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

Doctor 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").[1] I appreciate the opportunity to present the Commission's testimony on data security legislation.

In the last year, headlines have been filled with reports of data breaches impacting millions of Americans.[2] These events serve as a constant reminder that consumers' data is at risk. 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. But data breaches are not a new phenomenon. We have been hearing about them for over a decade. Every year, new incidents are reported that reignite concern about data security, as well as debate about the best way to provide it.

The need for companies to implement strong data security measures is clear: if sensitive information falls into the wrong hands, the results can be devastating. Consumers face the risk of fraud, identity theft, and other harm. 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] Apart from the significant impact on individual consumers'

---

[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 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 (discussing Michaels Stores' announcement of potential security breach involving payment card information).

[3] *See* Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at*

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, causes or is likely to cause substantial consumer injury.[8]

Since 2001, the Commission has used its deception and unfairness authority under these laws to take enforcement action and obtain settlements in more than 50 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information.[9] 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 and appropriate security is a continuous 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.

For example, the FTC's case against TRENDnet, Inc. involved a video camera designed

---

[7] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[8] 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.

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

to allow consumers to monitor their homes remotely.[10] 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 a camera's Internet address. According to the Commission's complaint, this resulted in hackers posting 700 consumers' live video 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 two years of free technical support.

The FTC also entered into settlements with Credit Karma, Inc.[11] and Fandango, LLC[12] to resolve allegations that the companies misrepresented the security of their mobile apps. Credit Karma's mobile app allows consumers to monitor and access their credit scores, credit reports, and other credit report and financial data, and has been downloaded over one million times. Fandango's mobile app allows consumers to purchase movie tickets and has over 18.5 million downloads. According to the complaints, despite claims that the companies provided reasonable security to consumers' data, Credit Karma and Fandango did not securely transmit consumers' sensitive personal information through their mobile apps. In particular, the apps failed to authenticate and secure the connections used to transmit this data, and left consumers' information vulnerable to exposure – including Social Security numbers, birthdates, and credit

[10] *TRENDnet, Inc.*, No. C-4426 (F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

[11] *Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc.

[12] *Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc.

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] According to the FTC's complaint, Wyndham and its subsidiaries repeatedly failed to take reasonable and basic security measures, such as using complex user IDs and passwords and deploying firewalls between the hotels and the corporate network. In addition, Wyndham allegedly permitted improper software configurations that resulted in the storage of sensitive payment card information in clear readable text. These systemic failures exposed consumers' data to unauthorized access – in this instance, the company allegedly suffered three data breaches in less than two years. The complaint alleges that these failures, among others, resulted in fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' account information to an Internet domain address registered in Russia.

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.

[13] *FTC v. Wyndham Worldwide Corp. et al.*, Civil No. 13-1887 (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation. An appeal of the district court's decision in this matter is pending in the Third Circuit. *FTC v. Wyndham Hotels & Resorts, LLC, et al.*, No. 14-3514.

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; 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

---

[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.

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 materials directed 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 specific guidance for mobile app developers as they create, release, and monitor their apps,[20] and

---

[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.

[20] Mobile App Developers: Start with Security (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.

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") file-sharing 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.[25] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[26] average more than 2.2 million unique visits per year.

Identity theft has been the top consumer fraud complaint to the FTC for 13 consecutive years, and tax identity theft – which often begins by thieves obtaining Social Security numbers and other personal information from consumers in order to obtain their tax refund – has been an

---

[21] *See* FTC Blog, *Tax ID Theft Awareness: Tips for Tax Preparers Bear (P)repeating*, Jan. 15, 2015, *at* http://www.ftc.gov/news-events/blogs/business-blog/2015/01/tax-id-theft-awareness-tips-tax-preparers-bear-prepeating.

[22] *See* FTC Blog, *HR Professionals: Deter Tax ID Theft with an Open-Door (but Closed-Drawer) Policy*, Jan. 27, 2015, *at* http://www.ftc.gov/news-events/blogs/business-blog/2015/01/hr-professionals-deter-tax-id-theft-open-door-closed-drawer.

[23] *See Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

[24] *See Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at* http://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

[25] *See* http://www.onguardonline.gov.

[26] *See* http://www.alertaenlinea.gov.

increasing source of the Commission's identity theft complaints.[27] The Commission hosts IDTheft.gov, which provides consumers who may be victims of identity theft with important information and tools to protect themselves and assist in the recovery process.[28] We are in the midst of overhauling the website to better assist consumers.[29] And recently, the FTC hosted a series of webinars and Twitter chats as part of Tax Identity Theft Awareness Week.[30] The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.

III. THE SUBCOMMITTEE'S DATA SECURITY BILL

The Commission would like to offer a few comments on the discussion draft of the subcommittee's bill. The FTC would like to thank the subcommittee for developing and proposing enactment of a federal data security and breach notification law, which the Commission has long supported on a bipartisan basis. The Commission supports the goals of the subcommittee's data security bill to establish broadly applicable data security standards for companies and require them, in certain circumstances, to notify consumers in the event of a breach.

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)

---

[27] In 2012, tax identity theft accounted for more than 43% of the identity theft complaints, making it the largest category of identity theft complaints by a substantial margin. *See* Press Release, *FTC Releases Top 10 Complaint Categories for 2012* (Feb. 26, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/02/ftc-releases-top-10-complaint-categories-2012.

[28] *See* http://www.idtheft.gov.

[29] In response to the President's Executive Order of October 17, 2014 on Improving the Security of Consumer Financial Transactions, the FTC is developing and implementing a plan to make the recovery process for identity theft victims quicker and less burdensome. By May 15, 2015, we will overhaul IdentityTheft.gov to provide streamlined information for identity theft victims and people whose information is stolen. In later phases, we will enhance the online victim assistance process to help people take steps to recover from identity theft more easily from their computer or mobile device.

[30] *See generally* http://www.consumer.ftc.gov/features/feature-0029-tax-identity-theft-awareness-week.

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 notification and data security standards are essential to protect consumers. Second, the legislation gives the Commission jurisdiction to bring cases against common carriers and non-

---

[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/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf; Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf.

profits. This would help ensure that whenever covered personal information is collected from consumers, entities that maintain such data – such as educational institutions – adequately protect it.[32] Third, the Commission supports the provision that gives us the ability to seek civil penalties, which are an important tool to deter unlawful conduct. Under current laws, the Commission only has the authority to seek civil penalties for data security violations with regard to children's online information under COPPA, or credit report information under the FCRA.[33] By expanding the Commission's jurisdiction and giving it civil penalty authority, the bill will give us additional tools that we do not currently have.

Additionally, the bill covers important personal information – including Social Security numbers, username and password when used to obtain money or anything of value, and biometric data when used to obtain money or anything of value – regardless of whether it is associated with an individual's name. Social Security numbers alone can be used to commit identity theft, even if not paired with a name and address, especially when such numbers belong to children without credit histories.[34] Similarly, both an account username and password, and biometric data such as a fingerprint, can be used to gain access to an account, including 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

---

[32] A substantial number of reported breaches have involved non-profit universities and health systems. *See* Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities), *available at* http://www.privacyrights.org/data-breach/new.

[33] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(*l*).

[34] *See, e.g.*, ID Analytics, *The Long Con: An Analysis of Synthetic Identities* (Oct. 2014); FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft* (July 12, 2011), *available at* http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft.

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 law. 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 other 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 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,

---

[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.

the Commission has seen instances where bad actors have 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 draft bill currently protect this information.[37]

The Commission believes that data security requirements should apply to all key parts of the data ecosystem, including to devices that collect data, such as some Internet-enabled devices, as bad actors could target such devices to cause physical harm even if they do not steal any data. For example, the Commission's recent IoT report noted the security risks associated with interconnected devices such as pacemakers and automobiles. Security breach of such devices could lead to the compromise of personal information, but also raise broader safety concerns. Accordingly, general data security legislation should address risks to both personal information and device functionality.

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

[37] *See, e.g.*, Fla. Stat. § 501.171(g)(1)(a)(IV)-(V) (defining "personal information" to include medical and health insurance information); Tex. Bus. & Com. Code § 521.002(a)(2)(B) (defining "sensitive personal information" to include medical information).

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. It is also subject to judicial review under well-established standards in the APA. In other circumstances where Congress has given the Commission rulemaking authority under the APA, the agency has acted judiciously in accord with Congressional direction.[38]

Finally, the FTC believes that any trigger for providing notification should be sufficiently balanced so that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive. Notification is crucial as it is the consumer who is best positioned to monitor and 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, or 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

[38] For example, the Commission has issued the Telemarketing Sales Rule, 16 CFR Part 310, under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, as well as rules, 16 CFR Part 316, under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. § 7701 et seq.

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.