September 12, 2017

The Honorable Mitch McConnell
Majority Leader
U.S. Senate
Washington, DC 20510

The Honorable Chuck Schumer
Minority Leader
U.S. Senate
Washington, DC 20510

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 Leader McConnell, Leader Schumer, Speaker Ryan and Leader Pelosi,

The undersigned associations represent over a million businesses in industries that directly serve American consumers. We are committed to protecting our customers' data with effective data security practices and we take the risk of breaches of security very seriously. The rampant nature of threats to consumer data is a top challenge for businesses of all kinds, including those that support companies' communications with consumers and facilitate the acceptance of their forms of payment, as well as for professional organizations, health care institutions and government agencies.

These risks to all businesses are well-known and were demonstrated once again with the news of the Equifax breach last week. The fact is that hackers do not discriminate as to the type of business they attack. Furthermore, the ecosystem between technology-based providers and Main Street businesses is more interwoven than ever; many of our companies partner with the tech and telecom industries on their cloud, software, broadband and other solutions to serve customer needs. In July, for example, a breach at one of Verizon's contractors – a cloud services company that handled consumer data – exposed information on millions of Verizon customers. Late last year, it was revealed that Yahoo suffered multiple breaches years before affecting one and a half billion customers but never notified affected individuals until last Fall. Similarly, beginning in 2013, AT&T had multiple breaches when rogue employees stole mobile phone customer account data, including social security numbers, and in 2014, JPMorgan Chase disclosed in a regulatory filing a breach affecting 83 million customer accounts but deliberately chose not to send written notice of their breach to affected individuals. These are just a few of the hundreds of breaches that occur every year across industry, and some where affected consumers remained unaware of the risks to them afterward.

Every industry sector – whether consumer-facing or business-to-business – faces data security threats 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%). In fact, well above 80% of all breaches in 2016 occurred *outside*

of the industries represented by the signatories to this letter. To protect customers and ensure effective public policy, Congress should ensure that any federal breach notification law applies to *all* affected sectors and leaves no holes in our system for some industries that criminals can exploit.

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 all but a few state laws that have adopted data security requirements generally applicable to commercial businesses handling sensitive personal information.

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.

These four principles 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 and/or 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 the debate on data security and breach notification legislation takes shape in this Congress. 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 U.S. Senate
Members of the U.S. House of Representatives