February 13, 2018

The Honorable Blaine Luetkemeyer
Chairman
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
Washington, DC 20510

The Honorable Willliam Lacy Clay
Ranking Member
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
Washington, DC 20510

RE: Hearing on "Examining the Current Data Security And Breach Notification Regulatory Regime"

Dear Chairman Luetkemeyer and Ranking Member Lacy Clay,

The undersigned associations represent over a million businesses in industries that directly serve American consumers. Our organizations appreciate the Committee calling a hearing to examine the current data security and breach notification regulatory regime. Our members are committed to protecting their customers' data with effective data security practices and take the risk of breaches of security very seriously. In addition to the financial services companies under the Committee's jurisdiction and our members' businesses, the rampant nature of threats to consumer data is a challenge for businesses of all kinds. This includes companies that support communications with consumers and facilitate the acceptance of their forms of payment, as well as for professional organizations, health care institutions and government agencies.

Every industry sector – whether consumer-facing or business-to-business – suffers data security breaches that may put consumer data at risk. Less well known, however, is that three sectors in particular account for more than half of all breaches (i.e., security incidents with confirmed data losses) according to the 2017 Verizon Data Breach Investigations Report: financial services (24.3% of all breaches); healthcare (15.3%); and the public sector (e.g., governmental entities) (12.4%). According to this report, well above 80% of all breaches in 2016 occurred *outside* of the industries represented by the signatories to this letter, whose businesses typically handle less sensitive data than the sectors accounting for most breaches.

To protect consumers comprehensively, wherever breaches occur, Congress should ensure that any federal breach notification law applies to *all* affected industry sectors and leaves no holes in our system that would enable some industries to keep the fact of their breaches secret. Under the breach legislation reported by the House Financial Services Committee last Congress, however, Equifax would have been exempt from the bill's provisions along with banks, credit unions and other entities that qualify as "financial institutions" under the Gramm Leach Bliley Act (GLBA). The absence of breach notice requirements for entities accounting for roughly a quarter of all security breaches annually would have left millions of Americans unaware of their potential risks of financial harm and identity theft. The exemption of Equifax and other financial services companies from the requirements of that bill would have created particularly weak

public policy given that the same bill provided those companies with preemption from the requirements of state laws.

Considering the widespread risk of data breaches afflicting all American industries and our governmental institutions, there are four key principles we support in federal data security and breach notification legislation:

1. **Establish Uniform Nationwide Law**: First, with the fifty-two inconsistent breach laws currently in effect in 48 states and 4 federal jurisdictions, 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-third law on this subject would not advance data security or consumer notification; it would only create more confusion.

2. **Promote Reasonable Data Security Standards**: Second, data security requirements in a federal law applicable to a broad array of U.S. businesses should be based on a standard of reasonableness. America's commercial businesses are remarkably diverse in size, scope and operations. A reasonable standard, consistent with federal consumer protection laws applicable to businesses of all types and sizes, would allow the right degree of flexibility while giving businesses the appropriate level of guidance they need to comply. Legislation taking this approach also would be consistent with the data security standard now used by the Federal Trade Commission (FTC) and nearly all state laws that include data security requirements in their breach notification statutes.

3. **Maintain Appropriate FTC Enforcement Regime**: Third, federal agencies should not be granted overly-punitive enforcement authority that exceeds current legal frameworks. For example, 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.

4. **Ensure All Breached Entities Have Notice Obligations**: Finally, businesses in every affected industry sector should have an obligation to notify consumers when they suffer a breach of sensitive personal information that creates a risk of identity theft or 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 breached entities to shift their notification burdens onto other businesses will weaken the effectiveness of the legislation, undermine consumer confidence, ignore the scope of the problem, and create loopholes that criminals can exploit.

We note that a group of organizations led by the Financial Services Roundtable (FSR) wrote to the House Energy and Commerce Committee on January 4, 2018, relaying the elements of legislation that those groups favor. The FSR letter advocated for a "flexible, scalable" data security standard that included factors such as the "size and complexity" of a business, the "cost of available tools to secure data," the "sensitivity" of the information the company maintains, and "guarantees" that small businesses are not excessively burdened. The reasonableness standard endorsed by the FTC that the undersigned organizations support already meets all of those criteria. However, as soon as laws mandate specific data security requirements for businesses, they become inflexible and burdensome for smaller entities, and outdated and inadequate for larger or more sophisticated businesses. We appreciate that the FSR-led letter appears to agree with us on this point.

We are also pleased that the FSR-led letter appears to agree with our principle on breach notification requirements for entities handling information that, if breached, may cause individuals to become victims of financial harm or identity theft. Their letter calls for a "notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators." In the past, this Committee's breach legislation has exempted businesses in industries such as telecommunications, financial services, and data storage from required consumer notice when they are breached. That certainly would not meet the language of the FSR-led letter and is not acceptable to our organizations either. While some businesses subject to GLBA have asked for exemptions from notice obligations in new legislation, those requests raise significant problems given that GLBA does not require breach notification.[1] No industries are exempt from the attention of data thieves and no industries should be exempt from a statutory requirement to provide notice to consumers when they have breaches. Legislation should not serve as cover for giving breached businesses the ability to keep secret their own breaches and the risks of harm to affected individuals.

The four principles above, which are supported by the undersigned organizations, are important to ensure that any data security and breach notification legislation advanced in Congress does not overly burden business already victimized by a breach, does not impose unfair burdens on unbreached entities, 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 four principles. Additionally, any such process needs to include input from all affected industries and from businesses of all sizes. Otherwise, it risks imposing unfair or

[1] GLBA's statutory language, approved by Congress in 1999, predates the first state breach notification law by several years and does not actually require notification of security breaches. Regulatory guidelines implementing GLBA adopted in 2005 recognized this omission, but did not correct it. Rather, the guidelines state that GLBA-covered entities *"should"* make breach notice, but notice is discretionary and not a *requirement*. Legislation exempting GLBA-covered entities therefore leaves them without a notice requirement.

crippling burdens on some sectors but not others, which, unfortunately, has been the case with several past legislative proposals.

We appreciate your consideration of our views as on this hearing 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 Restaurant Association
National Retail Federation
Society of Independent Gasoline Marketers of America
U.S. Travel Association

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