January 23, 2015

Dear Representative:

As the 114th Congress engages in public debate on the important issue of data security, the undersigned financial trade associations are writing you collectively to: 1) give our perspective on the key elements that should be included in any legislative approach; and, 2) to make you aware of the current robust regulatory regime already in place that requires financial institutions to protect the financial information of their customers/members and to notify them in the event of a breach that is likely to put them at risk.

We share your concerns about protecting consumers and strongly believe that the following set of principles should serve as a guide when drafting legislation to provide stronger protection for consumer financial information:

1. Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security regime, applicable to any party with access to important consumer financial information.
2. Banks and credit unions are already subject to robust data protection and notification standards. These Gramm-Leach-Bliley Act (GLBA) requirements must be recognized.
3. Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification standards.
4. 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. 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.
5. 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.

As noted above, some industries – including the financial industry – are required by law to develop and maintain robust internal protections to combat and address criminal attacks, and are required to protect consumer financial information and notify consumers when a breach occurs within their systems that will put their customers at risk. The same cannot be said for other industries, like retailers, that routinely handle this same information and increasingly store it for their own purposes. The Identity Theft Resource Center has compiled a list of ***all publicly reported breaches in the United States*** and shows that banks accounted for only 5.5 percent of all breaches in 2014. Other businesses accounted for 33 percent. Retailer groups continue to cite a Verizon report on data breach statistics as a way to distract policymakers regarding the primary focus of data security breaches, but the inconvenient truth is that this Verizon report is based on an ***international sampl***e of breaches as opposed to an actual compilation of all publicly reported breaches in the United States.

For more than 15 years, credit unions and banks have been subject to significant regulatory requirements and internal safeguards which have been substantially enhanced over the years. These include:

- Federal Requirements to Protect Information - Title V of the Gramm-Leach-Bliley Act and its implementing rules and guidance requires banks and credit unions to protect the security, integrity, and confidentiality of consumer information.
- Federal Requirements to Notify Consumers - Banks and credit unions are also ***required to notify*** customers whenever there is a data breach where the misuse of customer information has occurred or it is reasonably likely that misuse will occur.
- Strong Federal Oversight and Examination - Under their broad-based statutory supervisory and examination authority, the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration ***regularly examine*** financial institutions for compliance with data protection and notice requirements.
- Strong Federal Sanction Authority - Under numerous provisions of Federal law, banks and credit unions are ***subject to substantial sanctions and monetary penalties*** (e.g., up to $1 million per day fines) for failure to comply with statutory and regulatory requirements.

This extensive legal, regulatory examination and enforcement regime ensures that financial institutions robustly protect American's personal financial information. In contrast, retailers that accept electronic payments face no similar requirements or oversight, and as a result millions of American consumers' personal financial information has been compromised in recent years.

The groups below look forward to working with you and your colleagues in order to protect your constituents' personal financial information.

Sincerely,

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