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 CarperRanking Member Coburn, and members of then the chittee, I am Edith Ramirez Chairwoman of the Federal Trade Commission ("FTC" or "Commission"). appreciate the opportunity to present the Commission's testimony on data security your leadership, Chairman Carper, on this important issue

Consumers' data is at risk.eRent publicly anounced data breaches mind usthat hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that cause serious harm to consumers as well as businesse. These threats affect more than payment card data; breaches reported in recent years ave also comproissed 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 the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud, identity the fand other harm, along with a potential loss of consumer confidence in the marketplaces one example be Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and where victims of identity the ft in 2012.

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 ©mmissioner.

² SeeElizabeth A. Harris &Nicole Perlroth, For Target, the Breach Numbers Gr, My.Y. Times, Jan. 10, 2014, available http://www.nytimes.com/2014/01/11/business/tarlggetachaffected70-million-customers.htm(discussing recentlannounced breaches involving payment card information by Target and Neiman Marcus); Nicole Perlroth, Michaels Stores Is Investigating Datarland. Times, Jan. 25, 2014, available http://www.nytimes.com/2014/01/26/technology/michæthresis-investigating databreach.htm(announcement of potential security breach involving payment card information)

³ See Bureau of Justice Statist Metatims of Identity Theft, 201 (20ec. 2013), available at

As the nation's leading privacy enforcement agency, the Commission has undertaken substantial effortsor over a decade to promote data security privacy in the private sector through civil law enforcement, education, and policy initiativese 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 A company acts deceptively if it makes materially misleading statements or omission by sing its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims about the theory unity provide for consumers' personal dataurther, a company engages in unfair acts or practices i its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers or a company engages in unfair acts or practices to consumers or to competition. The Commission has settled more than 20 called in that a company's failure to reasonably safeguard consumer data was an unfair practice.

The FTC conducts its data security investigations to determine wheeltown pany'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 operation the cost of available tools to improve security and reduce vulnerabilities. Commission

to implement comprehensive information security programd undergo independent audits for the next 20years.

The FTC also recently announced a case agaresNDnet which involved video camera designed to allow consumers to monitor their homes remote the complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring Although TRENDnetlaimed that the camerasere "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 comprehensivity program, obtain outside audits, notify consumers about the security issues and the availability of software updates 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 debinfcarmation, leading to many millions of dollars of fraud loss. The Commissions settlement with JX provides agood example of the FTC's examination of reasonableness in the data seoutety t¹⁷ According to the complaint, TJX engaged in a number of practices that, taken together, failed to regasonable protect consumer information. Among other things, it (1) failed to implement measures to limit

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

wireless access to its stores, allowingsæker to connect wireldssto its networks without authorization; (2) did not require etwork 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 meet merchandise to the stores. As this matter illustrates, the FTG approach to reasonable messaks to see whether companies have implemented basic, fundamental safegual that are reasonable appropriate in light of the sensitivity and volume of the data it holds, the size and complexity of its data operation this ecot of available tools.

B. Policy Initiatives t[(Fpe)Tpen

In November the FTC held a workshop on the nomenon known as the ternet of Things" – i.e., Internet connected refrigerators, thermostats, cars, and other products and services that can communicate with each other and/or consumer to explore the security together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity in everyday devices, in areas assedingen art homes, connected health and fitness devices, and condenses. 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 orbitensecurity issues, including potential threats to U.S. consumers and possible solutions to the solutio

dispose of information that they no longer need. Finally, companies should hamerapplace to respond to security incidents, should they occur.

Reasonable and appropriate curity 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 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 gwing problem of child identity theft has brought to light in recent years,