Written Testimony of

Jason Oxman, CEO,
The Electronic Transactions Association

Before the
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
Hearing on
"Examining De-risking and its Effect on Access to Financial Services"

February 15, 2018

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee, the Electronic Transactions Association ("ETA") appreciates the opportunity to submit this statement for the Subcommittee on Financial Institutions and Consumer Credit hearing on "Examining De-risking and its Effect on Access to Financial Services."

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, all parts of the payments ecosystem, mobile payment service providers, mobile wallet providers, and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders.

The focus of this hearing – de-risking and financial inclusion – is closely tied to our industry's ongoing efforts to fight fraud and ensure all consumers have access to safe, convenient, and affordable payment options and other financial services. Today is, without a doubt, an exciting time in the payments industry. Consumers continue to benefit from a robust credit card payment system that provides nearly universal payment access and strong consumer fraud protections. Consumers can also pay for goods and services using their mobile devices, which may incorporate various payment options through "apps," including payment by credit card, debit card, automated clearing house ("ACH"), virtual currencies, and various closed loop payment systems. And, for small businesses, ETA's members are using technology-based credit solutions to increase the number and types of small businesses able to access credit, especially those unserved or underserved by traditional lenders

Notwithstanding this progress, there have been challenges along the way. Operation Choke Point, in particular, and other similar government enforcement initiatives, have contributed to bank de-risking that ultimately limits consumer access to financial services while also making it more

difficult for legitimate businesses to access payment systems. For the remainder of this statement, I would like to highlight the efforts of ETA members and the payments industry to combat fraud and explain why a collaborative approach between government and industry – as opposed to an enforcement approach – is the best way to protect consumer interests and expand financial inclusiveness.

Industry's Active Role in Keeping Fraud Off Payment Systems

ETA strongly supports the vigorous enforcement of existing laws and regulations to prevent fraud. Consumers in the United States choose electronic payments over cash and checks because they have zero liability for fraud, making electronic payments the safest and most reliable way to pay. As a result, payment companies are generally responsible for paying for fraud involving payment systems under federal law and payment network rules, and thus our members have a strong interest in making sure fraudulent actors do not gain access to payment systems. In 2016, there was nearly $6 trillion in debit, credit, and prepaid card transactions in the United States, but there was only $9 billion in credit card fraud. In addition, a recent survey of ETA members indicates that more than 10,000 merchants were discharged last year for fraud. actions demonstrate the commitment of ETA members to keeping fraudulent actors off payment systems.

Despite this strong record, however, payment processors can never take the place of regulators and law enforcement in protecting consumers. Because regulators and law enforcement can issue subpoenas, conduct investigations, and have far greater resources, personnel, and legal authorities, they will always be in a better position to combat fraud. Yet, payments companies are committed to doing their part.

With the benefit of decades of payment system expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems and

to terminate access for network participants that engage in fraud. These programs have helped to keep the rate of fraud on payment systems at remarkably low levels.

In an effort to further strengthen payment systems, ETA published in 2014 its "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" ("ETA Guidelines"). This document provides more than 100 pages of methods and suggested best practices to detect and halt fraudulent actors. Similarly, in 2016, ETA published "Payment Facilitator Guidelines," which provide payment facilitators with guidance on settlement, registration, funding delays, fraud, security, and related issues. These two documents were developed by ETA's member companies and other industry stakeholders through months of collaborative discussions and sharing of techniques to prevent fraud. Throughout this process, ETA has shared preliminary draft guidelines with, and sought comments from, the Federal Trade Commission ("FTC"), which had strongly encouraged the industry to strengthen its anti-fraud efforts.

The ETA Guidelines, in particular, provide a practical and targeted approach to combating fraud on payment systems. ETA members already have a strong commitment to, and financial interest in, keeping fraudulent actors off payment systems, and the targeted nature of the ETA Guidelines gives members enhanced tools to improve the effectiveness of their practices and help ensure that law-abiding merchants do not unfairly lose access to payment systems due to overly broad anti-fraud protections. ETA continues to actively encourage its members and companies across the payments ecosystem to make use of the Guidelines, especially smaller companies that may not have the resources to develop such advanced practices on their own.

ETA reviews its guidelines regularly, and, in connection with this hearing, ETA is announcing the publishing of a 2018 update to the ETA Guidelines. The updated ETA Guidelines contain updated sections that reflect the current best practices in the industry. In addition, the ETA

Guidelines were updated to the Financial Crimes Enforcement Network's new beneficial ownership rule, which becomes mandatory in May 2018.

A final benefit of the ETA Guidelines is that they provide a basis for payments companies to work cooperatively with federal regulators and law enforcement toward the common goal of stopping fraud. ETA strongly believes that such a collaborative approach is good public policy - it encourages companies to cooperate with law enforcement by fostering an environment of open communications between government agencies and payments companies. Unfortunately, such cooperation has not always been the case. Operation Choke Point, for example, employed the wrong legal tools, was unnecessarily confrontational, and created serious risks to law abiding processors and merchants without producing any benefits to consumers beyond those which could be obtained with a more industry-focused and collaborative approach.

Operation Choke Point Was the Wrong Approach

In an August 16, 2017 letter to Congress the Department of Justice ("DOJ") stated that Operation Choke Point "is no longer in effect, and it will not be undertaken again." Operation Choke Point was a DOJ initiative that aimed to limit the ability of fraudsters to access the banking system. The DOJ sought to implement Operation Choke Point by initiating investigations and civil suits under the Financial Institutions Reform, Recovery, and Enforcement Act, 12 U.S.C. § 1833a ("FIRREA").

Operation Choke Point was premised on the flawed assumption that increasing liability on lawful payments companies for the actions of fraudulent merchants would yield only benefits to consumers. In practice, however, imposing new liability standards on such institutions had serious adverse consequences for not only law-abiding merchants (de-risking), but also consumers generally. In particular, the blunt force of Operation Choke Point discouraged banks and other

financial service providers from forming relationships with merchants or other businesses deemed high-risk, leading to the "de-risking" of entire industries. De-risking can undermine financial inclusion, financial transparency, and financial activity.

ETA testified before this Subcommittee on these and other challenges presented by Operation Choke Point. Examples of the risks presented include:

- From a public policy perspective, the federal government should not restrict the access of law-abiding merchants to the payment systems. Enforcement actions against payment systems are an inappropriate tool for regulators to use to limit the ability of consumers to access legal but currently disfavored industries.

- Operation Choke Point and other similar initiatives put banks, payment processors, and other financial institutions in the difficult position of having to increase the prices of payment services for merchants and/or restrict access to payment systems to manage their expanded liability exposure. Invariably, the brunt of these burdens fall on small, new, and innovative businesses because they pose the highest potential risks.

- Consumers ultimately pay for the higher costs arising from increased liability, and are also harmed by the inconvenience of not being able to use their preferred methods of payment (credit, debit, and prepaid cards) with some merchants due to more restrictive access to payment systems. Similarly, consumers would be harmed if new liability on processors impedes continued innovation in electronic payments.

We know from our many opportunities to participate in hearings such as this that Congress shares many of these concerns. While the announced end of Operation Choke Point may be an important moment for the payments industry, it is equally important to recognize that there is nothing to stop the Department of Justice – or, for that matter, the Consumer Financial Protection Bureau ("CFPB"), the Federal Trade Commission ("FTC"), or a state attorney general – from bringing a case that looks very much like those that arose under Operation Choke Point.

Currently, the FTC can assert jurisdiction over payment processors that engage in unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act, and

violations of the Telemarketing Sales Rule.[1] The FTC also can bring cases against payment processors for "assisting and facilitating" a merchant's violations of the Telemarketing Sales Rule, but such liability only applies if a payment processor "knows or consciously avoids knowing" that the merchant violated the rule.[2] The FTC has expressed virtually a zero tolerance policy for credit card processors and independent sales organizations ("ISOs") that allow any such merchant to access the payments system when the processor or ISO knew or should have known that the merchant was engaged in such conduct.

The CFPB has been equally aggressive in pursuing actions against payment processors – which has lead in several cases to the CFPB's actions being dismissed in court. For example, in June 2016, the CFPB attempted a broad-scale lawsuit against payment processor Intercept Corporation and two of its executives for enabling withdrawals from consumer accounts on behalf of Intercept's payday lenders, auto-title lenders, debt collectors, sales financing, and other clients. In March 2017, a federal judge in North Dakota dismissed the CFPB's lawsuit because the CFPB did not include specific factual allegations about how Intercept violated industry standards or what Intercept had done wrong to cause injury to consumers.

Later that year, a federal Judge in Northern District of Georgia dismissed a CFPB case that had been filed against Global Payments and several other payments companies. In that case, the CFPB alleged that the payment processors had failed to conduct sufficient due diligence before providing certain merchants with accounts and ignored red flags once the merchants had been boarded. The judge ultimately dismissed the CFPB's case after the CFPB failed to comply with reasonable demands by defendants and orders by the court to play fair in the litigation.

---

[1] 15 U.S.C. § 45; 16 C.F.R. § 310.
[2] 16 C.F.R. § 310.3.

While ETA members share a commitment to protecting consumers from harm, ETA is concerned that these Operation Choke Point-type enforcement actions will continue to put pressure on its members to shun entire lines of business out of a fear that the members could be called upon to financially insure the total volume of a merchant's sales transactions. A more sensible policy recognizes the strong interest the payments industry has in preventing fraud and other illegal activities, and allows industry to focus on enhancing its underwriting and risk management tools to safeguard the payments system from unscrupulous merchants.

The Role of the Payments Industry in Promoting Financial Inclusion

Where Operation Choke Point caused de-risking, ETA members have been working diligently to expand consumer access to payment options, credit, and other financial services. One of the goals of our financial system is to provide high quality, affordable financial services for the broadest possible set of consumers. An inclusive financial system is one that provides consumers and businesses with access to a variety of financial products and services.

Over the past decade, financial institutions, payments companies, and financial technology companies have transformed the financial landscape through the introduction of new technologies that expand financial offerings for consumers, lower costs, improve financial management, and increase transaction security. These products and services – often referred to as "fintech" – have also expanded, and are continuing to expand, financial opportunities for underserved consumers. Examples of these include:

- Prepaid Products – Provide cost-effective, convenient, and innovative payment options for millions of consumers, including those that may not have access to traditional financial accounts.
- Mobile Banking Services – Provide financial independence and security for those demographic groups that lack easy access to physical FI branches, such as consumers in rural areas, the elderly, or persons with disabilities.

- Mobile Payments – Provide an exciting alternative to cash and checks that allow consumers to pay for goods and services in an efficient, cost-effective, and secure manner.
- Peer-2-Peer Payments – Enable consumers to send money to each other via mobile applications.
- Expanded Internet Access – Expands affordable access to the internet in underserved communities domestically and abroad by improving infrastructure and reducing costs so that more people can connect to the web-based world.
- Interactive, Automated Tellers – Transform traditional FI branches by making them economically sustainable in previously underserved communities.
- Online Small Business Lending – Expands access to credit for small businesses seeking capital to grow their businesses.
- Financial Literacy & Readiness Programs – Empower consumers to take control of their finances and prepare for the future.

As the leading trade association for the payments industry, ETA and its members encourage policymakers to support these efforts through policies that encourage innovation and the use of technology to improve financial inclusion for all consumers. ETA advocates that policymakers remain thoughtful and forward-thinking in how to best support the industry's on-going efforts to provide opportunities for all consumers and small businesses to access and benefit from innovative financial products and services. Efforts by policymakers to regulate financial products and services should be done collaboratively and with careful consideration. We encourage the government to be sensitive to the risk that applying a uniform or overly-restrictive regulatory framework to fintech products and services, without any appreciation of differences in products and services and consumer needs, will likely stifle creativity and innovation in the market (and potentially contribute to de-risking of these new and growing industries). Such an outcome would harm consumers, particularly at a time when new technologies, products, and services are providing the underserved with unprecedented access to FI and fintech company financial products and services.

Examples of Other Policy Recommendations to Encourage Growth and Inclusiveness

As discussed throughout this statement, ETA members are at the forefront of economic development by fighting fraud and expanding access to financial services for both consumers and small businesses. From a policy perspective, however, there is much that can be done to further encourage such activity. ETA supports a positive regulatory environment for financial innovation and has outlined several proposals below to achieve that goal.

Support the OCC Fintech Charter - ETA supports the Office of the Comptroller of the Currency's ("OCC") proposal to offer a limited-purpose national bank charter to financial technology, or "fintech," companies. Such a charter will provide numerous public policy benefits, including a regular and consistent regulatory framework for chartered fintech companies and increased competition to develop cost-efficient, inclusive products and services. ETA supports the OCC's chartering initiative and encourages the OCC to work collaboratively with the fintech community to develop a process that takes full advantage of the potential benefits offered by the proposed fintech charter.

National Cybersecurity Requirements – ETA supports a national cybersecurity approach. State-specific attempts to regulate cybersecurity undermine the progress that federal and self-regulatory efforts have made in combatting cybersecurity threats in the financial industry. The introduction of overlapping and potentially conflicting state regulations causes confusion and compliance challenges for the financial industry. ETA believes that a flexible national framework is the most effective approach for addressing cybersecurity risks and would encourage efforts to preempt a patchwork of state-specific requirements in this area.

National Data Breach Requirements – ETA supports a national data breach approach. Almost every state has its own data breach law which can leave consumers with inconsistent

protection and companies in the difficult position of dealing with conflicting requirements. One national standard will provide certainty and predictability to consumers and industry.

Conclusion

ETA's members have made great progress in expanding access to affordable, safe, and convenient payment methods and other financial services. To maintain this progress, there needs to be a careful balancing between the need to limit access to payment systems to prevent fraud and the need to ensure that all law-abiding businesses can access payment systems. A cooperative approach to combating fraud is far more likely to strike the right balance than blunt enforcement actions. Accordingly, ETA encourages Congress, federal regulators, and industry to work cooperatively toward our common goal of preventing fraud and expanding financial inclusion.

On behalf of ETA, thank you for the opportunity to provide this testimony before the Subcommittee.

For more info, please visit. www.electran.org