EPC ELECTRONIC PAYMENTS COALITION®

May 10, 2016

The Honorable Paul Ryan
Speaker of the House
United States House of Representatives
H-232, The Capitol
Washington, D.C. 20515

The Honorable Nancy Pelosi
Democratic Leader
United States House of Representatives
H-204, The Capitol
Washington, D.C. 20515

The Honorable Kevin McCarthy
Majority Leader
United States House of Representatives
H-107, The Capitol
Washington, D.C. 20515

The Honorable Steny Hoyer
Minority Whip
United States House of Representatives
H-148, The Capitol
Washington, D.C. 20515

The Honorable Steve Scalise
Majority Whip
United States House of Representatives
H-329, The Capitol
Washington, D.C. 20515

Dear Speaker Ryan, Majority Leader McCarthy, Minority Leader Pelosi, Majority Whip Scalise and Minority Whip Hoyer:

On behalf of the members of the Electronic Payments Coalition, which represents credit unions, banks of all sizes and payment networks, we ask for your assistance in facilitating the advancement of data security and data breach notice legislation.

The Data Security Act (H.R. 2205) passed the House Financial Services Committee last December by a strong bipartisan vote of 46-9. The bill was also referred to the Energy & Commerce Committee in May 2015, where it has not yet been considered. A similar bill, the Data Security and Breach Notification Act (H.R. 1770), has been approved by the Energy & Commerce Committee, but has not seen further action since it was reported out of the Committee by a party line vote in April, 2015. These bills have a number of provisions in common that could lead us to a sensible, workable solution to the ongoing problem of data breaches, which requires Congressional intervention and action for the sake of consumers.

Both bills contain provisions intended to require certain "covered entities" to secure data with which they are entrusted. Both bills also contain provisions that require notice to specified parties when a breach occurs. They both contain provisions that would resolve the patchwork of state laws related to data security and breach notice, through a single preemptive Federal standard for data security and breach notice. In addition, both bills include the general concept of functional regulation, where longstanding Federal regulators would continue enforcement for entities under their jurisdiction, with supplemental enforcement by state Attorneys General. This overall state of agreement between the

two committees regarding policy intent leads us to believe that a resolution between the two bills can be reached with concerted effort.

There are, however, some key differences between the bills. Of particular concern, H.R. 1770 does not flesh out any meaningful security standards for non-financial companies, and due to the rule writing limitations on the Federal Trade Commission, this regulator cannot fill the void for entities it oversees. Add to that the bill's preemption of existing state data security laws, and the result could be consumers actually receiving less data security from retailers under H.R. 1770 than under existing law.

Because H.R. 1770 is focused only on covered entities bound by laws and regulatory agencies under the jurisdiction of the Energy & Commerce Committee, the bill at very least must be married with H.R. 2205, the bill reported from the Financial Services Committee. Doing so ensures the concept of a uniform Federal standard for data security and breach notice, enforced through functional regulation.

We believe that H.R. 2205 strikes the right balance and should provide Congress with the bipartisan momentum needed to move towards enactment of legislation on behalf of consumers. With this in mind, we have urged the House Financial Services Committee and House Energy & Commerce Committee to work collaboratively to achieve these goals.

Those firms outside of the financial services industry that hold sensitive consumer data are still not bound by any national standards for protecting that data and notifying affected consumers when there is a significant risk of harm from a breach. Even at the state level today, retailers and other non-financial companies are generally not subject to data security standards. In stark contrast, financial institutions have complied with a national standard similar to that proposed in H.R. 2205 since at least 1999.

Consumers deserve protection of data they supply in the course of buying goods and services. For their benefit and to prevent unnecessarily prescriptive regulatory burdens, these protections should be tailored to the size and nature of the business involved. Merchants that accept payments with electronic information for their economic gain should also accept some minimal responsibility to safeguard that personal information. Additionally, it is neither equitable nor sustainable for community banks and credit unions to be forced to pick up the pieces after repeated retailer breaches. To serve their customers, our members must reissue credit and debit cards at significant financial cost after a breach. Unless action is taken, they will continue to incur unearned reputational damage when consumers attribute retailer data breaches to the financial institutions that reissue the cards. The negligence of merchants that accept payments without appropriate protective measures is too costly.

It is time to protect consumers' personal data by putting in place a national security standard. That is why we ask Congressional leadership to engage both the Energy & Commerce Committee and Financial Services Committee to enter into a constructive dialogue with each other to advance comprehensive data security and breach notice legislation that works for all interested parties.

Sincerely,

Molly Wilkinson
Executive Director
The Electronic Payments Coalition