February 14, 2018

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

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

Dear Chairman Luetkemeyer and Ranking Member Clay:

On behalf of the leading banking and payment companies represented by the Financial Services Roundtable, thank you for holding this hearing today to examine the current regulatory regimes for data security and consumer breach notification.

Data is increasingly the lifeblood of modern commerce. Technological innovation has made it possible for firms of any size to store, process and analyze terabytes of data with minimal investment. While these advancements have produced many positives for consumers, the proliferation of serious data breaches over the last decade has highlighted the gaps in the federal government's approach to ensuring customer information is kept safe.

The financial industry – along with healthcare – are the two sectors of the economy on which Congress has imposed specific data protection obligations. For FSR's members, those obligations originate from the Gramm-Leach-Bliley Act (GLBA). Enacted in 1999, that statute is the foundation of comprehensive data security obligations for the financial industry. These obligations center around a framework for administrative, technical and physical security safeguards that every financial firm must have in place, but recognize that a small community bank and a trillion-dollar global institution have dramatically different data security and resource needs. It also includes clear, obligatory requirements for financial institutions to maintain data breach consumer notification programs. To underscore the mandatory nature of these requirements, FSR members are regularly examined for compliance with both data protection and the requirements to maintain risk-based consumer response programs. Regulators have significant punitive tools that can be brought to bear on any institution not adhering to these obligations.

With this as background, FSR supports Congressional efforts to enact legislation that ensures all companies are required to protect sensitive personal and financial data with a strong but flexible, scalable data security framework that takes into account the sensitivity of the data held by any specific company; require timely notification to consumers that are at risk of identity theft or fraud when a breach occurs; ensure compliance via appropriate Federal and State oversight, while recognizing existing federal obligations – including GLBA; and eliminate overlapping and inconsistent state laws.

A letter submitted for this hearing by, among others, the National Association of Convenience Stores (NACS) was kind enough to remind this Subcommittee of FSR's efforts to build consensus among a diverse group of industry stakeholders for federal data security legislation when we

helped bring together 23 associations and coalitions on a recent letter to your colleagues on the Energy & Commerce Committee. This letter marked the first time multiple industries with a history of antagonism on this issue have joined together on a unified set of principles in urging Congress to enact strong data security legislation, rejecting the status quo regulatory gaps outside of healthcare and financial services. Of note, none of the groups on the NACS-led letter were part of that coalition.

We understand that building consensus and making compromises to achieve positive policy outcomes geared toward protecting our shared customers is hard work: But resorting to tired ad hominem attacks and – on a particularly ironic note, given the subject matter expertise of the members of this Subcommittee – assertions that banking rules are *optional*, seems a strategy aimed at maintaining the status quo. Taking into account existing requirements on certain sectors, we submit that no reasonable person would conclude that the status quo lack of federal requirements that *all* other companies should protect sensitive data and be required to notify consumers of a breach is acceptable in today's data-intensive economy.

A final note: The NACS letter urges this Committee not to pick "regulatory winners and losers," the insinuation being that the financial industry is somehow the "winner" if Congress recognizes our existing obligations under federal law. Given that the financial industry is subject not only to the stringent data protection and consumer response requirements of the Gramm-Leach-Bliley Act and examination and enforcement thereof, but literally every other law and regulation under the jurisdiction of this committee, it is not readily apparent how we come out ahead. However, our focus is that of this hearing – how to best protect consumers by requiring companies to secure data and notify consumers of a breach. That aim speaks to the lack of any federal requirements for the majority of companies operating in the U.S. economy, and the need for that to change. It is not too late for the members of NACS and those of like mind to grab the regulatory winner's mantle and join the growing numbers interested in working in good faith to enact rigorous, pro-consumer data security and consumer breach notification legislation.

FSR looks forwarding to continuing to work with this Subcommittee and multiple industry stakeholders to advance federal data breach legislation.

Sincerely,

/s/

Jason Kratovil
Vice President

CC: Members of the Subcommittee