

July 31, 2015

Members of the United States Senate  
Washington, DC 20510

Dear Senator:

The undersigned associations, representing over a million businesses, urge the Senate to consider data breach notification and data security legislation in the context of its consideration of cybersecurity legislation – but only if it is effective legislation.

Data security incidents raise concerns for American businesses as well as for our customers and clients. Organized groups of criminals and foreign nations have focused attacks on a broad range of U.S. industries. These criminals devote substantial resources and expertise to breaching even the most protected systems.

We support three essential principles that form the bedrock of effective data breach notification and data security legislation.

First, 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 card fraud and identity thieves. 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.

Second, there currently are 51 inconsistent breach laws on the books in 47 states and 4 other federal jurisdictions, such as the District of Columbia and Puerto Rico. Those inconsistencies create legal traps for Main Street businesses and uncertainty for the public. We need one, national, preemptive law so that every business and every consumer knows the singular rules of the road. A single 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. Enacting a different fifty-second law would not advance data security or notification laws.

Finally, data security requirements in a federal law should be based on a standard of reasonableness. American businesses are remarkably diverse in size, scope and operations. Laundry lists of specific security requirements do not work well given this diversity nor will they be able to adapt along with the rapidly changing picture of data security. Requiring reasonable security is the only way to allow regulators the right degree of flexibility while giving businesses the guidance they need to comply.

We look forward to working with the Senate on these issues but strongly urge that these principles be followed. In particular, carve-outs or exemptions for particular favored industry groups would be a critical mistake that would undermine data security for all of us.

Sincerely,

21<sup>st</sup> Century Fox  
International Franchise Association  
National Association of Convenience Stores  
National Association of Realtors  
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