September 21, 2015

To: Members of the United States House of Representatives
Members of the United States Senate

From: James Ballentine, Executive Vice President, Congressional Relations & Political Affairs

Re: ABA Memo on Transition to Chip Cards

You, like your constituents and millions of citizens across the country, probably have received your new bank-issued chip card that has new security features to better protect consumers and merchants against fraud. An estimated 575 million cards embedded with computer chips (EMV) are expected to be in the hands of consumers by the end of 2015. These cards produce a one-time transaction code that cannot be used for future payments, thus adding a dynamic, ever-changing layer of security on top of static card information like account numbers. Consumers continue to enjoy the same protections for any fraud that occurs– zero liability in most instances.

The EMV chip is the key to keeping sensitive information safe by making the financial data nearly impossible for criminals to create, sell and use for counterfeit cards. In fact, nearly all of today's fraud comes from either counterfeit cards made with stolen personal and financial data and used in stores or through online fraud where the card is not present.

EMV chips are an important innovation that will better protect consumers' financial data. But they are only one part of a larger fight against hackers and thieves. Ultimately, the only way to protect our data against these increasingly savvy criminals is by developing better technologies. As more and more commerce takes place online and with mobile phones, two areas where PINs are not effective, banks are pioneering cutting edge solutions designed to meet tomorrow's threats today. Tokenization technologies like those used on Apple Pay, for example, will play an increasingly vital role in keeping your data safe in the future.

Arguments that only EMV cards with PINs can protect consumers from fraud are flat out wrong and quite frankly are a diversion from the real issues. PINs only protect against lost and stolen cards, a small and rapidly diminishing portion of fraud, not counterfeiting or card-not-present transactions.

In fact, no single major data breach over the last few years could have been prevented with a PIN. The high profile data breaches that resulted in millions of Americans having their card accounts compromised were not caused by petty thieves stealing cards out of wallets—they were caused by criminals exploiting cracks in the retailers' security systems. The reality is that static four-digit PIN numbers are incapable of thwarting sophisticated hackers or disguising sensitive credit card information once stolen.

The payments system will only be secured if everyone—banks, payment networks, retailers and consumers—works together to fight a common enemy.

For more information, please visit: LetsInnovateNotMandate.com