COMMITTEE ON ENERGY AND COMMERCE
Chairman Fred Upton
114th Congress

# Data Security and Breach Notification Act of 2015

***Overview of Bipartisan Discussion Draft Authored By Energy and Commerce Committee Vice Chairman Marsha Blackburn (R-TN) and Rep. Peter Welch (D-VT)***

Data breaches are a growing problem as e-commerce evolves and Americans spend more of their time and conduct more of their activities online. Technology has empowered consumers to purchase goods and services on demand, but it has also empowered criminals to target businesses and steal a host of personal data. This costs consumers tens of billions of dollars each year, imposes all kinds of hassles, and can have a lasting impact on their credit. To help protect consumers, Energy and Commerce Committee Vice Chairman Marsha Blackburn (R-TN) and Rep. Peter Welch (D-VT) have put forward a bipartisan discussion draft of the Data Security and Breach Notification Act.

The Act requires certain entities that collect and maintain consumers' personal information to secure such information and to provide notice to affected individuals in the case of a breach of security involving personal information.

**Data Security**

- The legislation would, for the first time, set a national standard for covered entities to implement and maintain reasonable security measures and practices to protect and secure personal information.
- The requirement is a technology and process neutral standard to protect consumers while being flexible enough to allow for innovation and new technologies.

**Breach Notification**

- The draft requires covered entities to conduct a good faith investigation after discovering a breach of security to determine if there is a reasonable risk of identity theft, economic loss or harm, or financial fraud.
- A covered entity is required to notify consumers about a breach of personal information unless there is no reasonable risk of identity theft, economic loss, economic harm, or financial fraud.
- The notification must be provided to consumers as expeditiously as possible and not later than 30 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.
- Delay of notification to individuals is permitted for law enforcement or national security purposes.

**Personal Information**

- The draft defines personal information to include personal information tied to ID theft and/or payment fraud, such as: SS#; financial account credentials; other account credentials, including biometric, for accounts that allow consumers to obtain money or make purchases; name coupled with drivers license or other government-issued unique identification number; amongst others.

**Enforcement of the National Standards**

- The draft's Security and Notification standards are designed to create a uniform national policy – the scope of which members continue to discuss – replacing the patchwork of state and territory laws.
- A violation of the Act is an unfair and deceptive act or practice under the FTC Act and violations may be enforced by the FTC or state attorneys general.

- Both the FTC and state attorneys general have the power to obtain civil penalties for violations of the data security and breach notification requirements.
- No private right of action is extended under the draft.

**Maintenance of and Interaction With Existing Consumer Protections**

- The draft covers entities within the FTC's general jurisdiction but does not include entities subject to existing data security and breach notification regulatory regimes (e.g. HIPAA covered entities).
- For consistency, the draft provides the FTC jurisdiction over the data security and breach notification practices of non-profits, telecommunications, cable, and satellite providers.
- The Data Security and Breach Notification Act does not impact or preempt privacy law.