

CHAMBER OF COMMERCE  
OF THE  
UNITED STATES OF AMERICA

R. BRUCE JOSTEN  
EXECUTIVE VICE PRESIDENT  
GOVERNMENT AFFAIRS

1615 H STREET, N.W.  
WASHINGTON, D.C. 20062-2000  
202/463-5310

April 15, 2015

The Honorable Fred Upton  
Chairman  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Frank Pallone, Jr.  
Ranking Member  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Upton and Ranking Member Pallone:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, and dedicated to promoting, protecting, and defending America's free enterprise system, supports enactment of a truly uniform national data breach notification law, but we have serious concerns about multiple provisions in H.R. \_\_\_\_, the "Data Security and Breach Notification Act of 2015," which is scheduled to be marked up in your Committee.

**Preemption**

While the Chamber strongly supports the intent of Section 6 to preempt state law regarding data security, we strongly oppose Section 6(b). That provision would specifically maintain a covered entity's liability under state common law. This provision jeopardizes the legal sustainability of what could be an otherwise effective preemption clause. As currently drafted, this preemption provision would accomplish little more than add a new federal law to the myriad state common law causes of action that potentially impact data security and breach notification litigation. This would only continue the confusing patchwork of requirements and enforcement regimes related to data security and breach notification. Ultimately, it would undermine the purpose and effectiveness of the legislation and be a boon to the burgeoning trial lawyer involvement in data security and breach notification related litigation.

Moreover, by not preempting state common law, Section 6(b) would continue to allow class actions based on state common law. In effect, this would serve as an end-run around the legislation's purported limitation on private causes of action. Furthermore, the Chamber is also concerned that the legislation's weak preemption provision may result in an inconsistent assortment of court-ordered data security standards.

## **Enforcement and Liability**

The Chamber also has very strong concerns about the legislation's enforcement regime. The bill's current structure sets up a duplicative and confusing set of enforcement procedures including enforcement by both the Federal Trade Commission and state attorneys general (many of whom use outside contingency fee counsel). Under the bill's current language, companies would not be able to obtain guidance from the FTC to ensure that they are in compliance with what the agency considers to be reasonable security practices. Yet, under Section 4(a)(1)'s "straight-to-fines civil penalty authority" provision, the FTC could immediately impose civil penalties even though companies may not be aware they are out of compliance until the penalty is levied. Currently, under Section 5 of the FTC Act, the agency must issue a cease-and-desist order before being permitted to impose a fine for a violation of the Act; unfortunately this legislation does not follow a similar approach. Accordingly, the Chamber strongly recommends amending Section 4(a)(1) to eliminate the straight-to-fines civil penalty authority regarding violations of Section 2 (i.e., Requirements for Information Security).

Furthermore, the fact that the legislation includes an express grant of authority to state attorneys general to enforce its provisions is extremely problematic for multiple reasons. First, the FTC cannot stop a state AG's litigation under the bill, even if the state AG is attempting to enforce a standard inconsistent with those promulgated by the FTC. The bill's FTC intervention language is not strong enough in that it would not allow the FTC to take over the litigation and potentially dismiss it. Furthermore, the legislation does nothing to limit the ability of state AGs to utilize outside contingency fee counsel to enforce the bill's provisions. This is a significant litigation-expanding earmark in support of the plaintiff's contingency fee trial bar. Accordingly, the state AG enforcement language should be eliminated from the legislation in its entirety, or at a minimum 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 should be curtailed significantly.

Given the complexity and expense of responding to a data breach, the Chamber cautions that the bill's flawed liability provisions would further penalize an entity that is itself a victim of data breach by drawing away valuable resources necessary to fix the breach, notify customers, and augment existing security measures. Providing potentially massive damages to the Federal Trade Commission along with providing state attorneys general with the ability to impose penalties up to \$5,000,000 (by combining violations of Section 2 and Section 3 of the bill) seems disproportionate and would place an excessive financial burden on business, especially smaller ones. Therefore, the Chamber urges you to lower the cap to a much more reasonable amount as well as to cap the amount of liability which may be imposed by the FTC. The Chamber also recommends striking "economic harm" in Section 1(b)(1) because the term is subjective. In addition, the FTC should be required to prove "substantial consumer harm" in order to pursue violations of the consumer protections delineated in Section (1)(b)(1).

## **Personal Information**

The Chamber also recommends several changes regarding the bill's treatment of "personal information." We urge the Committee to delete Section 5(10)(A)(i)(II)(aa) because

this information often is widely available. For example, it is our understanding that voter registration information given to campaign volunteers often contains data that would trigger this section. In addition, in Section 5(10)(A)(iii), the Chamber seeks to ensure that “electronic identification numbers” excludes dynamic IP addresses. In the same section, the Chamber also recommends striking “any other thing of value” due to the vague nature of that term.

### **Data Security**

Given the FTC’s expansive and vague interpretation of “reasonableness” in the various data security suits it has brought, the Chamber recommends consideration of ways to further guide the FTC’s efforts in this area. One possible solution is to require that the FTC prove that the covered entity engaged in “unreasonable” security standards constituting an unfair or deceptive act or practice within the meaning of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

### **Notification of Information Security Breach**

The Chamber is also troubled by the notification of information security breach requirements contained in the bill. We recommend amending Section 3(a)(5) to require notice to the FTC only for breaches involving more than 10,000 individuals that require notification to consumers.

Section 3(a)(3) says notification is not required if there is “no reasonable risk that the breach of security has resulted in...” To avoid over-notification, the presumption should be reversed and require notice only when there is a breach of security that creates a significant risk of identity theft, economic loss, or financial fraud.

For greater clarity, the Chamber recommends adding “by a covered entity” after “discovery” in Section 3(a)(1). Additionally, notice and liability should be tied solely to unauthorized acquisition, not mere access.

For the Chamber to support this legislation, the issues identified above must be resolved. The Chamber does look forward to working with you and your colleagues to address our concerns with the bill as it proceeds through the legislative process.

Sincerely,

A handwritten signature in black ink, appearing to read "R. Bruce Josten", written in a cursive style.

R. Bruce Josten

cc: Members of the Committee on Energy and Commerce