November 12, 2014

The Honorable Harry Reid
Senate Majority Leader
522 Hart Senate Office Building
Washington, DC 20510-2803

The Honorable Mitch McConnell
Senate Minority Leader
317 Russell Senate Office Building
Washington, DC 20510-1702

The Honorable John Boehner
Speaker of the House
1011 Longworth House Office Building
Washington, DC 20515-3508

The Honorable Nancy Pelosi
Minority Leader
235 Cannon House Office Building
Washington, DC 20515-0512

Dear Leaders Reid and McConnell, Speaker Boehner and Leader Pelosi:

On November 6, 2014, a group of organizations representing elements of the retail industry wrote to you regarding recent breaches of consumer information. Their letter, unfortunately, is inaccurate and misleading, and recommends solutions that leave consumers vulnerable to enhanced risk of data breaches. The undersigned financial services organizations wish to set the record straight.

As evidenced by the massive breaches at Target, Home Depot, Michaels, Neiman Marcus, Jimmy Johns, Staples, Dairy Queen and others, retailers are being targeted by cyber criminals. While merchants and financial institutions are both the targets of these attacks, a key difference is that financial institutions have developed and maintain robust internal protections to combat criminal attacks and are required by Federal law and regulation to protect this information and notify consumers when a breach occurs that will put them at risk. In contrast, retailers are not covered by ***any*** Federal laws or regulations that require them to protect the data and notify consumers when it is breached.

Significant regulatory requirements and internal safeguards are already in place at U.S. financial institutions with respect to data security. These extensive requirements and safeguards were first required in 1999 as part of the Gramm-Leach-Bliley Act (GLBA) and have been substantially enhanced since then by regulatory action.

- Federal Requirements to Protect Information - Title V of the GLBA and its implementing rules and guidance requires banks and credit unions to protect the security, integrity, and confidentiality of consumer information. ***Extensive federal rules and regulatory*** infrastructure have evolved from this 15-year old statutory mandate.

- 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.

In short, an extensive regulatory oversight, examination and enforcement regime ensures that financial institutions provide robust protections for personal financial information for the American public.

In contrast, no similar internal safeguard regime and regulatory oversight exists with respect to retailers and others, and ironically, certain retail trade groups have been vigorously opposing legislation in both the House and Senate that would bring this about. National consumer notification alone – as advocated by the November 6th letter – will not solve this problem. It is only when coupled with the development of strong internal data protection standards and robust oversight that the retail community will find itself in a better position to protect consumers and their confidential personal financial information from criminal abuse.[1]

Financial institutions on their own are aggressively implementing new systems and leading the development of new technologies like tokenization to combat the ever-changing criminal threat. At the same time, the financial services industry is committed to working with all stakeholders to ensure that data breach protections are a shared responsibility requiring everyone in the payments chain to have a heightened awareness of potential emerging threats and work to address them.

In light of recent events, no doubt many in the retail community are attempting to do the same. But, as noted in the November 7, 2014 *Wall Street Journal*, by Frank Blake, Home Depot's former chief executive, "Data security just wasn't high enough in our mission statement."

It's time for that to change.

Sincerely,

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

[1] The Identity Theft Resource Center has compiled a list of ***all publicly reported breaches in the United States*** and shows that through November 4th of this year banks accounted for only 6.2 percent of all breaches this year. Other businesses accounted for 32 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.