November 29, 2016

The Honorable Paul Ryan
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, DC 20515

Dear Speaker Ryan and Leader Pelosi,

The undersigned associations, representing over a million businesses, strongly urge the House of Representatives to resist calls to consider H.R. 2205 or modified versions of this bill during the lame duck session. This legislation does not have the support of a broad consensus of the industry sectors currently subject to the jurisdiction of the Federal Trade Commission (FTC), an agency whose regulatory and enforcement authority would be greatly expanded under this proposal.

Our industries take data security practices and breaches of security very seriously. The rampant nature of threats to our data is a top challenge for businesses of all kinds, as well as for government agencies and private citizens. We are aware that the Financial Services Roundtable (FSR) has received some tepid support outside of its industry for its effort to come up with a draft federal data security and breach notification bill to add to the fifty-one such laws that currently cover forty-seven states and four other jurisdictions (including the District of Columbia and Puerto Rico).

We have concerns about the draft proposal they have put together, based largely on the text of H.R. 2205, and the negative impact it will have on businesses throughout the economy – particularly Main Street businesses. The FSR draft has not been introduced as a bill by a member of the House nor considered by the House Energy and Commerce Committee. That committee has jurisdiction over businesses subject to the FTC and oversight authority over the Commission, including its enforcement of data security practices with respect to the vast array of business that would be subject to this proposed legislation.

In our view, there are four key principles that a federal data security and breach notification bill should follow, and that the FSR draft does not meet:

1. **Establish Uniform Nationwide Law**: First, with the fifty-one inconsistent breach laws currently in effect, there is no sound reason to enact federal legislation in this area unless it preempts the existing laws to establish a uniform nationwide standard so that every business and consumer knows the singular rules of the road. One federal law applying to all breached entities would ensure clear, concise and consistent notices to all affected consumers regardless of where they live or where the breach occurs. Simply enacting a different fifty-second law would not advance data security or consumer notification; it would only create more confusion.

Principle Not Met: The FSR draft includes exceptions in its preemption language that would allow courts to create different standards for data security and breach notice in each state based on the common law – and would open up businesses to class action lawsuits based on these inconsistent standards.

2. **Promote Reasonable Data Security Standards**: Second, data security requirements in a federal law applicable to the broad array of businesses under FTC jurisdiction should be based on a standard of reasonableness. American businesses are remarkably diverse in size, scope and operations. A *reasonable* standard would allow the FTC the right degree of flexibility while giving businesses the guidance they need to comply.

   Principle Not Met: The FSR draft would mandate a laundry list of prescriptive data security requirements that would not work well, given the diversity of covered businesses, nor would be able to adapt to rapidly changing security threats. Furthermore, the prescriptive requirements in this draft were designed by banking regulators for financial institutions, and they are inappropriate to apply to a broad swath of unrelated companies subject to FTC jurisdiction and enforcement, which is wholly different than the enforcement regime under which banks come into compliance with their regulatory guidance. It should not be the case that Main Street businesses face mandatory data security standards in this bill while others remain subject only to guidance that is not mandatory.

3. **Maintain Appropriate FTC Enforcement Regime**: Third, the FTC should not be granted overly-punitive enforcement authority that exceeds its current legal framework. Currently, absent a completed rulemaking, the FTC must bring an action requiring a business to stop behavior that the FTC deems to be a violation of law. The FTC cannot seek civil penalties until it establishes what a violation is. That process gives businesses notice of the FTC's view of the law and is fair given the breadth of the FTC's discretion to determine what is legal.

   Principle Not Met: The FSR draft gives the FTC authority to impose penalties right away – to go straight to fines – without first establishing through a rulemaking or judicial clarification what constitutes a violation. That is a dramatic expansion of the FTC's authority and is unfair to Main Street businesses to which it would apply.

4. **Ensure All Breached Entities Have Notice Obligations**: Finally, every business should have an obligation to notify consumers when it suffers a breach of sensitive personal information that creates a risk of financial harm. Informing the public of breaches can help consumers take steps to protect themselves from potential harm.

Moreover, the prospect of public disclosure of breaches creates greater incentives for all businesses handling sensitive personal information to improve their data security practices. Creating exemptions for particular industry sectors or allowing them to shift notification burdens onto other businesses will weaken the effectiveness of the legislation, undermine consumer confidence, ignore the scope of the problem, and create loopholes criminals can exploit.

Principle Not Met: The FSR draft creates exemptions for favored industries and shifts liability and notification burdens to our member businesses that rely on those industries, which is unjustified when the breach happens at another business.

These four principles are important to ensure that any data security and breach notification legislation advanced in Congress does not overly burden business, does not impose unfair burdens, and does not pick regulatory winners and losers among differing business sectors in the process. We urge you to exercise your leadership to find legislation that can meet these principles. But, any such process needs to include input from *all* affected industries and from businesses of all sizes. Otherwise, it risks imposing unfair and/or crippling burdens which, unfortunately, the FSR draft does (while exempting its own members from such burdens).

For the reasons above, we oppose the FSR draft proposal. We hope that you will consider these concerns as the debate on data security and breach notification legislation continues, and we look forward to a continued constructive dialogue with you on these matters.

Sincerely,

American Hotel & Lodging Association
International Franchise Association
National Association of Convenience Stores
National Association of Realtors
National Association of Truck Stop Operators
National Council of Chain Restaurants
National Grocers Association
National Retail Federation
Society of Independent Gasoline Marketers of America
U.S. Travel Association

cc: Members of the House of Representatives