NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org

National Association of Federal Credit Unions | www.nafcu.org

October 20, 2015

The Honorable Steve Chabot
Chairman
House Small Business Committee
2361 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Nydia Velázquez
Ranking Member
House Small Business Committee
2361 Rayburn House Office Building
Washington, D.C. 20515

Re: Tomorrow's Hearing on EMV Implementation

Dear Chairman Chabot and Ranking Member Velázquez:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association that exclusively represents the federal interests of our nation's federally-insured credit unions, I write in conjunction with tomorrow's hearing, "The EMV Deadline and What it Means for Small Businesses: Part II." Thank you for your interest in these important issues and for allowing us to share our views.

As NAFCU testified before the Committee two weeks ago, it is important to note that the EMV transition in the U.S. is a voluntary one established by the market, and not a government mandate. EMV is the established global standard for "chip" cards and their compatibility with point of sale terminals. As you know, EMV cards contain an embedded microprocessor (or "chip") that stores data and adds additional protection by making it harder to produce a counterfeit card that can be used at a point of sale terminal. This is because the chip generates unique data (a new, random number) for each transaction. If that data is stolen, it is not traceable back to the account. It is the EMV "chip" technology that makes the new cards more secure – not a PIN or signature.

Concerns regarding the lack of a PIN requirement that are raised by merchants and their allies in their testimony are misplaced and a "red herring" to the broader issue of data security and identity theft prevention. Chip technology, with or without a PIN, prevents counterfeit fraud, which represents the biggest category of payment card fraud in the U.S. The bottom line is that if a merchant has an EMV-enabled card reader and it is turned on, they do not have new liability, whether PIN or signature authentication is used. A PIN mandate would not prevent online or mobile fraud, often referred to as "card-not-present" fraud. This type of fraud is expected to rise significantly after the EMV transition. Wider use of PINs in countries using EMV technology has done nothing to prevent spikes in card-not-present fraud.

A truly secure payments system must be one that is constantly evolving to meet emerging threats and uses a wide range of dynamic authentication technologies – EMV, tokenization, encryption, biometrics and more. Many retailers today are increasingly moving away from traditional point-of-sale authentication methods, like PIN or signature, and relying on network-based monitoring

to identify fraud, as this can improve the customer experience by reducing time spent in the checkout line. Many merchants do not request a signature or PIN with card usage. Retailers have demanded this change of the industry in order to speed the checkout process. Because retailers do not have standards requiring them to protect consumer data collected at the point of sale, they have prioritized the speed of the transaction to increase customer sales at the expense of the security of the payments system. This makes retailers a vulnerable point of entry to data breaches in the payments ecosystem, even with PIN and signature authentication.

While financial institutions are subject to the robust standards of the *Gramm-Leach-Bliley Act* (GLBA), retailers and others who handle financial data are not subject to the same type of national standard. NAFCU has long argued that protecting consumers and financial institutions by preventing future data breaches hinges on establishment of strong federal data safekeeping standards for retailers and merchants akin to what credit unions already comply with under the GLBA. Unfortunately, merchants have attempted to use the EMV and PIN debate to stop any meaningful discussion about data security legislation—thus not addressing the real issue of the broader responsibility of merchants to protect consumers' financial data.

The time has come for Congress to enact a national standard of data protection for consumers' personal financial information. We urge you to support H.R. 2205, the *Data Security Act of 2015*, which would create such a standard.

Again, thank you for your attention and continued interest in these important issues. If my staff or I can be of assistance to you, or if you have any questions, please feel free to contact myself, or NAFCU's Associate Director of Legislative Affairs, Chad Adams, at (703) 842-2265.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the House Small Business Committee