FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

March 23, 2015

To: Subcommittee on Commerce, Manufacturing, and Trade Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Markup of H.R. ___, the "Data Security and Breach Notification Act of 2015"

On Tuesday, March 24, 2015, immediately following the conclusion of opening statements for the Environment and Economy Subcommittee Markup (5:00 p.m.) in room 2123 of the Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will meet in open markup session for opening statements on "H.R. ___, Data Security and Breach Notification Act of 2015." The Subcommittee will reconvene on Wednesday, March 25, at 12:00 p.m. in room 2123 of the Rayburn House Office Building.

SUMMARY OF H.R. ___, THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2015[1]

The discussion draft imposes security and breach notification requirements on covered entities, which is defined in Section 5 as all entities over which the Federal Trade Commission (FTC) currently has authority, common carriers subject to the Communications Act, and non-profit organizations.

A. Purpose of the Bill

[1] The draft that will be marked-up is virtually identical to the draft that was the subject of the legislative hearing held last Wednesday, March 18, 2015.

Section 1 of the draft explicitly states that the purposes of the bill are to create uniform standards to protect consumers from financial harms and to preempt state laws, including common law,[2] relating to data security and breach notification.

B. Data Security

Section 2 of the discussion draft requires covered entities to maintain reasonable data security, appropriate for the business and its activities, to protect personal information as defined in the draft.

C. Breach Notification Requirements

Section 3 of the discussion draft establishes the obligations of covered entities in the event of a breach of electronic data. Following a data breach, covered entities would be required to conduct an investigation to determine whether the breach has resulted in identity theft or other financial harm. Notice to affected individuals is required unless there is no reasonable risk of such harm, and must be made within 30 days after the scope of the breach has been determined and the security holes have been plugged. If the information of 10,000 or more individuals was accessed, the FTC and the Secret Service or FBI must also be notified.

Notice to individuals is required to be made through regular mail or e-mail, if e-mail is the business's primary method of communication with its customers. Notice must include a description of the information accessed, the date range of the breach, a telephone number for affected individuals to obtain information about the breach, the contact information for a credit reporting agency, and the telephone number and website for the FTC. If the breached entity does not have current contact information for 500 or more individuals, the breached entity must also provide substitute notice through e-mail and notice on the breached entity's website.

Third party entities that store or process information on behalf of a covered entity must provide notice to the covered entity and may, if agreed in writing in advance, provide direct notice to affected individuals. Direct notice by third parties must indicate that the notice is being provided on behalf of the covered entity.

The notification requirements for service providers is limited to providing notice to a covered entity that connects to or uses the service, if that covered entity can be reasonably identified. Service providers are defined as communications service providers to the extent that they act as so-called "dumb pipes" in that they provide simple data transmission or transient data storage.

D. Federal and State Enforcement

[2] The words "common law" appear in brackets in this section. A note in Section 6 of the draft states that the parties to the draft have not yet agreed on whether common law will be preempted by this bill.

Section 4 of the discussion draft provides for enforcement of this proposed law by the FTC and allows the agency to seek civil penalties. The bill also includes a savings clause in Section 6 that explicitly states that nothing in this act limits or affects the authority of the FTC under any other provision of law.

Section 4 also provides for enforcement of this act by state attorneys general in cases in which the state attorney general believes that residents of the state have been adversely affected by violations of Sections 2 or 3. All legal actions brought under this act would be required to be brought in federal court. State attorneys general may obtain an injunction, compel compliance, or obtain civil penalties. The maximum penalties available to state attorneys general is $2.5 million for each violation of the data security requirement and $2.5 million for all violations of the notification requirements. These limits do not apply to the FTC. This section also provides for intervention by the FTC at the agency's discretion.

E. Personal Information

Section 5 of the discussion draft provides a definition of personal information covered by the bill, among other definitions. Personal information includes data that can directly lead to financial harm, such as an individual's name in combination with driver's license number, a financial account number with a password or other access code, another unique account identifier with a security access code, or a full social security number. Personal information also includes, for telecommunications carriers or interconnected VoIP providers, certain telephone call information, such as the location of the call, the destination number of the call, and the time and duration of the call.

Personal information does not include data that is encrypted or otherwise rendered unusable or information obtained from public sources.

F. State Preemption

The discussion draft includes a state preemption provision in Section 6. The provision as written would preempt all state data breach and breach notification laws, and preempts state consumer protection laws as they are applied to data security and breach notification. In addition, the preemption provision includes language that, according to United States Supreme Court precedent, expressly preempts state common law as applied to data security and breach notification.[3] However, section 6 also includes a paragraph stating that state common law is not preempted. The scope of the state preemption is still under discussion between the parties to the discussion draft.

G. Effect on Telecommunications and Television Services

Section 6 of the discussion draft includes a provision preempting data security and breach notification requirements that currently apply to telecommunications, satellite, and cable companies under the Communications Act and corresponding regulations. The bill potentially

[3] *Northwest, Inc. v. Ginsberg*, 134 S. Ct. 1422 (2014).

preempts the privacy provisions in the Communications Act and the corresponding regulations as well. The language attempts to limit the preemption to only preempt certain provisions that cover privacy and data security as they apply to "securing information in electronic form from unauthorized access."

Telecommunications providers must comply with the data security requirements under Section 2 of the draft with respect to certain telephone call data. Cable and satellite providers, however, have no security obligations under the bill. In addition, while certain telephone call information must be secured, a breach of this information would not trigger notification because it would not directly lead to identity theft or other financial harm.