October 12, 2018

Joseph Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Rebecca Slaughter
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Noah Phillips
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Christine Wilson
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Rohit Chopra
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: Hearings on Competition and Consumer Protection in the 21st Century

Dear Chairman Simons and Commissioners Slaughter, Phillips, Wilson and Chopra;

The undersigned associations represent over a million businesses in industries that directly serve American consumers. Our organizations appreciate the Federal Trade Commission (FTC or the Commission) soliciting comments and holding hearings on the current state of competition and consumer protection law. While these are broad topics, our associations have worked together to develop a set of principles regarding federal policy on the data security standards and consumer notification requirements in the event of breaches of sensitive data.

Our members are committed to protecting their customers' data with effective data security practices and take the risk of data breaches very seriously. 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. To protect consumers comprehensively, wherever data breaches occur, any policy in this area should ensure that breach notification requirements apply to *all* affected industry sectors and leave no holes in our system that would enable some industry sectors to keep the fact of their breaches secret. Under some legislative proposals, however, Equifax would have been exempt from the breach notification requirements along with banks, credit unions and other entities that qualify as "financial institutions" under the

Gramm Leach Bliley Act (GLBA). Such policy decisions could leave millions of Americans unaware of their potential risks of financial harm and identity theft. Exemptions would result in particularly weak public policy if they are paired with preemption from the breach notice requirements of state laws that would otherwise apply to these sectors that have no federal requirements.

Considering the widespread risk of data breaches afflicting all American industries and public institutions, there are four key principles our associations collectively support in setting any federal data security and breach notification policy:

1. **Establish Uniform Nationwide Law**: First, with the fifty-four inconsistent breach laws currently in effect in 50 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-fifth law on this subject would not advance data security or consumer notification; it would only create more confusion and provide no incremental benefit.

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 data security 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. Federal policy, including proposed breach legislation, taking this approach also would be consistent with the reasonable data security standard the Commission now enforces.

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. Congress has limited the FTC's authority to seek civil penalties until it establishes what constitutes a violation. 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. However, creating exemptions for particular industry sectors or allowing breached entities to shift their notification burdens onto other businesses – as some industry sectors have proposed – will weaken the effectiveness of the legislation, undermine consumer confidence, ignore the scope of the problem, and create loopholes that criminals can exploit.

The four principles above, which are supported by the undersigned organizations, are important to ensure that any data security and breach notification policy does not overly burden businesses already victimized by a breach, does not impose unfair burdens on non-breached entities, and does not pick regulatory winners and losers among differing business sectors in the process. We urge you to consider these four principles as you set Commission policy and formulate legislative recommendations for Congress. Additionally, we urge you to continue to solicit input from all affected industries and from businesses of all sizes. Otherwise, there is a risk of the federal government imposing unfair or crippling burdens on some sectors but not others that should have equal burdens for handling the same or more sensitive consumer data.

We appreciate your consideration of our views 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
Petroleum Marketers Association of America
Society of Independent Gasoline Marketers of America
U.S. Travel Association

cc: The Honorable John Thune
The Honorable Bill Nelson
The Honorable Greg Walden
The Honorable Frank Pallone
Mr. Bruce Hoffman, Director, Bureau of Competition
Mr. Andrew Smith, Director, Bureau of Consumer Protection
Mr. Bilal Sayyed, Director, Office of Policy Planning