October 16, 2015

The Honorable Steve Chabot
Chairman
Committee on Small Business
Washington, D.C. 20515

The Honorable Nydia Velazquez
Ranking Member
Committee on Small Business
Washington, D.C. 20515

Dear Chairman Chabot and Ranking Member Velazquez:

On behalf of the 14,000 banks and credit unions of all sizes that are taking on criminal hackers by issuing payment cards with highly secure "EMV" microchips, we appreciate the Committee's interest in the transition to the next generation in payments security. With an estimated 575 million so-called "chip" cards to be issued by year-end and millions of merchants on the road to implementation, the U.S. marketplace will be significantly safer at the cash register for our nation's consumers.

As you know, EMV (or "chip") technology makes stolen card numbers useless to thieves if they try to create counterfeit cards, and address the lion's share of today's fraud for in-store (or "card-present") transactions. The rollout of chip or "EMV" technology demonstrates how the financial services and retail industries can and must work together to better protect consumers.

While the Committee's October 7th hearing was helpful in highlighting some of the issues around EMV, we want to share additional information based on some of the questions raised at that hearing to assist you in preparation for the Committee's next hearing on EMV.

First, the move to chip technology has been underway for quite some time. The transition to EMV began in 2011, and card networks, banks and credit unions, merchant bank processors, and the merchants themselves have been involved in implementing the transition since that time. Indeed, many merchant banks have worked with small businesses to identify ways to upgrade payment terminals at low- or no-cost. Merchants are our customers—we want them to succeed.

Second, consumers will benefit greatly from this transition. After the major data breaches at big box stores, like Target and Home Depot, tens of millions of account numbers were posted online, which could have easily been used to create counterfeit cards. In response, banks and credit unions reissued millions of cards at an unprecedented pace in order to protect consumers from fraud. Going forward, chip cards greatly reduce the fraud risks stemming from such breaches by generating a one-time code for each transaction, eliminating the possibility that those chip cards can be counterfeited and used at another store. Once chip cards fully replace the magstripe – *the U.S. has already issued the most chip cards of any country in the world* – and merchants turn on their chip card readers, counterfeit cards will become a lot harder to create.

Third, merchants are fully empowered to protect themselves from any increased liability as part of this transition. Once merchants install chip card readers and turn them on, liability returns to the financial institution. Chip card readers are available for very reasonable prices. Depending upon the vendor and type of upgrade needed, it can be zero or as little as $49, which makes it easy for merchants of all sizes to protect their customers at minimal cost. Moreover, liability shifts only for accounts that are chip-enabled—so if the card issuer has not done its part, it bears the risk. This is a private sector incentive to encourage adoption and better consumer protections.

Fourth, the "PIN argument" is a smokescreen used by retail trade groups to deflect attention from the high profile retail data breaches at big box stores over the past few years and their underlying causes. Rather than coming together to improve internal data security practices, the retail trades are fixating on a PIN technology that fights a small and declining share of today's fraud and which would have been meaningless in breaches like those at Target and Home Depot. The reality is that if a merchant is EMV enabled and has their card readers turned on, they have the same protections whether PIN is used or not. Instead of fighting, we should embrace ideas like H.R. 2205, the Data Security Act of 2015, introduced by Representatives Neugebauer (R-TX) and Carney (D-DE), to apply meaningful and consistent data protection for consumers nationwide.

Finally, an attempt is being made to interject one of the most controversial parts of the Dodd-Frank Act – the price controls of the Durbin Amendment - into the chip card discussion. The fact is that banks and credit unions annually spend billions on innovation in payment security in order to stay ahead of the thieves. We are pioneering cutting-edge solutions - like the "tokenization" technologies used in Apple Pay and Samsung Pay, end-to-end encryption, and biometric authenticators – to protect transactions wherever they take place. That forward-looking approach to "tomorrow's threats" today should be the focus of our collective discussions.

Ultimately, the only way to protect our data is to stay ahead of the ever-changing criminal element through joint efforts. The security of our payments system impacts all of us and the payments system will only be secured if everybody—banks, credit unions, payment networks, retailers and consumers—work together to fight a common enemy.

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

cc: Members of the House Committee on Small Business