October 15, 2015

Dear Representative:

Well publicized data breaches have rightly focused Congress's attention on consumer data security, and as we transition to the use of EMV "chip" payment cards, many in Congress have again focused on this issue. We are proud to be leading the way to achieve a safer and more secure payment system, and the adoption of EMV technology is an important part of that effort. However, data security requires all participants in the payments ecosystem – financial institutions, payment networks and processors, and merchants – to do their part to ensure that consumers' sensitive payment information is protected. The payments system is only as strong as its weakest link; that is why we urge you to cosponsor H.R. 2205, the "Data Security Act of 2015." This bipartisan legislation introduced by Reps. Neugebauer and Carney will establish uniform national standards for consumers' sensitive payment and personal information that are scalable and flexible to the size and risk profile of the covered entity.

Legislation addressing data security is long overdue. Millions of American consumers have had their financial and personal data exposed because of data breaches at well-known merchants. Data breaches at Target, Neiman Marcus, Home Depot, Michaels, and T-Mobile are just a few of the major breaches that have compromised millions of consumers' sensitive information. The Target breach alone is estimated to have affected 5.4 million payments cards. Not only are consumers negatively impacted, the cost of reissuing payments cards disproportionally falls on small financial institutions. We respectfully suggest that the time is long past for Congress to address this situation.

Financial institutions of all sizes are already required by the Gramm-Leach-Bliley Act (GLBA) to develop and maintain robust internal protections to combat and address network intrusions and data theft. We are committed to compliance with GLBA to ensure the security and confidentiality of customer records and information; protect against any anticipated threats to the security or integrity of such records; and protect against any unauthorized access to or use of such records or information that would result in both harm and inconvenience to any customer. Retailers, however, are not subject to requirements similar to GLBA, but recent history shows that it is clearly vital to protect data on both sides of the transaction. H.R. 2205 ensures that all entities that handle consumers' sensitive financial data have in place robust processes to protect data which should help prevent data breaches in the first place.

Because data security should be a shared responsibility by all participants in the payments ecosystem, we strongly urge you to cosponsor H.R. 2205, which will help ensure that minimum standards are in place to protect your constituents' sensitive financial and personal information.

Sincerely,

Electronic Payments Coalition
Credit Union National Association
Consumer Bankers Association
Financial Services Roundtable
Independent Community Bankers of America
National Association of Federal Credit Unions
American Bankers Association