March 23, 2015

Dear Members and Senators:

Recently, you received a letter from a handful of retailer trade groups once again suggesting that a decades-old technology – personal identification numbers, or PINs -- is the panacea for our current data security challenges. As you think about their letter, the undersigned trades encourage you to consider the following facts:

- Currently, 75% of U.S. merchants do not have the capability to accept PINs, even on debit transactions.[1]
- A report by the Federal Reserve Bank of Atlanta published in 2012 found that PIN debit fraud rates have increased more than threefold since 2004[2]. When a PIN is compromised, it can open a backdoor for criminals to access and drain consumers' bank accounts at an ATM.
- As recent news stories attest[3], most merchants (80%) fail on card security compliance.
- When asked on a survey about their level of readiness to accept chip cards (also called EMV), nearly one in five merchants answered, "What is EMV?"[4]
- Chip and PIN does not protect consumers against online and other types of card-not-present fraud. When other countries moved to Chip and PIN, online and card-not-present fraud skyrocketed.
- *None of the recent wide-scale merchant data breaches we endured would have been prevented had Chip and PIN been accepted by those merchants.*

Congress is poised to apply strong data security requirements on the weak link in the payments system -- merchants. While we disagree with merchants on the one-sided notion that a technology developed in the 1960s – PINs – is the way to protect consumer information now and into the future, we do agree that questions need to be asked.

Since lax data security at merchants is what allowed tens of millions of consumers to have their financial information exposed, why are merchants pointing fingers at banks and credit unions? Why do merchants oppose common-sense requirements to secure sensitive financial information?

Most importantly, why are merchants fighting to maintain a status quo that is clearly not working for consumers?

---

[1] Board of Governors of the Federal Reserve System, Regulation II Final Rule. Accessed at: http://www.gpo.gov/fdsys/pkg/FR-2011-07-20/html/2011-16861.htm

[2] Douglas King. *Chip-and-PIN: Success and Challenges in Reducing Fraud*. Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, 2012.

[3] http://www.cnbc.com/id/102495280#.

[4] "NRF 2015 Retailer Survey Findings," ACI International. Accessed at: http://www.aciworldwide.com/-/media/files/collateral/nrf-2015-aci-survey-retailer-findings.pdf

Winning the war against cybercrime will take a forward-looking approach to preventing data breaches anywhere they occur – at the register, with a mobile phone or online. The financial industry is innovating and building the security technologies that will evolve our payments system, ensuring consumers feel confident that their data is safe. Despite what merchants would like you to believe, focusing on just one technology, like PINs, gives a false sense of security at a cost that everyone bears.

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