Dear Attorney General:

Our understanding is that you are reviewing technology and considering options for electronic payment security. You undoubtedly share our belief that the security of the electronic payments system is of paramount importance. To that end, the payments industry has led the way in developing leading-edge technology and investing billions to ensure the integrity of the system.

Most recently, this has taken the form of a small chip on your new credit or debit card. This EMV microchip generates a unique, one-time use code for every consumer transaction. This chip prevents the most common type of payment card fraud by making it nearly impossible for hackers to use credit card data to create counterfeit cards. These EMV chip cards provide a new innovative layer of security, helping to better protect consumers' payment information.

Unfortunately, certain merchant lobbying groups have been spreading an outdated narrative that mandating the use of PINs could eliminate fraud and singlehandedly secure the electronic payments system. Such a narrative is dangerous. Focusing on just one technology bestows a false sense of security at a cost that everyone bears. It also conflates credit card fraud and data breaches. As discussed below, PINs would not have prevented any of the recent data breaches at so-called "Big Box" retailers.

The truth is, there is no single technology that is a panacea when it comes to preventing data breaches and the payments-related fraud that results from it. Effectively fighting these threats requires multi-layered and flexible solutions that work in different situations to effectively secure the system. Proven and existing technologies include encryption, tokenization (which is used in ApplePay), biometrics, and network-based monitoring. The dynamic nature of these cybersecurity threats is one of the reasons that we recommend against mandating any specific technology, particularly a static data element like a PIN.

Federal regulators who have carefully studied the issue and considered all options have consistently concluded that PIN is not the answer to today's security challenge. Regulators as diverse as the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, and Federal Trade Commission, all agree that mandating PINs is not an effective way to protect the electronic payments system or consumers' personal data. These regulators have emphasized the importance of allowing the payments industry to innovate, adopt a multi-layered approach to payment security, and avoid mandating particular security technologies that tend to be quickly outdated.

Following are just a few of the comments federal regulators have shared regarding PIN mandates and payment system security:

> "In our role as supervisor, the Federal Reserve does not mandate use of a specific technological approach to payment card security in recognition of

the evolving nature of payment card fraud threats and of the variety of tools that can be employed to address these threats. This approach is intended to allow financial institutions and other industry participants sufficient flexibility to design policies and procedures that most effectively reduce fraud losses to all parties involved in payment card transactions.

"The Federal Reserve supports a layered approach to payment card security that does not mandate a particular security technology." – *Board of Governors of the Federal Reserve System (March 5, 2015 – P. 1)*

"The industry is undertaking a number of initiatives focused on strengthening the security of online transactions, including online PIN-based solutions, tokenization, one-time account numbers and other measures. This type of innovation illustrates why the FDIC generally does not mandate technology as the threats and technology evolve rapidly." – *Federal Deposit Insurance Corporation (February 12, 2015 – P. 7)*

"Although PINs may reduce fraud in certain circumstances, they do not eliminate it. Further, chip-and-PIN may not be adequate for card-not-present transactions, such as those occurring online or via telephone. That is why the OCC believes that a layered approach rather than a single technological solution is best for strengthening security, reducing fraud and responding to evolving threats." – *Office of the Comptroller of the Currency (March 9, 2015 – P. 4)*

PIN technology was developed by the banking industry in 1967 for ATM transactions. The payments industry is fully aware of its uses and limitations, as well as the fact that PIN fraud rates have increased more than threefold since 2004. Again, PIN is a static data element, and subject to compromise – it is yesterday's solution to tomorrow's problem. Since the high-profile Target breach during the 2013 holiday season, numerous retailers including Home Depot, UPS, eBay, Michaels Stores, and Neiman Marcus have all suffered noteworthy breaches. It's critical to note that none of these breaches were the result of customers using debit or credit cards without PINs and none of these breaches would have been prevented by the use of PINs.

It is worth noting that the banking industry also introduced EMV/chip technology to deal with European telecommunications networks that lacked available and affordable data capacity at the time. As a result, European transactions had to be authenticated in an "offline" environment and PIN was one of the ways to make that possible. In contrast, the US had sufficient data capacity to permit real time online authorization of transactions. Unlike PIN, EMV is a dynamic technology and its ability to stop counterfeit fraud ensures it will hold a long-term place in our suite of security measures.

In its compilation of every publicly reported breach in the United States in 2014, the Identity Theft Resource Center has reported that businesses (e.g., retailers) accounted for almost six times as many breaches as banks. In most cases, hackers stole customer data through weaknesses in the security system of businesses, not through credit card fraud, and certainly not because a card had a signature instead of a PIN.

The payments industry is committed to driving electronic payment security innovation forward, constantly looking for ways to keep customers' information safe and secure; but, we can't go it alone. Banks, networks, retailers, and customers must all work together to ensure the security of the payments system.

We need merchant trade associations to stop trying to halt progress and distract the attention of policymakers from serious data breach vulnerabilities. Instead, we need them to work with us to help everyone implement new and improved solutions that will better protect consumers and secure the payments ecosphere.

Sincerely,

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