind us that hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harm to consumers as well as businesses. These threats affect more than payment card data; breaches reported in recent years have also compromised Social Security numbers, account passwords, health data, information about children, and other types of personal information.

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 wrong hands, resulting in fraud, identity theft, and other harm, along with a potential loss of consumer confidence in the marketplace. As one example, 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]

---

[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 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

As the nation's leading privacy enforcement agency, the Commission has undertaken substantial efforts for over a decade to promote data security and privacy in the private sector through civil law enforcement, education, and policy initiatives. The Commission is here today to reiterate its longstanding

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[8] A company acts deceptively if it makes materially misleading statements or omissions.[9] Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims about the security they provide for consumers' personal data. Further, a company engages in unfair acts or practices if its 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.[10] The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[11]

The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission

to implement comprehensive information security programs 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.[15] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. 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 software updates to correct them, and provide affected customers with free technical support for the next two years.

The FTC also has brought a number of cases alleging that unreasonable security practices allowed hackers to gain access to consumers' credit and debit card information, leading to many millions of dollars of fraud loss.[16] The Commission's settlement with TJX provides a good example of the FTC's examination of reasonableness in the data security context.[17] According to the complaint, TJX engaged in a number of practices that, taken together, failed to reasonably protect consumer information. Among other things, it (1) failed to implement measures to limit

[15] p6 --2.32 (3090/(et)t(et))T Td( )]Tnd5(a)need

wireless access to its stores, allowing a hacker to connect wirelessly to its networks without authorization; (2) did not require network administrators to use strong passwords; (3) failed to use a firewall or otherwise limit access to the Internet on networks processing cardholder data; and (4) lacked procedures to detect and prevent unauthorized access, such as by updating antivirus software and responding on security warnings and intrusion alerts. As a result, a hacker obtained tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers who turned merchandise to the stores. As this matter illustrates, the FTC's approach to reasonableness asks to see whether companies have implemented basic, fundamental safeguards that are reasonable and appropriate in light of the sensitivity and volume of the data it holds, the size and complexity of its data operations, and the cost of available tools.

B. Policy Initiatives t[(Fpe)Tpen

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.[20] 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. Commission staff is developing a report on privacy and security issues raised at the workshop and in the public comments.

And last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[21] As the use of

dispose of information that they no longer need. Finally, companies should have in place a plan to respond to security incidents, should they occur.

Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from

Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC in implementing the legislation to respond to changes in technology. For example, whereas a decade ago it would be incredibly difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. And, as the growing problem of child identity theft has brought to light in recent years,