March 7, 2018

The Honorable Blaine Luetkemeyer
Chairman, Subcommittee on Financial Institutions and Consumer Credit
House Committee on Financial Services
Washington, DC 20515

The Honorable Lacy W. Clay, Jr.
Ranking Member, Subcommittee on Financial Institutions and Consumer Credit
House Committee on Financial Services
Washington, DC 20515

RE: Hearing on "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

Dear Chairman Luetkemeyer and Ranking Member Clay,

The undersigned associations, representing over a million businesses in industries that directly serve American consumers, sent a letter to you on February 13, 2018, laying out four critical principles that any federal legislation on data security and breach notification should meet. These include establishing a nationwide law, setting data security standards reasonable and appropriate for the covered businesses, maintaining an appropriate enforcement regime, and ensuring all breached entities have notice obligations.

With these principles in mind, we have reviewed the draft legislation that Chairman Luetkemeyer and Representative Carolyn Maloney have circulated. We have some significant concerns regarding this draft as set forth in greater detail below:

- **Breach Notice:** The draft bill does not ensure that ***all*** breached businesses have obligations to investigate and provide notice to regulators and consumers of their breaches. Instead, the draft carves out exceptions from notice for three categories of businesses: "third parties;" "service providers;" and a large category of financial institutions. For example, the bill creates an exemption for "service providers" that is not found in any state breach notification laws but, as defined, could apply to virtually any third-party service that handles data. The draft bill does not require "service providers" to even investigate the nature and scope of a suspected data breach, ensuring they will never *know* whether personal information is acquired in their breaches of security. Consequently, these breached businesses will never have to notify anyone at all. Exempting businesses from investigatory and notice obligations and, in some cases, requiring other businesses to undertake those notice obligations for them, is fundamentally unfair and undermines data security efforts in the U.S. Exempted business will have reduced incentives to protect data if they are not required by federal law to shine a light on their breaches. The fact that the draft legislation gives these exempted businesses preemption from any states that might want to require them to provide notice under state laws would effectively shield these breached businesses from *ever* disclosing their breaches.

- **Data Security:** The draft legislation sets data security requirements that are unreasonable and inappropriate for millions of commercial businesses. Mandating a checklist of specific requirements that all businesses must meet to comply with a federal data security statute does not work for the millions of diverse businesses across the nation that will be subject to prescriptive obligations inappropriate for the nature of their operations. These businesses vary tremendously in size, complexity, sophistication, the type of data they touch and the volume of data they exchange. According to data security experts who have testified before Congress in recent years, effective data security standards use a risk-based approach applying the highest security standards to the most sensitive data at the greatest risk. A one-size-fits-all standard misses the mark on this critical point. The draft legislation itself seems to partially recognize this problem by exempting financial institutions from its data security requirements, but doesn't fully recognize it because the bill also applies security requirements designed for banks onto businesses with less sensitive data. Rather than establishing a check list, the bill should employ, as the Federal Trade Commission (FTC) does, a flexible, reasonable standard for data security that could be applied appropriately to each kind of business handling personal information.

- **FTC Enforcement:** The draft legislation modifies the FTC's traditional enforcement powers so that its actions can be punitive and the Commission could exact fines *even before* the specifics of the data security standards it is applying have been established. That breaks with over one hundred years of agency enforcement practices and means that businesses could be fined that could not have known what they were required to do to avoid those fines. The bill should maintain an appropriate FTC enforcement regime consistent with the agency's long-standing traditions.

The above are a few of the fundamental concerns we have with the approach to data security taken by the draft legislation. We also have concerns that the legislation: sets an "immediate" standard for notice which is not a legal standard we have seen employed and may be unachievable; does not allow practical ways for breached systems to be secured or for law enforcement to seek a delay prior to requiring public notice to be given; requires notice in states where the breached business may not be aware any affected consumers reside; inappropriately requires notice to private businesses as though they are federal regulators; and allows financial institutions to provide their customers with inaccurate information in the event of a breach.

In light of these many concerns and the importance of this issue, we strongly urge you to take the time to fully consider all of these and other issues with the draft and work through them with stakeholders prior to moving to a markup. We appreciate the process and consideration that Chairman Luetkemeyer and Congresswoman Maloney have given to these issues to date, and believe more discussion and work is needed to produce legislation that will be effective and fair.

We appreciate your consideration of our views and we look forward to a continued constructive dialogue with you on these matters.

Sincerely,

International Franchise Association
National Association of Convenience Stores
National Association of Truck Stop Operators
National Council of Chain Restaurants
National Grocers Association
National Restaurant Association
National Retail Federation
Petroleum Marketers Association of America
Society of Independent Gasoline Marketers of America
U.S. Travel Association

cc: Members of the U.S. House of Representatives