U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

March 16, 2015

TO: Members, Subcommittee on Commerce, Manufacturing, and Trade

FROM: Committee Majority Staff

RE: Hearing entitled "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015"

I. INTRODUCTION

On Wednesday, March 18, 2015, at 10:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing entitled "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015." The hearing will examine the discussion draft and provide stakeholders the opportunity to discuss how the discussion draft can be improved further to secure individual's personal information and to provide notice in the case of a breach of security to those individuals.

II. WITNESSES

Panel 1

- Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission; and,
- Clete Johnson, Chief Counsel for Cybersecurity, Public Safety and Homeland Security Bureau, Federal Communications Commission.

Panel 2

- Mallory Duncan, Senior Vice President and General Counsel, National Retail Federation;
- Jon Leibowitz, Partner, Davis Polk & Wardwell LLP, Co-Chairman of, and on behalf of, the 21st Century Privacy Coalition;
- Laura Moy, Senior Policy Council, Open Technology Institute, New America;
- Yael Weinman, Vice President for Global Public Policy and General Counsel, Information Technology Industry Council; and,
- Sara Cable, Assistant Attorney General, Office of the Massachusetts Attorney General.

III. BACKGROUND

Consumers face an increasing risk of identity theft and financial fraud created by criminals with varying motivations, but a common goal: to steal personal information for financial gain.

Currently, there are forty-seven different State laws dealing with data breach notification and twelve State laws governing commercial data security. This patchwork of State laws creates confusion for consumers looking for consistency and predictability in breach notices as well as complex compliance issues for businesses as they secure their systems after a breach. Moreover, this patchwork has not always resulted in better consumer protections and may lead to additional opportunities for cyber criminals to exploit vulnerable individuals with phishing attacks or other schemes because there is no consistent standard for data security or breach notification. Following a breach, consumers must take steps to protect their accounts and their credit by replacing their cards, updating accounts, and monitoring their credit with existing tools. In addition, consumers ultimately bear the costs of the breach through higher fees and prices.

In today's digital economy, a patchwork of State laws with varying requirements and breach notification standards is not an effective way to protect consumers and creates complex and, at times, competing or conflicting regulatory requirements for industry. The costs to consumers and the economy of these malicious data breaches are substantial, costing tens of billions of dollars and hundreds of thousands of jobs.

The robust Federal Trade Commission (FTC) and State attorneys general enforcement standard under this bill would require better security. While the FTC has tried to use enforcement to impose a security requirement, its remedies are limited and its authority is being challenged. First, the discussion draft puts companies on notice that security is required. Second, the standard is technology agnostic, but does require a company to use current, effective technologies or risk enforcement. The bill also provides both the FTC and State attorneys general with clear authority and civil penalties to pursue enforcement.

On January 27, 2015, the Commerce Manufacturing and Trade Subcommittee held a hearing on the elements of sound data breach legislation. The Subcommittee received testimony from the retail industry, a company that has suffered a data breach, the technology industry, and an academic. Members received testimony from a national industry privacy and ecommerce coalition, financial institution trade associations, several retail trade associations, and several technology and software trade associations regarding existing data security and breach notification requirements and the benefits of Federal legislation.

IV. SECTION-BY-SECTION

The discussion draft addresses the growing problem of identity theft and payment fraud by requiring covered entities to implement reasonable security measures for the type of personal information that criminals use for identity theft and payment fraud and to notify individuals in

the case of a breach of security for such personal information. The draft would establish a single Federal regime enforced by the FTC and subject to civil penalties. Additionally, State attorneys general would be authorized to enjoin violations, compel compliance, or seek civil penalties for violations of the Act. The discussion draft is limited in scope to address those categories of information that result in identity theft and payment fraud. The draft neither addresses privacy issues nor preempts existing privacy laws.

Section 1. Short Title; Purposes.

This Act may be cited as the "Data Security and Breach Notification Act of 2015." Its purposes are to protect consumers from identity theft, economic loss or economic harm, and financial fraud by establishing uniform national data security and breach notification standards for electronic data in interstate commerce

Section 2. Requirements for Information Security.

This section requires covered entities to implement and maintain reasonable security measures and practices that are appropriate to the size and complexity of the entity and the nature and scope of its activities, and to protect and secure electronic personal information against unauthorized access.

Section 3. Notification of Information Security Breach.

Following a breach of security, this section requires a covered entity that uses, accesses, transmits, stores, disposes of, or collects personal information to conduct a reasonable and prompt investigation of the breach to determine whether there is a reasonable risk that the breach has resulted in, or will result in, identity theft, economic loss or economic harm, or financial fraud.

This section requires covered entities to notify individuals affected by, or is reasonably believed to have been affected by the breach of security, unless 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. Notice is required within thirty days after the covered entity has taken the necessary measures to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

This section requires that any notice to affected individuals about a breach of security must include: 1) a description of the personal information that was, or reasonably believed to be, accessed or acquired by an unauthorized person; 2) the date range or approximate date range of the breach; 3) a telephone number or toll-free number (if the covered entity does not meet the definition of a small business concern or non-profit organization) that an affected individual may use to inquire about the breach; 4) the toll-free contact telephone number and addresses for a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis; and 5) the toll-free telephone number and Internet website for the FTC where individuals can get more information about identity theft.

This section requires covered entities to notify affected individuals of a breach of security within thirty days after the covered entity has taken the necessary measures to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. If a covered entity discovers additional individuals to whom notification is required after providing notice under this section, the covered entity shall notify such individuals as expeditiously as possible and without unreasonable delay.

This section requires a covered entity to also notify the FTC and the Secret Service or Federal Bureau of Investigation of a breach of security if more than 10,000 individuals' personal information was, or there is reasonable basis to conclude was, accessed or acquired by an unauthorized person. This section allows Federal, State, or local law enforcement to delay notification to affected individuals if it would impede a civil or criminal investigation.

This section requires third-party entities that store, process, or maintain personal information for a covered entity to promptly notify the covered entity if there is a breach of security involving the personal information. If a covered entity is acting solely as a third-party entity, the third-party entity has no other notification obligations under this section. After receiving notice from a third-party, the covered entity must then notify affected individuals.

A covered entity may contract out its notice obligation as long it is clear that the notice is sent on behalf of the covered entity.

This section provides certain accommodations for non-profits or where there is limited contact information for an individual. This section requires covered entities to notify a consumer reporting agency of a breach of security affecting more than 10,000 individuals. This section requires a service provider to notify a covered entity if it becomes aware of a breach of security involving electronic data containing personal information and can reasonably identify the sender.

Section 4. Enforcement.

This section establishes that a violation of this Act will be treated as an unfair or deceptive act or practice under the Federal Trade Commission Act and violations will be enforced by the FTC. Any covered entity that violates this Act shall be subject to the penalties and immunities provided in the Federal Trade Commission Act and as extended by this Act to common carriers and non-profit organizations.

This section allows for State attorneys general to bring enforcement actions for violations of either the security or notification requirements of this draft. They may bring civil penalties of up to $11,000 per violation.

This section establishes a maximum civil penalty of $2.5 million in cases filed by a State attorney general. Civil penalties will be annually adjusted for inflation.

This section requires that the covered entity's degree of culpability, history of prior conduct, ability to pay, effect on ability to continue to do business, and any other matters must be taken into account in determining the amount of a civil penalty.

This section provides certain process requirements so that there is not redundant enforcement between State attorneys general and the FTC.

This section provides that nothing in this Act establishes a private cause of action against a person for a violation of this Act.

Section 5. Definitions.

This section provides definitions for the following terms: breach of security, Commission, consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, covered entity, data in electronic form, encryption, non-profit organization, personal information, service provider, small business concern, and State.

Section 6. Effect on Other Laws.

This section prevents States from adopting, maintaining, enforcing, or imposing or continuing in effect any law, rule, regulation, duty, requirement, standard, or other provision related to the security of data in electronic form or notification following a breach of security with respect to a covered entity.

[*This section would not exempt a covered entity from liability under common law*. [*The parties to this staff draft have not yet reached agreement of State common law and continue to discuss the issue.*]]

This section provides that any regulations in sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 that pertain to information security or breach notification practices of covered entities are superseded by this Act.

This section provides that nothing in this subsection otherwise limits the Federal Communications Commission's authority with respect to sections 201, 202, 222, 338, and 631 of the Communications Act of 1934.

This section provides that nothing in this Act should be construed in any way to limit or affect the FTC's authority under any other provision of law.

Section 7. Effective Date.

This Act will take effect one year after the date of enactment of this Act.

V. ISSUES

The following issues may be examined at the hearing:

- What are the advantages of providing for the first time a national security standard for covered entities?

- Is the scope of personal information in the discussion draft appropriate to target identity theft and payment fraud?

- How would industries deal with fifty different security requirements? Would the discussion draft have the effect of setting a single, national standard if common claim claims are permitted under State law?

- Does the "reasonable" data security requirement appropriately protect consumers' personal information and protect business with adequate guidance?

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Paul Nagel or Melissa Froelich of the Committee staff at (202) 225-2927.