January 27, 2015

The Honorable Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing and Trade
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing and Trade
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

The undersigned trade associations and business groups representing hundreds of thousands of U.S. companies from a wide variety of industry segments strongly supports enactment of a truly uniform national data breach notification law. Protecting individuals' sensitive personal information from theft or illegal uses has been and will continue to be a top priority for the business community. Federal data breach notification legislation would help businesses by reducing the complexity associated with complying with 47 state data breach laws.

As you continue drafting data breach notification legislation, we urge you to be mindful that any such legislation, to be workable and effective, must recognize that both consumers and U.S. businesses are victims of crimes that give rise to a data breach. To that end, we would like to take this opportunity to share with you our thoughts on specific provisions that should be included in the bill.

Preemption

We support a true national, uniform standard for data breach notification. With 47 states having already enacted data breach notification statutes, the only reason for Congress to act now is to expressly preempt obligations under related state and common laws to ensure uniformity of the federal act's standards and the consistency of their application across jurisdictions. A weak or poorly drafted preemption provision would accomplish little other than adding a new federal law to the state statutes and common laws already in effect, resulting in a confusing patchwork of requirements and enforcement regimes that would undermine the purpose and effectiveness of this legislation.

Breach Notification Timing

We agree that consumers should be notified in a timely manner after the occurrence of a reportable data breach. However, rather than specifying a specific timeframe, we recommend language—consistent with nearly all of the state breach notification laws—permitting greater flexibility given the complexities of responding to a data breach, All entities that suffer a breach, whether government agencies, nonprofits or commercial businesses, must first and foremost secure and restore the integrity of any breached system before notifying the public of their

vulnerability or else they will simply face continual cyber-attacks to further exploit the breached system. Additionally, breached entities must conduct extensive forensic analyses, often with the assistance of law enforcement, to determine which data may have been compromised and the identity of any potentially affected individuals. We therefore suggest the Subcommittee consider, as a model, the timeliness of notice provisions in S. 1193, in which notifications would be required to be made "as expeditiously as practicable and without unreasonable delay," while permitting breached entities reasonable time following a breach to restore the integrity of their systems, determine the scope of the breach, and identify affected individuals to be notified.[1]

Enforcement

If the FTC—acting on behalf of the federal government—exercises its right to enforce what would be federal law, then the states should be estopped from pursuing any action based on the "same or related acts" upon which the FTC prosecution is based. For example, S. 1897, adopts such a provision.[2] All enforcement actions should be filed in the appropriate federal district court.

When state enforcement is permitted, the legislation should only authorize an enforcement action under the new federal law to be brought by the state attorney general. The legislation should curtail the ability of state attorneys general to utilize contingency fee arrangements with private attorneys to enforce the Act or to litigate claims on behalf of their constituents.

Liability

We urge you to recognize that an entity that suffers a data breach is often also the victim of a crime. Therefore, the main focus of any liability provision should be on the bad actor. Rather than applying a strict liability standard, the severity of the conduct must be a factor in assessing liability and any civil penalties. Specifically, we recommend that minor technical violations should not result in either civil penalties or liabilities. Given the complexity and expense of responding to a data breach, we caution that a flawed liability provision would further penalize an entity that is a victim of data breach by drawing away valuable resources necessary to fix the breach, notify customers, and augment existing security measures.

We look forward to working with you and your Subcommittee colleagues on this important legislation.

Sincerely,

Consumer Data Industry Association
Interactive Advertising Bureau
National Business Coalition on E-Commerce and Privacy
National Retail Federation
U.S. Chamber of Commerce

[1] Section 3(c) of S. 1193 (113th Congress).
[2] Section 203(c)(5) of S. 1897 (113th Congress).