May 17, 2018

Hon. Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Hon. Maureen K. Ohlhausen
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Hon. Rohit Chopra
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Hon. Rebecca K. Slaughter
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Hon. Noah J. Phillips
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons and Commissioners Olhausen, Slaughter, Chopra, and Phillips:

As you know, the United States is the global center for payments innovation. American technologies and brands have been, and are being, adopted worldwide. Options are growing, participation is increasing, and cost is down for everyone involved. The undersigned organizations represent institutions that have made access to reliable and secure payments a priority.

Our industry is greatly concerned by calls for mandates or for governmental intervention in a marketplace that is clearly working in serving the most sensitive of consumer needs. Above all, we are concerned that the short-term commercial interests of individual companies or sectors should not result in the rigidity and moral hazard that government intervention too often fosters – to the detriment of future competition, real-world security, and innovation.

We are also concerned when a legitimate area of constant improvement, namely security, is used to cloak private interests. The private sector approach to upgrading credit and debit cards to incorporate EMV microprocessors was, by global standards, a success that continues to grow. As you are likely aware, the EMV chip card upgrade was undertaken in large part because of the massive data breaches at major retailers whose internal data security safeguards proved inadequate. These leaks of data from unregulated retailer systems (which were consistently out of compliance with payment card industry security standards) led directly to an increase in counterfeit magnetic stripe payment cards. Thankfully, regulated payment companies, banks, and credit unions stepped up by investing in deploying EMV chip cards -- a plan which has drastically reduced the incidence of counterfeit card fraud. It is important to note that the anti-counterfeiting effects of EMV deployment are purely a result of the EMV *chip*, regardless of the separate cardholder authentication method used (such as signature).

The competing payment systems that exist today were built over time. Historically, network economies – where consumers' and small businesses' desire to use a payment technology to make payments must be matched by businesses' willingness to accept payments in that form — have required significant investment in resources, time, and energy to develop. New payment communication technologies are facilitating that process and new service providers are emerging every day, attracting significant investment– a sign that the competitive market is continuing to work.

At the same time, this competition has resulted in a high level of interoperability so that merchants can use the same equipment to accept transactions for a variety of service providers. Standards have evolved that balance retaining the benefits of, and therefore the incentive for, private innovation with interoperability. In the absence of government mandates, private organizations have incorporated multi-stakeholder participation and facilitated broader use of new payment options, allowing innovators to leapfrog past the basics and focus their startup budgets on those higher-value features which differentiate their particular offering.

This is apparent in our everyday lives: in just a few short years, the legacy options for conducting payment transactions via cash, wire, and checks have been joined by payment cards, smartphone wallets, and even smartwatch payments. Payment cards themselves are evolving. While paying with a card was once limited to fixed-location retailers, electronic payment acceptance is now ubiquitous online and is widely available at smaller retailers such as food trucks and the local farmers markets that previously relied on cash transactions.

As with new payment conveniences, the future of payment security is evolving. The payments industry is committed to improving and deploying layers of security such as next-gen authentication, biometrics, geolocation, neural networks, and end-to-end encryption. Because threats are constantly evolving, an inordinate focus on any single static technology (like antiquated Personal Identification Numbers -- PINs) is an obstacle to the nimble, adaptive approach required to defeat fraudsters. Security and trust are major competitive imperatives and the marketplace's incentives are aligned towards protecting consumers and commercial participants.

This is an exciting time for payments, as innovation constantly breaks boundaries once thought to be permanent and insurmountable. We hope the information in this letter is helpful and we would be pleased to meet with you to discuss how the future of payments is developing.

Sincerely,

American Bankers Association

Consumer Bankers Association

Credit Union National Association

Electronic Payments Coalition

Financial Services Roundtable

National Association of Federally-Insured Credit Unions