ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Statement for the Record of
The Electronic Transactions Association
Before the
Committee on Oversight and Government Reform
Subcommittee on National Security and Subcommittee on Government Operations
Hearing on
"The Federal Trade Commission's Enforcement of Operation Chokepoint-Related Businesses"

July 26, 2018

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Chairman DeSantis, Ranking Member Lynch, Chairman Meadows, Ranking Member Connolly, and members of the Subcommittees on National Security and Government Operations, the Electronic Transactions Association ("ETA") appreciates the opportunity to submit this statement for the hearing on "The Federal Trade Commission's Enforcement of Operation Chokepoint-Related Businesses."

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, payment processors, and all other parts of the payments ecosystem (collectively "payment processors"), as well as non-bank online lenders that make commercial loans, primarily to small businesses.

This hearing comes at a critical time for the payments industry. Although ETA supports the enforcement of existing laws and regulations by federal agencies to stop fraud by unscrupulous merchants, we are deeply troubled by the Federal Trade Commission's ("FTC") increasingly aggressive use of Operation Choke Point-type tactics to hold payment processors and even individual owners and employees of processors financially responsible for fraud committed by merchants. The FTC has been targeting payment processors for over 20 years, and while the FTC's actions have received less scrutiny than those of other agencies, it has escalated the frequency of its enforcement and severity of its tactics in recent years.

The continued use of the discredited Operation Choke Point enforcement theory is concerning given that the Department of Justice ("DOJ") ended its own Operation Choke Point in 2017 following years of Congressional scrutiny and criticism. That scrutiny demonstrated that imposing liability on payment processors for *merchant fraud and misconduct* has serious adverse

consequences, including processors fearfully abandoning lawful industries disfavored by the FTC and higher prices for consumers.

To be sure, ETA recognizes that there have been a few, isolated instances when a payment processor actively participated in merchant fraud, and we support the FTC in protecting consumers in those rare cases. But while the FTC justifies its targeting of the payments industry based on these handful of cases, the Commission's testimony does not address the dozens of nonpublic investigations and overly burdensome and costly investigative requests it launches each year against payment processors that did not engage in egregious conduct. Responding to these investigations can cost processors millions in legal fees and lost productivity. Also left unaddressed is the fact that the FTC has been ratcheting up the aggressiveness of its discovery and investigation tactics in recent years to place additional pressure on payment processors. The *in terrorem* effect of the FTC's efforts has been for legitimate processors to abandon providing services to certain types of lawful merchants that the FTC staff disfavors. This forces merchants to use overseas processors, which pushes jobs overseas and often leaves consumers with fewer protections.

For the remainder of this statement, I would like to highlight the efforts of ETA members and the payments industry to combat fraud, discuss the flawed premise underlying the FTC's approach to enforcement, along with examples of enforcement overreach and abuse, and explain why a collaborative approach between government and industry – as opposed to an enforcement approach – is the best way to protect consumer interests while encouraging innovation and growth in the critically important payments industry.

The Payments Industry's Active Role in Fighting Fraud

The payments industry is dedicated to using innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. Our members, for example, are service provides that work on behalf of sponsor banks to set up merchants with payment processing accounts so that consumers can purchase goods and services in person, online, or through a mobile phone. Indeed, consumers choose electronic payments over cash and checks because they have zero liability for fraudulent charges, making electronic payments the safest and most reliable way to pay. In most cases, payment processors bear financial responsibility for fraud involving payment systems under federal law and payment network rules. When it comes to credit cards, for example, a consumer can submit a chargeback request to his or her card issuing bank disputing a particular card transaction. This process serves to protect consumers and ensures that the acquiring bank or merchant bears ultimate responsibility for fraudulent transactions. Thus, our industry has a strong interest in making sure fraudulent actors do not gain access to payment systems.

In addition, the payments industry has a long history of fighting fraud through the implementation of robust underwriting and monitoring policies and procedures. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. In 2014, ETA published its "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" ("ETA Guidelines"), which was updated earlier this year. This document provides more than 100 pages of best practices to detect and halt fraudulent actors. Similarly, in 2016, ETA published "Payment Facilitator Guidelines," which

provide underwriting and diligence guidance tailored for payment facilitators, including information on registration, funding, anti-fraud tools, 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 shared preliminary draft guidelines with, and sought comments from, the FTC, which had encouraged the industry to strengthen its anti-fraud efforts.

The ETA Guidelines, in particular, provide a practical 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.

These efforts have helped to keep the rate of fraud on payment systems at remarkably low levels. In 2016, there was $31.878 trillion in credit, debit, and prepaid card transactions across the world, but only $22.80 billion in fraud losses (which were covered by the card acquirers and merchants).[1] This equates to a fraud rate of .07% of all global card transactions.

[1] The Nilson Report (Oct 2017).

The FTC's Increasingly Aggressive Targeting of Payment Processors

The FTC has been bringing enforcement actions against payment processors since 1996, and has continued to bring numerous cases almost every year since. In this regard, the FTC's targeting of the industry actually predates the DOJ's Operation Choke Point and exceeds the DOJ's efforts in scope, but has somehow managed to fly under the radar. While the DOJ abandoned Operation Choke Point in 2017 in response to Congressional scrutiny, the FTC has forged ahead, taking on more cases and, as explained below, engaging in even more aggressive enforcement tactics to bully the payments industry.

According to the FTC, it has brought 25 enforcement actions against various types of payments companies since 1996. Although these cases involved allegations of egregious conduct, the FTC does not address the many non-public investigations that it launches against the payments industry each year. These investigations fall into several categories, including investigations of merchants, entire industries, and processors themselves. In the case of investigations of merchants, our members frequently receive civil investigative demands ("CIDs") from the FTC asking for dozens of categories of information about dozens of different merchants. Like a subpoena, a CID requires the recipient to provide the FTC with requested information and documents. It takes significant staff time, and often outside counsel legal assistance, to collect, organize, and produce these materials to the FTC. And many of our processors receive multiple CIDs a year, often part of a broader FTC fishing expedition around a particular industry, such as businesses providing education to consumers on how to earn money.

In addition, the FTC ignores that payment processors often serve thousands or even millions of customers, the vast majority of which are the type of law-abiding, small businesses that

serve as the backbone of our economy. Even though processors do their part to fight fraud through robust underwriting and monitoring, they are simply not equipped (nor could they be) with the same resources or expertise as law enforcement to root out all potential fraud. And, studies have shown there is "no basis for believing that a processor's ability to monitor return and chargeback transactions, and to do financial underwriting on the basis of such data, translates into the ability to make meaningful inferences about law enforcement matters" or to discern legitimate businesses from frauds.[2] The fact is that sometimes processors miss red flags or make mistakes, but when they do, it's a big leap to suggest that the processor was intentionally aiding and abetting a merchant in fraud and should be left to cover the total amount of consumer injury caused by the merchant or even put out of business.

Perhaps most concerning is that the FTC continues to hold payment processors, and even individual owners and employees responsible for the total volume of sales transactions processed for a merchant, even where the processor made just pennies on the dollar for such transactions. Emboldened by the recent, but misguided, Eleventh Circuit decision in *Universal Processing v. FTC*, the FTC's aggressive use of joint and several liability represents a tremendous shift of the regulatory burden for merchant fraud to payment processors and individual owners and employees, in some cases.

This tactic essentially conscripts payment processors to police and insure the behavior of their merchant clients, a function that payment processors are ill-positioned to perform. It also threatens to put targeted processors out of business or to bankrupt individuals based on the conduct

[2] Jeffrey A. Eisenach, Economic Effects of Imposing Third Party Liability on Payment Processors, NERA Economic Consulting (July 2014), at 7, available at www.electran.org/wp-content/ uploads/Exhibit-A-NERA-Study.pdf

of a single bad merchant out of the processor's entire portfolio. And, as discussed in greater detail below, the FTC has made it impossible for the industry to protect against this new financial risk because the FTC aggressively seizes any reserves that a processor withholds to cover chargebacks and consumer refunds.

As a result, processors are left with an unfair responsibility to "guarantee" their merchant's conduct, but without any means to protect themselves financially. In this regard, one is reminded of the FTC's unfairness doctrine, which aims to protect consumers from harms they could not themselves have reasonably have avoided. The same is happening here, except that the FTC has imposed a regulatory burden on payment processors that they cannot reasonably address. There is no insurance available to processors to protect against this risk, and they cannot reasonably be expected to "police" their portfolios to the same standards as a regulator. Yet even a single misstep by a processor in failing to catch a clever fraudster can result in an FTC enforcement action that forces the processor to shut down operations.

Examples of FTC Enforcement Overreach and Process Abuses

The DOJ announced the end of Operation Choke Point in 2017, but the FTC continues to charge ahead relatively unnoticed. In fact, the FTC appears to have gone several steps beyond Operation Choke Point in targeting the industry through the use of aggressive – some might say abusive – investigation, discovery, and enforcement tactics. This is a deeply troubling development for several reasons, including that the FTC's aggressive posture threatens the payments industry's long history of cooperation and success in fighting fraud.

The following examples are just a few of the scorched earth, winner take all tactics that the FTC uses against the payments industry. It is important for Congress to understand that the FTC

uses the same aggressive tactics in all cases, even where industry cooperates to assist in the FTC's law enforcement activities.

1. The FTC's insistence on joint and several liability for payment processors makes it almost financially impossible for a processor to try and defend itself in court. In terms of simple economics, a small processor that earns a few thousand dollars processing for a merchant cannot take the risk of litigating against the FTC when the FTC seeks to hold the processor liable for millions of dollars. Likewise, in cases where the FTC looks to hold a processor's individual owner or employees financially responsible for the entire volume of a merchant's sales transactions, the individual has no realistic choice but to settle, which usually involves the individual having to turn over all of his or her assets (and family possessions) to the FTC after invasive financial discovery.

2. When the FTC sends a CID to a processor or bank regarding a merchant, the CID will advise the processor or bank to maintain confidentiality and continue processing for the merchant that is the target of the investigation. This forces banks and processors to continue processing transactions for merchants that are under active investigation, which increases the processor's liability when the FTC inevitably turns on the processor and seeks to hold it financially liable for the merchant's sales. And often, as noted, the FTC sends CIDs to processors that blanket an entire industry of merchants.

Similarly, in cases in which a court appoints a receiver to manage a merchant's assets, the FTC freezes reserve accounts and then pressures the receiver to take possession of a processor's reserves for the merchant. This practice is questionable given that the receiver is supposed to stand in the place of a merchant, which has no contractual right to demand access to the reserves until all chargebacks and other liabilities are paid out by the processor and bank. Again, the result of

having to relinquish the reserves is that a processor is forced to cover chargebacks out of its own funds, which creates financial instability for the processor.

3. The FTC refuses to discuss settlement of a case against a processor until the processor or its individual owner provides financial disclosures to the FTC, which the FTC then uses as a financial floor for settlement discussions, irrespective of the economics of the underlying case. This is nothing more than a shake down designed to ensure that the FTC extracts every dollar possible from a processor or individual owner for the wrongful conduct of a merchant. This risks putting processors out of business or bankrupting individual owners, who are often forced to liquidate or hand over to the FTC almost every asset they own.

4. The FTC engages in aggressive prosecution of individual officers and employees at processors for "assisting and facilitating" the conduct of a merchant customer, even when the employee or officer had little or no control over the alleged unlawful conduct. In certain instances, the FTC has banned individuals from making a living in their chosen profession simply to send a message to the industry as a whole.

5. Almost all CIDs issued to merchants in connection with FTC investigations seek information on the merchant's payment processors. Once this information is obtained, the FTC routinely sends CIDs to all of the merchant's processors and banks for information on the merchant and its processing activities. In many cases, it appears that the FTC may also be sending CIDs to processors without having opened a formal investigation of a merchant. ETA understands the need for the FTC to obtain information in connection with investigations, but the FTC should not use the payments industry as an information resource except where there is a legitimate, identified need for specific information. Responding to CIDs is an expensive and time consuming process,

and the FTC must take these costs into account before sending out CIDs with dozens of requests for information about dozens of merchants to processors.

6. The FTC regularly uses its CID process to request information from third parties when that information is readily available from the target of the investigation. We can think of no justification for this tactic other than as an attempt by the FTC to intimidate banks, processors, and other key service providers into terminating their relationships with the target of the investigation.

For example, in a confidential ongoing investigation, the FTC sent CIDs to every financial institution that was connected in any way with the target or its principals, even where those institutions had nothing to do with the conduct being investigated, or the information requested was not necessary to determine whether any law had been violated. These CIDs have unnecessarily threatened the target's banking and processing relationships. In doing so, the FTC staff appears to be attempting to choke off the ability of an entire legal industry it disfavors to access banking and payments services.

Moreover, the CIDs to the banks and processors continued after the target learned of the investigation, agreed to cooperate, and had received its own CID. Importantly, the FTC did not request that the target produce the type of information that the FTC had requested from the third parties, even though the target could have easily provided the information. While it may be appropriate for the FTC to engage in such conduct when it does not want a company to know it is being investigated, in the instant case the motive seems to be to damage the target's business relationships before the FTC has even brought an enforcement action.

7. The FTC is increasingly reaching out to the card networks through CIDs and even informal means to obtain information on processors and their merchants, which has resulted in

card network scrutiny of processors – even where the FTC does not bring an investigation. Our payment processor members have noticed a frequent correlation between when they receive an FTC CID regarding a merchant in a particular industry, and a subsequent notice from a card network related to an audit or request for information on the processor's merchants in the same industry. There is a significant financial cost to processors in responding to these inquiries.

8. In a number of recent cases the FTC has pushed beyond its territorial jurisdiction by targeting foreign banks, processors, and merchants, even though the FTC lacks extraterritorial jurisdiction over such activities under the Safe Web Act amendments to the FTC Act. As part of these efforts, the FTC has grabbed foreign processors' reserves that are meant to protect them and their foreign consumers that initiate chargebacks.

* * * * *

One of the challenges for payment processors, as noted above, is that the FTC's insistence on joint and several liability makes it near impossible for payment processors to defend themselves in court. Where the FTC cites to a handful of egregious cases in its testimony to support its approach, there are relatively few "public" examples of overreach because of the FTC's ability to force companies to settle investigations under the threat of joint and several liability.

But it is worth noting that when payment processors have fought in court, most recently, for example, against the Consumer Financial Protection Bureau ("CFPB"), they have had success in discrediting Choke Point-type enforcement actions. In June 2016, the CFPB attempted a broad-scale lawsuit against payment processor Intercept Corporation and two of its executives for providing payments services to payday lenders, auto-title lenders, debt collectors, sales financing companies, 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 the 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 dismissed the CFPB's case after the CFPB failed to comply with reasonable demands by defendants and orders by the court to identify with more specificity the alleged wrongful conduct by the processors.

Why Targeting Payment Processors Harms Industry and Consumers

The FTC has taken Operation Choke Point to a new level through its focus on holding processors jointly and severally liable and its aggressive discovery and enforcement tactics. The FTC states in its testimony that it aims to achieve maximum benefits for consumers, but we are not aware of any study conducted by the FTC analyzing the collateral damage brought by its aggressive enforcement efforts. In fact, like Operation Choke Point, the FTC's misguided enforcement approach will result in significant negative repercussions for processors, merchants, and consumers. The cumulative effect of the threat of joint and several liability, the costs of responding to multiple CIDs, and having reserves taken away creates risks and costs for processors that threaten their existence if they decide to do business with industries the FTC disfavors, such as businesses providing education to consumers on how to earn money. This is Operation Choke Point at its worst.

First, from a public policy perspective, the federal government should not engage in enforcement efforts intended to restrict or otherwise discourage 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 industries that happen to be disfavored by a government agency.

Second, the FTC's enforcement approach, including its focus on joint and several liability, places liability on processors for fraud committed by merchants – and not just for the refund of pending chargebacks, but in many cases for the entire proceeds of a merchant's allegedly illegal activity and for the entire period that merchant used the processor's services, simply because the payment processor is solvent while the wrongdoer is not. Payment processors, however, have no way to protect against this increased liability exposure. Under the FTC's theory, even a single bad merchant out of a portfolio of thousands or hundreds of thousands of merchants could bankrupt a payment processor or individual owner in the case of privately held companies. And even if processors were to increase reserves to protect against increased liability, the FTC has demonstrated that it will seize every last dollar held by a processor, effectively leaving processors with no way to insure against financial risk.

In response to this increased risk, banks, payment processors, and other financial institutions have had no choice but 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. The only alternative that many of these merchants have is to use processors located

overseas. This can result in higher costs for the merchant, less oversight of transactions, and harm to the economy generally by pushing jobs to foreign countries.

Third, consumers will 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. This increased liability will also harm consumers through less innovation in electronic payments.

Finally, the FTC's aggressive enforcement posture focuses payment processor resources on responding to costly and time-consuming investigations and litigation by multiple regulators instead of fighting fraud. Although the payments industry has a remarkable record of success in preventing the use of payments systems for illegal activities, the FTC's continued targeting of the payments industry threatens this success to the detriment of merchants and consumers. And, as noted, there is already a robust chargeback system in place to protect credit card holders from fraud, meaning that the FTC's additional efforts are unnecessary in the first instance.

A Better Path Forward

While ETA members share a commitment to protecting consumers from harm, ETA is concerned that the FTC's enforcement actions are pressuring 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.

As discussed throughout this statement, ETA members are willing to do their part to fight fraud. From a policy perspective, however, there is much that can be done to encourage collaboration between industry and law enforcement:

1. Congress should encourage the FTC to review and reconsider its overly aggressive use of CIDs and questionable discovery and enforcement tactics. ETA applauds the efforts of former Chairman Ohlhaussen, who in 2017 announced efforts to reform the FTC's CID process, including steps to minimize the burden of responding to CIDs. The FTC should revisit this issue in light of the concerns raised by the payment industry.

2. Congress should include a provision in the FTC's budget authority limiting the FTC's ability to seek joint and several liability against payment processors except where the processor is alleged to be a part of a common enterprise with the merchants.

3. Congress should direct the FTC to halt all enforcement actions against payment processors until the FTC engages in a public workshop investigating the impact of Operation Choke Point-type enforcement actions on small businesses, consumers, and the economy as a whole.

4. Congress should encourage the FTC to support additional industry self-regulation, such as ETA's development of the ETA Guidelines and Payment Facilitator Guidelines. These documents provide a basis for payment processors 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 payment processors.

In the meantime, the payments industry will continue to fight fraud to the best of its ability and cooperate with law enforcement to the greatest extent possible.

Conclusion

Today, it is recognized that DOJ's Operation Choke Point was premised on a flawed assumption that targeting lawful payment processors for the actions of fraudulent merchants would yield only benefits to consumers. In practice, this assumption has had serious adverse consequences for the payments industry, merchants, and consumers. Fortunately, Congress commenced a series of investigations into Operation Choke Point and the negative impact it was having on the payments industry and the economy at large. On several occasions ETA testified before Congress on these and other challenges presented by Operation Choke Point, including on how the initiative was harming the payments industry, businesses, and ultimately consumers.

Our members are now raising similar concerns with respect to the FTC, which has largely flown under the radar in carrying out its own aggressive targeting of the payments industry for over a decade. We ask that Congress take a closer look at the FTC's enforcement practices and tactics outlined in this testimony. The FTC's actions, just like Operation Choke Point, are harming the payments industry, merchants, and consumers. We believe a cooperative approach to combating fraud is far more likely to strike the right balance than the FTC's 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.

Committee on Oversight and Government Reform
Witness Disclosure Requirement — "Truth in Testimony"

Pursuant to House Rule XI, clause 2(g)(5) and Committee Rule 16(a), non-governmental witnesses are required to provide the Committee with the information requested below in advance of testifying before the Committee. You may attach additional sheets if you need more space.

Name: Jason Oxman

1. Please list any entity you are representing in your testimony before the Committee and briefly describe your relationship with each entity.

Name of Entity	Your relationship with the entity
Electronic Transactions Associaiton	CEO

2. Please list any federal grants or contracts (including subgrants or subcontracts) you or the entity or entities listed above have received since January 1, 2015, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount
None	n/a	n/a	n/a	n/a	n/a

3. Please list any payments or contracts (including subcontracts) you or the entity or entities listed above have received since January 1, 2015 from a foreign government, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount
None	n/a	n/a	n/a	n/a	n/a

I certify that the information above and attached is true and correct to the best of my knowledge.

Signature  Date: 7.20.18

Jason Oxman

CEO

Electronic Transactions Association

Biography

Jason Oxman is the CEO of ETA, the global trade association of the payments technology industry. Since joining in 2012, Oxman has led ETA and its membership through unprecedented technological transformations, and ETA now represents more than 500 global financial and technology companies. ETA also owns and produces TRANSACT, the premier annual event for the payments technology industry, and is the voice of the payments industry on Capitol Hill.

Before joining ETA, Oxman was Senior Vice President of Industry Affairs of the Consumer Electronics Association, prior to which he served as general counsel of a technology industry trade association and vice president of a Silicon Valley-based technology company. He worked at the Federal Communications Commission to develop and implement technology policy. He began his legal career as a law clerk for the Maine Supreme Court, and he is also a former broadcast journalist. Oxman received his B.A. *cum laude* from Amherst College, and his M.S. and J.D. from Boston University.

Contact Information

Email: joxman@electran.org
Twitter: @joxman