

August 19, 2010

The Honorable Jay Rockefeller  
Chairman  
Committee on Commerce, Science and  
Transportation  
United States Senate  
Washington, D.C. 20510

The Honorable Mark Pryor  
Chairman  
Subcommittee on Consumer Protection,  
Product Safety, and Insurance  
United States Senate  
Washington, D.C. 20510

**Re: S. 3742, Data Security and Breach Notification Act of 2010**

Dear Senators Rockefeller and Pryor,

The undersigned industry associations, business groups and coalitions, together representing the vast array of businesses that make the U.S. the leading economy in the information age, write this letter to express serious concerns which we have regarding the text of S. 3742, the Data Security and Breach Notification Act, introduced on August 5, 2010.

We appreciate the time and effort you and your staff have undertaken to draft legislation this Congress, building on the work by the Commerce Committee in previous Congresses. We also recognize that other committees are considering data security legislation, including the Judiciary Committee, which has reported S. 1490, the Personal Data Privacy and Security Act, and the Banking Committee, to which S. 3579, the Data Security Act, was recently referred. Consistent with the bill's purpose, as S. 3742's short title implies, the principal industry position with respect to all federal data security legislation is the same, in that it should be focused on two important objectives: 1) ensuring adequate federal application of data security standards across industries, recognizing compliance with existing federal standards, and 2) providing a set of uniform, national standards with respect to data security breach notification requirements, given that nearly all states have already enacted their own separate standards. Since 2005, the undersigned have consistently supported such carefully tailored and focused legislation, and we believe that the public will benefit enormously by the enactment of such legislation.

We believe that there are other provisions, including but not limited to those designed to regulate "information brokers", that are not only extraneous to the underlying goal of promoting data security standards, but are actually counter-productive. It is notable, for example, that none of the 46 state laws include this kind of additional regulation, as states have rightly focused, as we believe Congress should, on workable standards regarding data security and data breach notification. Most importantly, the Obama Administration's strategy for securing cyberspace calls for increased authentication of an individual's identity when accessing networks and commercial services offered on the Internet. Industry supports this goal, however, including the information broker provisions in S. 3742 will decrease the effectiveness of information-based authentication systems that help reduce and prevent fraud and identity theft in the first place.

Beyond what we believe the proper scope of data security legislation should cover, there are a number of other important issues that we wish to raise with you as the Committee and the Senate consider upcoming legislation. As the process proceeds, we would very much like to work with you and your staff to address each of these issues as the legislation is refined for potential consideration by the full Senate. Specifically, we ask you to seriously consider the following concerns:

- **Preemption:** Our principal concern with S. 3742's preemption provision is that its effort to preserve state law exceptions within the federal preemption clause effectively swallows the rule. Allowing continued application of state laws on the same subject matter as the federal act would undermine the purpose of enacting a purportedly preemptive law. Any federal legislation in this area therefore should be unequivocally preemptive or should not be enacted.

- **Harmonizing Federal Data Security Laws:** Entities that are subject to existing federal data security standards<sup>1</sup> should not be subject to duplicative and potentially conflicting standards promulgated by the Federal Trade Commission (FTC). Additionally, the FTC should not be empowered with "super-agency" authority to determine the sufficiency of the other federal standards to determine who is deemed to be in compliance with the FTC's standards.

- **Enforcement:** S. 3742 would authorize state attorneys general (AGs) to enforce the Act's provisions, but it also unnecessarily authorizes any unnamed "official or agency of a state" to bring an enforcement action in federal court. This language would jump-start endless unnecessary litigation by entities that Congress neither defines nor contemplates. State AGs are uniquely capable of carrying out their mandate to protect all the citizens of their state, and extending federal litigation authority to unnamed state officials and agencies would set a counter-productive precedent whereby literally hundreds of potential plaintiffs would be authorized to sue in federal court on the same issues involving the same facts as litigated by both the federal government and their state AGs. Additionally, the civil penalty provisions of S. 3742 are excessive, especially in this economic environment, and should be reconsidered in light of the fact that most companies suffering breaches of security are themselves the victims of a crime. Moreover, liability in any form must, of necessity, be accompanied by a demonstration of "actual harm." Otherwise, too many unjustified lawsuits will inevitably result. For example, it is unclear what actual harm would trigger a violation of section 2's data security requirements, leaving it up to the courts to determine what Congress should more appropriately decide.

- **FTC Website Publication of Breaches:** S. 3742 would grant the FTC broad discretion to publicize on its website any breach of which it is notified. Because the bill requires covered entities to notify the FTC of all breaches, this FTC authority could well result in the global publication of any breach of any size, unnecessarily alarming unaffected consumers, hampering statutorily-required efforts to notify those consumers actually affected, and inflicting "piling on" damage to the reputations of companies that may have suffered unavoidable criminal breaches and handled them in accordance with best practices.

- **Other Obligations Following Breaches:** While the FTC or another agency may propose that breached entities adopt reasonable remedial steps for affected individuals, the Act should not specify the particular remedies an entity must adopt. Such specificity may preclude more advanced and effective alternatives for consumers that are also less expensive. In this respect, rigid statutes may not serve consumer interests and would also impose unfair, unfunded mandates on businesses suffering breaches. Ultimately, an entity that has suffered a breach should take remedial steps that are proportional to the level of risk of harm. The principles of reasonable and proportional remedies are reflected elsewhere in S. 3742 but not in this provision.

- **Over-Delegation of Congressional Authority Allows FTC to Expand Scope:** S. 3742 grants the FTC broad discretionary authority to expand unilaterally the definition of

---

<sup>1</sup> See Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and Health Insurance Portability and Accountability Act.

“personal information”, which defines the scope of the Act’s coverage. Under this provision, the statute could be stretched to cover information that – even if breached – would not result in economic harm to consumers. Permitting a future FTC to expand a definition that is at the core of the applicability of the proposed federal statute is an inappropriate delegation of Congressional authority to the rulemaking capacity of an enforcement agency. This critical function should require Congressional action and not be abdicated to unelected officials.

We hope these comments on S. 3742 will be received in the manner with which they are submitted: as a reflection of the desire of the signatories to promote the adoption of effective federal legislation which, once and for all, would establish national “rules of the road” for companies to follow in the event of data breaches. We look forward to working with you and other Senators that have shown leadership on these data security issues as you consider legislation over the remainder of this Congress.

Sincerely,  
American Financial Services Association  
Consumer Data Industry Association  
Financial Services Roundtable  
National Business Coalition on  
E-Commerce and Privacy  
National Retail Federation  
Shop.org  
U.S. Chamber of Commerce

cc: The Honorable Harry Reid  
The Honorable Mitch McConnell  
Members of the Committee on Commerce,  
Science and Transportation