PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

March 18, 2014

I. INTRODUCTION

Chairman Burgess, Ranking Member Schakowsky, and members of the Subcommittee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").

lives, there are business and commercial ramifications – data breaches can harm a business's financial interests and reputation and also result in the loss of consumer confidence in the marketplace. With unrelenting reports of data breaches, and with a significant number of Americans suffering from identity theft, the time for strong legislation is now.

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. The Commission has undertaken substantial efforts for over a decade 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 the Commission's efforts and its views on the subcommittee's draft data security legislation.

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 non-bank financial institutions.[4] 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,[5] and imposes safe disposal obligations on entities that maintain consumer report information.[6] The

---

http://www.bjs.gov/content/pub/pdf/vit12.pdf

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

[5] 15 U.S.C. § 1681e.

[6] Id. at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

Children's Online Privacy Protection Act ("COPPA") requires reasonable security for children's information collected online.[7] In addition, the Commission enforces the FTC Act's prohibition against unfair or deceptive acts or practices in cases where the Commission has reason to believe that a business made false or misleading claims about its data security procedures, or failed to employ reasonable security measures and, as a result,

For example, the FTC's case against TRENDnet, Inc.,[10] involved a video camera designed to allow consumers to monitor their homes remotely. 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

information vulnerable to exposure – including Social Security numbers, birthdates, and credit report information in the Credit Karma app, and credit card information in the Fandango app. The Commission's settlements prohibit Credit Karma and Fandango from making misrepresentations about privacy and security, and require the companies to implement comprehensive information security programs and undergo independent audits for the next 20 years.

The FTC also has spent significant resources litigating two data security matters, both of which are ongoing. The first is a case against Wyndham Hotels, in which the Commission filed a lawsuit in federal court alleging that the company failed to protect consumers' personal information.[13]

The second matter is in administrative litigation that the Commission will decide as an adjudicative body. Accordingly, the Commission cannot discuss the matter in detail while it remains in administrative adjudication

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security, such as by issuing reports and hosting workshops on emerging business practices and technologies affecting consumer data. For example, recently the FTC released a staff report about the Internet of Things ("IoT"), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people.[14] The report found a wide range of security practices among manufacturers of these products. Among other things, the report recommends that companies developing IoT products should secure device functionality and implement reasonable security by, for example, conducting risk assessments, hiring and training appropriate personnel, and monitoring access controls.

Last year, the FTC hosted a three-part "Spring Privacy Series" to examine the privacy implications of new areas of technology that have garnered considerable attention for both their potential benefits and the possible privacy concerns they raise for consumers.[15] The series focused on three areas: mobile device tracking in retail stores, the use of predictive scoring to help companies predict consumer behavior and shape how they market to particular consumers;

---

[14] FTC Staff Report, Internet of Things: Privacy and Security in a Connected World (Jan. 2015), available at http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Commissioner Ohlhausen issued a concurring statement. See http://www.ftc.gov/system/files/documents/public_statements/620691/150127iotmkostmt.pdf. Commissioner Wright dissented to the release of the report. See http://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf

[15] See Press Release, FTC to Host Spring Seminars on Emerging Consumer Privacy Issues, Dec. 2, 2013, available at http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues

and health apps that consumers increasingly use to manage and analyze their health data. At the seminar on health apps, panelists noted that many businesses operating in the consumer generated and controlled health information space might not be covered by the Health Insurance Portability and Accountability Act ("HIPAA"), and thus would not be subject to HIPAA's data security protections. Participants also expressed concern that inadequate data security could result in unauthorized access to data, and cited the importance of building security into products and services, as well as the risks of failing to do so. Participants pointed to secure storage, encryption, and strong password protection as steps companies could take to secure consumers' data.

C. Business Guidance and Consumer Education

The Commission also promotes better data security practices through business guidance and consumer education. On the business guidance front, the FTC widely disseminates a business guide on data security,[16] and has developed both an online tutorial[17] and a recent blog post[18] based on the guide. 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. The Commission also releases industry-targeted to a non-legal audience regarding basic data security issues for businesses.[19] In addition, the FTC develops data security guidance for specific industries. For example, the FTC has developed

---

[16] See Protecting Personal Information: A Guide for Business, available at http://www.ftc.gov/tips-advice/business-center/protecting-personal-information-guide-business.

[17] See Protecting Personal Information: A Guide for Business (Interactive Tutorial), available at http://www.ftc.gov/news-events/audio-video/video/protecting-personal-information-guide-business-promotional-video.

[18] FTC Blog, Time 2 Txt About Data Security Basics, Jan. 23, 2015, at http://www.ftc.gov/news-events/blogs/business-blog/2015/01/time-2-txt-about-data-security-basics.

[19] See generally http://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

specific guidance for mobile app developers as they create, release, and monitor their apps,[20] and we also recently developed blogs to provide data security guidance for tax preparers[21] and human resource professionals.[22]

The FTC also creates business educational materials on specific topics – such as the risks associated with peer-to-peer ("P2P") filesharing programs and companies' obligations to protect consumer and employee information from these risks.[23] Further, the FTC recently released guidance about ways to provide data security for IoT devices, which includes tips such as designing products with authentication in mind and protecting the interfaces between an IoT product and other devices or services.[24]

The Commission also engages in outreach to consumers. The FTC sponsors OnGuard Online, a website designed to educate consumers about basic computer security.

and other personal information from consumers in order to obtain their tax refund – has been an increasing source of the Commission's identity theft complaints.[27] The Commission hosts

In prior testimony before Congress, the FTC has called for federal legislation that would (1) strengthen its existing authority governing data security standards for companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[31] It is critical that companies implement reasonable security measures in order to prevent data breaches and protect consumers from identity theft and other harms. And when breaches do occur, notifying consumers will help them protect themselves from any harm 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 or security freezes be placed in their credit files, obtain 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 could simplify compliance by businesses while ensuring that all consumers are protected.

The Commission supports a number of elements in the proposed legislation. First, the bill includes a provision requiring that companies implement reasonable data security standards, in addition to a breach notification requirement. The Commission believes that both breach

[31] See, e.g., Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, available at http://www.ftc.gov/

potentially an account that allows charges to be incurred, even if the thief does not have the name of the account holder.

However, other aspects of the draft legislation do not provide the strong protections that are needed to combat data breaches, identity theft, and other substantial consumer harms.[35] First, the definition of personal information does not protect some of the information which is currently protected under state laws. Second, the bill should address the entire data ecosystem, including Internet-enabled devices. Third, the bill does not provide the Commission with rulemaking authority under the Administrative Procedure Act (APA), which is necessary to ensure that the bill's goals can still be achieved in an evolving marketplace. Finally, the scope of the breach notification trigger should be expanded to cover more substantial harm.

While the Commission understands the importance of targeting concrete, substantial harms, and has sought to do so in its own enforcement efforts, we are concerned the draft bill does not strike the right balance.[36] For instance, the draft bill does not cover certain types of consumer information – such as precise geolocation and health data – even though misuse of this and other information can cause real harm, including economic harm, to consumers. Revelations

---

[35] Commissioner Wright supports the data security and breach notification legislation as drafted and believes that it strikes the right balance in protecting consumers from cognizable and articulable economic and financial harms. He disagrees with his colleagues to the extent that they recommend expanding the proposed legislation beyond its current economic and financial scope.

[36] For example, our Unfairness Statement notes that when evaluating whether a business practice is unfair, "the Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm. Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair." FED. TRADE COMM'N., Letter to Hon. Wendell H. Ford & Hon. John C. Danforth, Committee on Commerce, Science, and Transportation, FTC Policy Statement on Unfairness (Dec. 17, 1980) (appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984)). See also GMR Transcription Services Inc., No. C-4482 (F.T.C. Aug. 21, 2014) (consent order) (alleging deception and unfairness violations in a case where sensitive private medical information was made publically available), available at https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.

of cancer treatment, for example, might cause an individual to lose a job or to receive calls from debt collectors. Furthermore, bad actors have an economic incentive to target reservoirs of valuable geolocation and health data for sale to debt collectors or private investigators. Indeed, the Commission has seen instances where bad actors hacked into company systems and stolen consumers' personal information in order to extract payments for its return. In addition, a breach revealing very personal and private details, such as the fact that an individual attends counseling for addiction, or a child walks back and forth from school at a particular time every day, can result in real economic and physical harms. Therefore, companies that collect precise geolocation information that can pinpoint a consumer's physical location, or information about an individual's physical or mental health condition, should have a duty to provide reasonable security for this data. Some of the state data security and data breach laws that would be preempted under the drafrsndiata6(a b)a(e)-10(co)-4(m)-(at)-6c be

The FTC also continues to believe that data security and breach notification legislation should include rulemaking authority under the APA. For example, a decade ago it would have been extremely difficult and expensive for a company to track an individual's precise geolocation. The privacy of such sensitive information was protected by the sheer impracticality of collecting it. Today the explosion of mobile devices has made such information readily available. Similar situations will no doubt arise as technology advances. Rulemaking authority would allow the Commission to ensure that even as technology changes and the risks from the use of certain types of information evolve, companies are required to appropriately protect such data. Such rulemaking authority would ensure the continuing vitality of the proposed law in light of the almost certain innovations in technology and business models, which may use different types of personal information than those currently enumerated but still raise the same risks of identity theft, economic loss or harm, financial fraud, or other substantial harm. APA rulemaking requires a notice and comment process, in which the Commission receives feedback from all stakeholders.

APA d74(r)3(om)-2(Tc 0 T 0.004 Tw [(ar)-1(e)]TJ 0 c 0 Tw4( )]TI)19(c 0 Tw-6(s)-5(uhc 0 Tw)-15(c-5

protect his/her interests in the event of a breach. Under the current draft of the bill, consumers are entitled to notice "[u]nless there is no reasonable risk that the breach has resulted in, will result in, identity theft, economic loss or economic harm, or financial fraud." The Commission is concerned that this standard will prevent consumers from receiving important breach notifications. The harm resulting from a breach may very well extend beyond economic or financial injury. For example, as discussed above, the breach of location data can reveal very sensitive information, such as whether an individual attends counseling, or the daily routines of a child. In the wrong hands, such information can result in economic and physical harm. For these reasons, the Commission supports an approach that requires notice unless a company can establish that there is no reasonable likelihood of economic, physical, or other substantial harm.

VI. CONCLUSION

Thank you for the opportunity to provide the Commission's views. The FTC remains committed to promoting reasonable security for consumer data, and we are ready to work with this subcommittee as it develops and considers legislation on this critical issue.