March 18, 2015

Chairman Michael C. Burgess
Subcommittee on Commerce,
Manufacturing and Trade
Committee on Energy and Commerce
United State House of Representatives
Washington, D.C. 20515

Ranking Member Janice Schakowsky
Subcommittee on Commerce,
Manufacturing and Trade
Committee on Energy and Commerce
United State House of Representatives
Washington, D.C. 20515

Statement for the Record for the Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade Hearing
On the Data Security and Breach Notification Act of 2015

Dear Chairman Burgess and Ranking Member Schakowsky:

Thank you for holding a hearing on the Discussion Draft of the Data Security and Breach Notification Act of 2015.

We share your concerns about protecting consumers and submitted a joint letter on January 23, 2015 in advance of your Subcommittee hearing on this issue. Our letter outlines a set of principles to serve as a guide when drafting legislation to provide stronger protection for consumer financial information. For more than 15 years, the financial industry has been subject to significant regulatory requirements and internal safeguards which have been substantially enhanced over the years, and we commend you on moving forward with legislation that is intended to increase consumer protection by encouraging greater protection of sensitive personal and financial information.

We look forward to working with you in a constructive way on the Discussion Draft. However, we have concerns about the Draft and believe that it would be improved by the following modifications:

Requirements for Information Security

Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security bill and these standards should be applicable to any party with access to important consumer financial information.

The Discussion Draft takes a step forward by including data protection requirements in Section 2. However, the current "reasonable security measures" standard set forth in this draft would be strengthened by including flexible and scalable standards similar to those applied to financial institutions through the Gramm-Leach-Bliley Act (GLBA) and its subsequent rules and regulations.

Since this draft does not include an FTC rulemaking requirement, it is especially important that meaningful data protection standards be included in the bill. In addition, since the bill preempts state laws, and because we are obliged to support a standard that protects consumer information

throughout the entire supply chain, we believe a strong data security requirement would help protect against the unintended consequence of providing consumers with less protection than afforded under current law.

Current GLBA standards require entities 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.

Definition of "Covered Entity"

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 entities already covered by Federal data protection and notification laws and regulations should not be subject to dual and perhaps inconsistent regulation.

We therefore appreciate the Committee's efforts to ensure no industry is burdened by unnecessary duplicative regulation, and the Discussion Draft appears to address this, at least in part. However, the language included in Section 5 may not be broad enough to completely exempt those already covered by GLBA data protection and notice provisions. In particular, state-chartered credit unions, certain non-bank subsidiaries of banks and bank holding companies and affiliates of credit unions may be subjected to dual oversight and enforcement. Subsequently, because such entities are also governed by their parent companies' regulatory requirements, this could effectively subject them to dual regulation. We look forward to working with the Committee to solve this problem.

Preemption of State Law

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 Discussion Draft or covered by other laws such as the GLBA. As drafted, Section 6 does not accomplish this.

Consumer Notification

In the event of a breach, the public should be informed where it occurred as soon as reasonably possible to allow consumers to protect themselves from fraud. Section 3 of the Discussion Draft contains detailed notification requirements. However, this section should also be modified to clarify that banks and credit unions, which often have the most direct relationship with affected consumers, should be able to inform their customers and members about the information regarding the breach, including the entity at which the breach occurred.

Costs of Breach

Too often, banks and credit unions bear a disproportionate burden in covering the costs of breaches occurring beyond their premises. All parties must share in protecting consumers. Therefore, the costs of a data breach should ultimately be borne by the entity that incurs the breach. Section 4 of the Discussion Draft should be modified to reflect this. Specifically, an entity that fails to comply with the data protection requirements of Section 2 that experiences a breach involving sensitive account information would be liable for any losses resulting from the breach and for any reasonable costs to protect the accounts.

We look forward to working with you and your colleagues on the Energy and Commerce Committee, as well as other Committees, such as the Financial Services Committee, to craft data protection and notice legislation to better protect your constituents' personal financial information.

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