As you know, an important upgrade to payment technology has been under way for the last several years – the transition to microchip-equipped credit and debit cards. The chip is a major leap forward over the magnetic stripe found on the back of debit and credit cards for decades. The chip literally places a computer into the wallets of consumers, producing a one-time use code for each transaction when used at a chip-enabled retailer. Virtually uncopiable, the chip cannot be counterfeited using data stolen from data breaches or through “skimming.” Simply put, the United States is on the cusp of a major reduction in counterfeit credit card fraud.

This transition away from magnetic stripes requires close collaboration between banks, card networks and retailers: banks have to issue new cards, and retailers have to install terminals capable of accepting them. The benefits of this robust payment credential are directly related to the number of merchants who allow consumers to use them. Unfortunately, some retail trade associations continue to resist this critical security upgrade by inappropriately raising long-running economic concerns about the payment system. Rather than enthusiastically supporting a security upgrade and arguing their other issues later, major retailers continue to barrage Congress and regulators with tangential arguments which divert attention from the task at hand. The payment industry continues to focus on its role in the economy: protecting consumers and enabling the continued implementation of innovative payment technologies (Infographic).

A large retail trade association is hosting a fly-in this week and may be meeting with your office. Our understanding is that they will once again attempt to divert your attention from their ongoing, massive data breaches and shift blame to the payment industry for not implementing an unconnected technology (PINs) on all payment cards. Rather than argue over one particular authentication method, we think it is time to take stock of the successes of the EMV transition.

The EMV Transition Is Benefiting Consumers
Though the EMV transition requires investments on the part of banks and retailers, it is well worth it for every stakeholder in the payments system. We’ve already seen significant strides:

- Nearly 600 million EMV chip cards were issued in the U.S. in 2015, making the U.S. the largest EMV market in the world (ABI Research).
- More than one million merchants have turned on their chip card terminals, and more than 75 percent of these merchants are small and medium-sized businesses.
Payment networks are already innovating to further improve the consumer experience, with the introduction software capable of expediting chip card transactions.

The October 1, 2015 liability shift was not a deadline, but rather a milestone intended to incentivize timely adoption of EMV. The process began in 2011, when U.S. payment networks announced a gradual transition process and roadmap to give issuers and businesses flexibility to upgrade their technology over time. As of October 1, the party that has not adopted EMV, whether the bank or the retailer, is liable for fraudulent in-store purchases. If both parties have upgraded, banks retain liability for the purchase. All of this is good news for consumers, who now have more secure cards in their wallet and continue to enjoy zero-liability protection.

The PIN Diversion
Some retailer trade associations have fixated on arguments that only EMV cards with PINs can prevent fraud. These arguments are flawed and a diversion from the issues at hand. The reality is that:

- It’s the chip that matters because it defeats counterfeit fraud – which is 70% of all in-person fraud.
- PINs only guard against lost and stolen card fraud, an already small and rapidly diminishing portion of overall fraud.
- PINs do not prevent data breaches of substandard retailer systems.
- PINs do nothing to stop counterfeiting or card-not-present fraud (for online transactions), and have the same inherent vulnerabilities as other static security features: they can easily be stolen and used to commit fraud.
- Data shows that hackers increasingly target PINs: a report by the Federal Reserve Bank of Atlanta found that PIN debit fraud rates increased more than threefold over an eight-year period from 2004-2012.

As new threats emerge, retailers’ efforts to divert policymakers’ attention to PINs means that we run the risk of not devoting requisite energy and resources to developing the cutting-edge technologies needed to thwart increasingly sophisticated hackers.

Prioritizing a Holistic Approach to Payments Innovation
While EMV chips are a necessary step toward a more secure system, they are not a silver bullet. Chip technology better protects customers at the register, but it cannot safeguard all types of payment transactions. Technologies like tokenization, which is used with mobile wallets like Apple Pay and can protect online purchases, will play an increasingly vital role in keeping data safe. It is critical that the payments industry and our partners invest in such tools.

The Data Security Act of 2015: Protecting Consumers Against Data Breaches
When arguing that banks should be forced to issue cards with PINs, retailer trades often fail to acknowledge that PINs would have done nothing to prevent recent high-profile retailer data breaches, which were caused by criminals exploiting vulnerabilities in retailers’ own systems. Entities that hold sensitive consumer financial information, whether banks or retailers, must invest in preventive data security measures that meet a basic standard of security. Some retailer
trade associations complain about the costs of these security measures and, preferring to have the costs of their inaction absorbed by consumers and financial institutions.

Financial institutions are already subject to stringent data security and breach notification standards under the Gramm-Leach-Bliley Act. No similar regime at the federal level applies to retailers, an exemption made long before retailers made the collection, retention, and monetization of “big data” from customers a part of their business models. Times have changed and consumers deserve to know that retailers who demand more personal data than ever before also have real security measures in place. The American Bankers Association believes H.R. 2205, the Data Security Act of 2015, will address this gap in consumer protection by:

- Requiring any entity handling sensitive consumer financial data to meet basic security standards and follow breach notification requirements.
- Enacting the strongest protections for consumers while ensuring flexibility for businesses of all sizes, something other legislative proposals cannot match.

**Investment in the Payments System is Critical**

The payments system is efficient and safe but it cannot operate without continued investment. It is a competitive market with many stakeholders, but security is a non-negotiable cost of doing business – trust is our foundation. Hackers never stop innovating, so staying a step ahead requires enormous resources. Banks and credit unions annually spend billions on innovation in payment security.

**Big Retailers’ Increasingly Dubious Price Cap Fails Consumers, Small Businesses, and Security**

Interchange is a critical part of the system because it covers a range of costs for card-issuing banks and credit unions, including customer service, system efficiency and convenience, the costs of online transactions, protection of customer data, and card production costs. Yet despite the importance of interchange, certain retailers continue to defend failed price-fixing measures that serve to pad their bottom line.

During debate on the Durbin Amendment, which capped debit card interchange, merchants promised Congress that they would lower their retail prices if the measure passed. Six years later, however, those promises have evaporated. Consumers are paying more than ever and the retailer trades which made those “debit discount” predictions to Congress and consumers have yet to explain why the windfall went to big retailers, not American shoppers or into payment security. One major retailer which was breached years after the Durbin Amendment passed had not even invested in keeping security patches current – a situation which their consultants described as “no controls limiting… access to any system.”

Despite their broken promises and mounting evidence that the Durbin Amendment does not serve any public policy purpose, big retailers are lobbying Congress and tying up federal courts to preserve their special break. These efforts are an unfortunate distraction that negatively impacts consumers at a time when big retailers should be investing in security at their own businesses, not attorneys to sue others who are making security investments.
Working Together To Fight a Common Enemy
The payments system will only be secure if everyone—banks, payment networks, retailers and consumers—work together to fight a common enemy. To advance our shared goal, we must work together to advocate for public policy that holds all players to high data security standards and fosters the innovation of security solutions for the future. We hope that retail trades will change their approach to one that puts our mutual customers ahead of parochial economic interests.

For more information, please visit: LetsInnovateNotMandate.com and StopTheDataBreaches.org.