April 14, 2015

The Honorable Fred Upton
2183 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
237 Cannon House Office Building
Washington, D.C. 20515

Dear Chairman Upton and Ranking Member Pallone:

We appreciate your continued work on data protection legislation and share your concerns about the seemingly endless security breaches at major retailers and other entities that acquire consumer information. Accordingly, we support legislation that would raise the data protection standards for those entities that are not required to protect consumer information by Federal law. Since passage of the Gramm-Leach-Bliley Act (GLBA) over fifteen years ago, the financial industry has been subject to significant regulatory requirements and internal safeguards and processes to ensure the security of data that have provided consumers with substantial protections. We believe that others should be held to similar data protection requirements.

The essential principles for strong data protection legislation are contained in the joint letter we submitted on March 18, 2015 in advance of the Commerce, Manufacturing and Trade Subcommittee's markup of the Discussion Draft of the Data Security and Breach Notification Act. In that letter we expressed several serious concerns with the Discussion Draft. Based upon the most recent draft released on April 10 in advance of your Committee's markup this week, we continue to believe that this legislation falls short of adequately protecting consumers as set forth below.

Strong Data Protection Standards

Strong national data protection and consumer notification standards coupled with effective enforcement provisions should be part of any comprehensive data security bill and these standards should be applicable to any party with access to important consumer financial information. That is why the current one-line "reasonable security measures" standard set forth in section 2 of the April 10 draft should be strengthened. This is especially true since the draft does not include an FTC rulemaking requirement or any other provision that clarifies what, in fact, companies must do to protect customer information.

Current GLBA standards, which your Committee helped pass into law in 1999 and which regulators have built upon since, require financial institutions that acquire personal and financial data to put in place a process to protect that data. It does not mandate specific technology, but the extent to which entities need to ensure the information is protected is based on the size and complexity of the entity, the activities the entity undertakes, and the sensitivity of the information being held. We urge the Committee to include flexible and scalable standards in the draft similar to those applied to financial institutions through the GLBA and its subsequent rules and regulations.

Recognition of Existing Federal Data Protection and Consumer Notice Standards

Since banks and credit unions are already subject to robust data protection and notification standards under the GLBA, these requirements must be recognized in legislation and we strongly urge the Committee to ensure that entities already covered by Federal data protection and notification laws and regulations would not be subject to dual and perhaps inconsistent regulation.

No industry should be burdened by unnecessary duplicative regulation. Unfortunately, the exceptions contained in Section 5 of the April 10 draft are not broad enough to completely exempt those already covered by GLBA data protection and notice provisions. In particular, bank holding companies, certain non-bank subsidiaries of banks and bank holding companies and affiliates of credit unions may be subjected to dual oversight and enforcement. Since such entities are also governed by their parent companies' regulatory requirements, this could effectively subject them to dual regulation.

Liability for Breaches

We believe that all parties must share in protecting consumers. Too often, banks and credit unions bear a disproportionate burden in covering the costs of breaches occurring beyond their premises. As such, Section 4 of the draft should be modified to ensure that the costs of a data breach are borne by the entity that incurs the breach.

Preemption

Finally, inconsistent state laws and regulations specifically dealing with data protection and consumer notification should be preempted for all entities that are subject to strong Federal data protection and notification standards, whether they are considered "covered entities" within the meaning of the draft or are covered by other laws such as the GLBA. As drafted, Section 6 does not accomplish this.

We strongly support legislation that would increase consumer protection by encouraging greater protection of sensitive personal and financial information, and sincerely appreciate the hard work of the Members and staff of the Committee. However, the April 10 discussion draft falls short of that shared goal. In our view, the issues outlined above must be addressed before this bill is brought to the House floor. We hope to continue to work with you to make the case for strong consumer data protection legislation both in your Committee and in other Committees with jurisdiction over this issue.

Sincerely,

American Bankers Association
The Clearing House
Consumer Bankers Association
Credit Union National Association
Financial Services Roundtable
Independent Community Bankers of America
National Association of Federal Credit Unions