March 15, 2016

To: Members of the U.S. Senate
Members of the U.S. House of Representatives

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

Re: The Facts on Payment and Data Security

The consumer payments industry is committed to protecting consumers' data from hackers, but we need the cooperation of other sectors, like retail. A retail industry trade association is visiting Capitol Hill this week, and they may ask for lawmakers' signatures on a letter to federal regulators regarding data security and payment card Personal Identification Numbers (PINs). We want to alert you that their policy narrative conflicts with the broadly held views of the financial services industry. Even if you are not contacted by this trade, here are a few key facts you should know.

Data Security Starts with Retailer Action, Not PIN Mandates

Some retail lobbyists want the federal government to impose a PIN mandate on every American consumer, small business, and financial institution under the guise of security. But their rhetoric is misleading, and is intended to distract members of Congress from the simple fact that retailer **computer systems remain virtually unregulated** because of an outdated and dangerous loophole.

National retailer groups fail to mention that PINs only protect against the use lost or stolen cards in brick and mortar stores – a small and rapidly diminishing portion of fraud. Although PINs deter some pickpockets who steal cards out of wallets, they ***would not*** have prevented the massive breaches at Target, Home Depot or Neiman Marcus, and other major hacking incidents that resulted from inadequate retailer security investments.

Banks and credit unions are covered by a data safeguarding standard that was put into law almost two decades ago (GLBA). The result has been robust yet flexible data protection standards which are enforced through regular reviews. In the earliest days of the internet, retailers were excluded from these common-sense requirements, allowing them to provide whatever level of security they want. Too often corners are cut.

This "mandatory-for-some, but optional-for-others" approach does not make sense in 2016. Payments flow between retailers and banks, yet consumers are subject to vastly different levels of protection, depending on who holds their payment data. Consumers suffer real harm as a result, including frequent card replacement, identity theft, and hours of hassle that come in the aftermath of a breach.

Cybercriminals around the globe find the U.S. status-quo quite satisfactory, but the unnecessary economic damage being done by these organized crime rings is inexcusable. The payments industry supports the bipartisan, bicameral **Data Security Act of 2015** (H.R. 2205 & S. 961), which would equalize data standards across sectors and make life very tough for hackers. Yet retail groups are actively opposing this

basic level of security.

Although retail trades represent the flexible standards in these bills as regulatory burdens, Home Depot recently agreed to implement substantially similar protocols as part of a class action settlement related to the 2014 data breach which compromised 56 million cards used at their stores.

It's the Chip, Not a PIN, That Matters Most

Banks and credit unions are aggressively upgrading cardholders to EMV "chip" cards. EMV chips, unlike the magnetic stripe found on the back of cards, cannot be counterfeited using data stolen from retailers. This counterfeit-proof chip also creates a one-time use code for each transaction, which criminals cannot reuse for future transactions. The U.S. is already the largest chip card market in the world, with saturation expected to reach 98 percent by the end of 2017. But retailers are lagging behind, choosing not to turn on their chip readers, or even turning them off.

Chip technology is the key security feature, whether the consumer signs for a purchase or enters a PIN. Retailers need to tell criminals that their tills are closed by turning on their chip card readers now.

Investing in security for the future: Despite its significant improvement in security, EMV is not a silver bullet. This is why banks and payment networks are focused on rolling out the newest, most promising technologies: ***end-to-end encryption***, which scrambles consumer information on its path from the point of sale through card network, to the bank and back; ***tokenization***, which replaces sensitive consumer account information at the register or online with a random "token" unusable for fraudulent transactions; and ***biometrics***, which use a fingerprint or retina scan to authenticate a purchase. Unfortunately, some big retailers have turned off these secure options at the register.

Dynamic solutions, not rigid, one-size-fits-all mandates: All of these technologies hold significant promise, and innovation is flourishing in payment security. In a changing threat environment, we need flexible, layered data security, not an unchanging "one-size-fits-all" approach. A clunky government technology mandate would impose more levels of bureaucracy on the very security professionals who are combating new threats.

Big Retail's Broken Interchange Promises

Certain retailers are trying to reignite the interchange debate and double-down on the failed Durbin Amendment to the Dodd-Frank Act, which imposed government price controls on debit card interchange fees. But, like technology mandates, this is another bad policy distraction.

Merchants Have Pocketed Savings They Promised to Consumers: Before the Durbin price cap was implemented, Mallory Duncan of the National Retail Federal promised that "merchants are ready to pass lower swipe fees along to consumers in the form of discounts and other benefits as soon as reform goes into effect…" But a 2014 study by the Federal Reserve Bank of Richmond concluded "few merchants are found to reduce prices or debit restrictions as debit costs decrease," demonstrating that promises of congress price cuts made to Congress during the Durbin debate have evaporated. It just ended up being a redistribution from one sector to another.

Distorting the Market Reduces Financial Inclusion: Many community financial institutions are not-for-profits, and the Durbin Amendment has made it harder to offer the free or low-cost checking accounts which are attached to debit cards. Many community institutions previously depended on interchange revenue to cover the cost of these typically "money-losing" accounts. In fact, an academic study found more than 1 million people, mostly low-income families, have faced the loss of those accounts or increased fees and restrictions since the Durbin Amendment became law. This translates into an annual

wealth transfer of between $1 billion and $3 billion from low-income households to the large retailers that have benefited from the fee cap, all because of arbitrary price controls.

Undermining Security Investments: Big retail trades refuse to support common-sense security standards like those which apply to banks, and now they want to cut off the funding source that the financial sector uses to keep data safe by expanding the Durbin Amendment. Financial institutions route a significant portion of interchange fees toward security of the payments system, but some retailers do not want to share the bill for that security, either. In their proposed world of race-to-the-bottom government price controls, who will make the large investments to keep consumers safe?

The bottom line is that protecting our payments system is incumbent upon all of us: card issuers, payment networks, retailers, policymakers and consumers. 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 about the American Bankers Association's Card Policy Council's ongoing payment security efforts, please visit www.LetsInnovateNotMandate.com.