THE FEDERAL TRADE COMMISSION'S ENFORCEMENT OF OPERATION CHOKEPOINT–RELATED BUSINESSES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY

AND THE

SUBCOMMITTEE ON
GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 26, 2018

Serial No. 115–99

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.govinfo.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

31–425 PDF WASHINGTON : 2018

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana
Michael Cloud, Texas

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Jimmy Gomez, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Stacey E. Plaskett, Virgin Islands
John P. Sarbanes, Maryland

SHERIA CLARKE, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
SHARON ESHELMAN, *National Security Subcommittee Staff Director*
JULIE DUNNE, *Government Operations Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY

Ron DeSantis, Florida, *Chairman*

Steve Russell, Oklahoma, *Vice Chair*
John J. Duncan, Jr., Tennessee
Justin Amash, Michigan
Paul A. Gosar, Arizona
Virginia Foxx, North Carolina
Jody B. Hice, Georgia
James Comer, Kentucky

Stephen F. Lynch, Massachusetts, *Ranking Minority Member*
Peter Welch, Vermont
Mark DeSaulnier, California
Jimmy Gomez, California
John P. Sarbanes, Maryland
Vacancy
Vacancy

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

Mark Meadows, North Carolina, *Chairman*

Jody B. Hice, Georgia, *Vice Chair*
Jim Jordan, Ohio
Mark Sanford, South Carolina
Thomas Massie, Kentucky
Ron DeSantis, Florida
Dennis A. Ross, Florida
Rod Blum, Iowa

Gerald E. Connolly, Virginia, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey

CONTENTS

THE FEDERAL TRADE COMMISSION'S ENFORCEMENT OF OPERATION CHOKEPOINT–RELATED BUSINESSES

Thursday, July 26, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, JOINT WITH THE
SUBCOMMITTEE ON GOVERNMENT OPERATIONS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittees met, pursuant to call, at 10:30 a.m., in Room 2154, Rayburn House Office Building, Hon. Ron DeSantis [chairman of the Subcommittee on National Security] presiding.

Present from the Subcommittee on National Security: Representatives DeSantis, Amash, Foxx, Comer, Lynch, and Welch.

Present from the Subcommittee on Government Operations: Representatives Meadows, Hice, Massie, Connolly, and Maloney.

Mr. DESANTIS. The Subcommittees on Government Operations and National Security will come to order.

Without objection, the presiding member is authorized to declare a recess at any time.

Mr. Meadows is not here yet. He does have an opening statement. I think he is on his way. So if he wants to give it, we will obviously do that.

I am second seat here, so I don't have one. So what I will do is I will recognize the ranking member.

Mr. Connolly is not coming, right?

Mr. LYNCH. I know he is around, but I know we have a lot going on this morning.

Mr. DESANTIS. Okay. So I will recognize the ranking member on my subcommittee, Mr. Lynch, and I will let him do his opening statement.

Mr. LYNCH. Thank you very much. Mr. Chairman. I appreciate the courtesy. I want to thank you for holding this hearing, and I also want to thank the witnesses for helping us with our work.

This hearing is to examine the anti-consumer-fraud efforts undertaken by the Federal Trade Commission following the end of Operation Chokepoint. I would also like to thank all of the staff on both sides for preparing this hearing.

The Consumer Protection Branch at the Department of Justice initiated the investigative and enforcement program known as Operation Chokepoint in November of 2012. This operation examined efforts of fraudulent practices perpetrated through the U.S. banking system against bank customers by unscrupulous merchants, fi-

nancial institutions, and intermediaries referred to as third-party payment processors.

As reported by the Department of Justice, fraudulent online merchants would typically unlawfully direct their payment processors to initiate debit transactions against consumer accounts and transmit the money back to them.

In the most egregious cases, the payment processors had full knowledge that merchant clients were committing those fraudulent transactions and illegally siphoned money from customer accounts anyway as some banks simply looked the other way.

In furtherance of Operation Chokepoint, the Department of Justice issued 60 administrative subpoenas from February 2013 through August 2013 to entities that are believed to have evidence pertaining to consumer fraud schemes.

One of the most recent settlements that arose out of this operation occurred in March of 2015 when the Department of Justice announced that it had reached a $4.9 million settlement with CommerceWest Bank of California.

The civil complaint in the case alleged that the bank had ignored a series of red flags and facilitated consumer fraud by permitting Las Vegas payment processors to make millions of dollars in unauthorized withdrawals from consumer bank accounts on behalf of fraudulent merchants.

The warning signs included an extremely high rate of rejected debit transactions that were returned by customers and their banks as well as inquiries that CommerceWest received from other financial institutions about suspicious illegal activity involving its payment processor.

I understand that some Members of Congress expressed concern that the Department of Justice, in cooperation with the financial regulators such as the Federal Deposit Insurance Corporation, was unlawfully targeting certain categories of legitimately operating businesses. In response, the House Financial Services Committee, the House Judiciary Committee, and this committee all conducted extensive investigations of Operation Chokepoint, beginning back in the 113th Congress.

In December of last year, the House also passed H.R. 2706, the Financial Institution Consumer Protection Act, by a bipartisan vote of 395 to 2. I voted in favor of this legislation, which seeks to address concerns stemming from the facts surrounding Operation Chokepoint by prohibiting the FDIC and other financial regulators from terminating their relationship with specific customers without a valid and written justification.

As underscored in a letter to Congress sent to the Department of Justice in August of 2017, quote, "All of the Department's bank investigations conducted as part of Operation Chokepoint are now over. The initiative is no longer in effect, and it will not be undertaken again," close quote.

It is my understanding that the purpose of today's hearing is to examine whether Operation Chokepoint has nevertheless continued at the Federal Trade Commission despite its official termination.

I greatly appreciate the willingness of our witnesses to testify on this topic today. However, as ranking member of the Subcommittee on National Security, it is my sincere hope that during the remain-

der of the 115th Congress we will work together on a bipartisan basis to conduct meaningful oversight on those issues that are most pressing to the safety and security of the American people, our dedicated military and civilian personnel deployed overseas and our returning veterans.

It simply does not serve the interest of national security when the principal oversight committee in the House has held more hearings on shark finning, believe it or not, shark finning, and red snapper fishing in the Gulf of Mexico than it has on the ongoing civil war in Syria—can you believe that?—which is now entering its eighth year.

We currently have more than 2,000 American troops deployed in a destabilized country that just witnessed a massive offensive undertaken by the forces of Syrian President Bashar al-Assad to recapture the southwestern city of Daraa. The operation caused catastrophic damage to the city and displaced more than 300,000 Syrians to the Syrian-Jordanian border in the Golan Heights frontier. And just yesterday, Islamic State militants launched a series of coordinated suicide bombings across Sweida in southern Syria, killing more than 200 people.

So this committee has not held a single hearing on our national security policy toward North Korea either. This issue demands robust oversight following the statement of principles on nuclear nonproliferation signed by President Trump and North Korean President Kim Jong-un at their Singapore summit in June and the initiation of diplomatic talks led by Secretary Pompeo.

We have held zero hearings on the state of our counterterrorism operations in Africa, believe it or not. Our American Green Berets, U.S. Navy SEALs, and other commandos are currently on the ground in Africa under so-called section 127e special ops authority. These units are undertaking perilous counterterrorism raids with African partner forces in Nigeria, Somalia, Libya, Tunisia, Kenya, and other nations, and their safety necessitates rigorous oversight by this Subcommittee on National Security.

And, of course, our ongoing military and counterterrorism operation in Iraq and Afghanistan, where we still have an estimated 6,000 and 15,000 American troops deployed, respectively, should command our regular attention. While Iraqi Prime Minister Haider al-Abadi declared final victory over the Islamic State last December, the terrorist group is reemerging across Kirkuk, Diyala, and Saladin provinces through a wave of insurgent attacks and kidnapping.

The security environment in Afghanistan also continues to deteriorate. This week alone, a suicide bomber carried out an attack near Kabul Airport, killing 14 and wounding more than 50 individuals. Earlier this morning, a Taliban suicide bomber attacked a security convoy of the Afghan National Intelligence Agency.

So, Mr. Chairman, I respectfully request that we begin to work on those issues and conduct oversight of those issues and other critical national security issues going forward.

And, with that, I will yield the balance of my time. Thank you.

Mr. DESANTIS. The gentleman yields back.

I am pleased to introduce the witnesses. We have Mr. Andrew Smith, the Director of the Bureau of Consumer Protection at the

FTC; Jason Oxman, chief executive officer of the Electronic Transactions Association; and Ms. Lauren Saunders, associate director of the National Consumer Law Center.

Welcome to you all.

Pursuant to committee rules, all witnesses will be sworn in before they testify, so if you guys can please stand and raise your right hand.

Do you solemnly swear or affirm the testimony you about to give is the truth, the whole truth, and nothing but the truth, so help you God?

All right. Please be seated.

All witnesses answered in the affirmative.

In order to allow time for discussion, please limit your testimony to 5 minutes. Your entire written statement will be made part of the record. As a reminder, the clock in front of you shows the remaining time during your opening statement. The light will turn yellow when you have 30 seconds left and red when your time is up. Please also remember to press the button to turn your microphone on before speaking.

And, with that, Mr. Smith, you are recognized.

WITNESS STATEMENTS

STATEMENT OF ANDREW SMITH

Mr. SMITH. Thank you, Mr. Chairman and Ranking Member Lynch. My name is Andrew Smith, and I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission.

My written statement submitted for the record represents the views of the Commission, but this opening statement represents my views alone and not necessarily the views of the Commission or of any individual commissioner.

The FTC is the Nation's primary consumer protection agency. We are a bipartisan and independent agency governed by five commissioners, and we are dedicated to pursuing law enforcement actions to stop unlawful practices, including fraud against consumers.

In the last 10 years alone, the FTC has brought more than 600 cases in Federal court against companies and individuals who engage in unfair and deceptive conduct, including countless cases challenging fraudulent telemarketers and online scammers. The FTC has returned hundreds of millions of dollars to American consumers while obtaining strong injunctive relief to protect consumers going forward.

When we bring a case against a fraudster, we routinely look for others who knowingly facilitated the fraud, whether it be a telemarketing boiler room, a robocalling platform, a lead generator, or a payment processor who actively participated in the fraudulent scheme.

In only 15 of these hundreds of fraud cases that we have brought since 2008—in only 15 of these cases have we seen fit to bring an enforcement action against a culpable payment processor. And these 15 instances weren't the product of the FTC staff acting on its own whim. The bipartisan Commission, both Republicans and Democrats, approved each of these matters by a unanimous and a public vote.

As these numbers demonstrate, the FTC doesn't take action against payment processors lightly, and the 15 cases that we have brought were not even remotely close calls. In each case, we had specific evidence that these payment processors were knowingly facilitating the misconduct of their merchants by actively evading the antifraud protections of the national payment system.

For example, we have sued payment processors who have opened multiple, sometimes hundreds, of dummy merchant accounts to hide fraudulent transactions, dilute consumer complaints and charge-backs, and subvert the critical systems established by banks and the card networks to monitor for illegal activity.

We also have seen payment processors that deliberately lie to banks and the payment networks about the line of business of their merchants, as well as payment processors engaging with merchants in a high volume of sham payment transactions to paper over the real but fraudulent transactions that resulted in consumer charge-backs.

And I should note that the frauds perpetrated by the merchants in these 15 cases were of the most egregious sort, causing hundreds of millions of dollars of injury to consumers. These constituted sham business opportunities, credit card interest rate reduction scams, fraudulent online discount clubs in which consumers never enrolled, and "grandparent scams" harming older Americans.

The FTC doesn't intend to impose on payment processors the responsibility to police their customers, but we do expect payment processors to follow the well-established rules of their industry, and they must abide by the law. So when we see evidence that a payment processor is knowingly facilitating a fraudulent scheme, we will not hesitate to act to protect consumers.

As the law enforcement numbers show, this isn't a game of "gotcha" for us at the FTC. We sue payment processors sparingly and only where we have powerful evidence of their complicity in the underlying fraud.

Thank you for the opportunity to testify. I welcome your questions.

[Prepared statement of Mr. Smith follows:]

Prepared Statement of
The Federal Trade Commission

on

The Federal Trade Commission's Enforcement of Operation Chokepoint-Related Businesses

Before the

Committee on Oversight and Government Reform
Subcommittee on National Security and Subcommittee on Government Operations

United States House of Representatives

Washington, D.C.
July 26, 2018

Chairman DeSantis, Ranking Member Lynch, Chairman Meadows, Ranking Member Connolly, and members of the Subcommittees, I am Andrew Smith, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to tell you about the Commission's law enforcement program to fight consumer fraud and the Commission's actions against payment processors that facilitate this fraud.

I. Consumer Protection Mission

As the nation's primary consumer protection agency, the FTC has a broad mandate to protect consumers from unfair, deceptive, or fraudulent practices in the marketplace. It does this by, among other things, pursuing law enforcement actions to stop unlawful practices, and educating consumers and businesses about their rights and responsibilities. The FTC targets its efforts to achieve maximum benefits for consumers, which includes working closely with federal, state, international, and private sector partners on joint initiatives. Among other issues, the FTC addresses fraud, combats illegal robocalls, protects privacy and data security, and helps ensure that advertising claims to consumers are truthful and not misleading.

Fighting fraud is a major focus of the FTC's law enforcement. The Commission's anti-fraud program stops some of the most egregious scams that prey on U.S. consumers—often, the most vulnerable Americans who can least afford to lose money. For example, the FTC brings actions against fraudsters who pose as imposter government agents (including the IRS and even the FTC), family members, or well-known companies in order to trick consumers into sending

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

them money. Fraudsters also target small businesses, sometimes cold-calling businesses to "collect" on invoices they do not owe.

During the past year, the FTC joined federal, state, and international law enforcement partners in announcing "Operation Tech Trap," a nationwide and international crackdown on tech support scams that trick consumers into believing their computers are infected with viruses and malware, and then charge them hundreds of dollars for unnecessary repairs.[2] Just last month, the FTC announced "Operation Main Street," an initiative to stop small business scams. The FTC, jointly with the offices of eight state Attorneys General, announced 24 actions targeting fraud aimed at small businesses, as well as new education materials to help small businesses identify and avoid potential scams.[3]

Illegal robocalls also remain a significant consumer protection problem and consumers' top complaint to the FTC. In FY 2017, the FTC received more than 4.5 million robocall complaints.[4] The FTC is using every tool at its disposal to fight these illegal calls.[5] Because part

---

[2] FTC Press Release, *FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams* (May 12, 2017), https://www.ftc.gov/news-events/press-releases/2017/05/ftc-federal-state-international-partners-announce-major-crackdown.

[3] FTC Press Release, *FTC, BBB, and Law Enforcement Partners Announce Results of Operation Main Street: Stopping Small Business Scams Law Enforcement and Education Initiative* (June 18, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-bbb-law-enforcement-partners-announce-results-operation-main.

[4] Total unwanted-call complaints for FY 2017, including both robocall complaints and complaints about live calls from consumers whose phone numbers are registered on the Do Not Call Registry, exceeded 7 million. *See Do Not Call Registry Data Book 2017: Complaint Figures for FY 2017*, https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2017.

[5] *See* FTC Robocall Initiatives, https://www.consumer.ftc.gov/features/feature-0025-robocalls. Since establishing the Do Not Call Registry in 2003, the Commission has fought vigorously to protect consumers' privacy from unwanted calls. Indeed, since the Commission began enforcing the Do Not Call provisions of the Telemarketing Sales Rule ("TSR") in 2004, the Commission has brought 138 enforcement actions seeking civil penalties, restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains against 454 corporations and 367 individuals. As a result of the 125 cases resolved thus far, the Commission has collected over $121 million in equitable monetary relief and civil penalties. *See* Enforcement of the Do Not Call Registry, https://www.ftc.gov/news-events/media-resources/do-not-call-registry/enforcement. Recently, the FTC and its law enforcement partners achieved an historic win in a long-running fight against unwanted calls when a federal district court in Illinois issued an order imposing a $280 million penalty against Dish Network—the largest penalty ever

of the increase in robocalls is attributable to relatively recent technological developments, the FTC has taken steps to spur the marketplace to develop technological solutions. For instance, the FTC led four public challenges to incentivize innovators to help tackle the unlawful robocalls that plague consumers.[6] The FTC's challenges contributed to a shift in the development and availability of technological solutions in this area, particularly call-blocking and call-filtering products.[7] In addition, the FTC regularly works with its state, federal, and international partners to combat illegal robocalls, including co-hosting a Joint Policy Forum on Illegal Robocalls with the Federal Communications Commission, as well as a public expo featuring new technologies, devices, and applications to minimize or eliminate the number of illegal robocalls consumers receive.[8]

II. The FTC's Legal Actions against Payment Processors

Since 1996, the FTC has brought 25 actions against a variety of entities that help fraudulent merchants obtain payment processing for sales that violate the FTC Act. Each of these cases was approved by a unanimous vote of the bipartisan Commission. These lawsuits against

---

issued in a Do Not Call case. *U.S. v. Dish Network, L.L.C.*, No. 309-cv-03073-JES-CHE (C.D. Ill. Aug. 10, 2017), https://www.ftc.gov/enforcement/cases-proceedings/052-3167/dish-network-llc-united-states-america-federal-trade.

[6] The first challenge, announced in 2012, called upon the public to develop a consumer-facing solution to block illegal robocalls. One of the winners, "NomoRobo," was on the market within six months after the FTC selected it as a winner. NomoRobo, which reports blocking over 600 million calls, is being offered directly to consumers by a number of telecommunications providers and is available as an app on iPhones. *See* FTC Press Release, *FTC Announces Robocall Challenge Winners* (Apr. 2, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners; *see also* FTC Press Release, *FTC Awards $25,000 Top Cash Prize for Contest-Winning Mobile App That Blocks Illegal Robocalls* (Aug. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/ftc-awards-25000-top-cash-prize-contest-winning-mobile-app-blocks; FTC Press Release, *FTC Announces Winners of "Zapping Rachel" Robocall Contest* (Aug. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-announces-winners-zapping-rachel-robocall-contest.

[7] Consumers can access information about potential solutions available to them at https://www.consumer.ftc.gov/features/how-stop-unwanted-calls.

[8] FTC Press Release, *FTC and FCC to Host Joint Policy Forum on Illegal Robocalls* (Mar. 22, 2018), www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls; FTC Press Release, *FTC and FCC Seek Exhibitors for an Expo Featuring Technologies to Block Illegal Robocalls* (Mar. 7, 2018), www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-seek-exhibitors-expo-featuring-technologies-block-illegal.

payment processors generally arise out of fraudulent conduct the FTC has challenged in a prior or pending FTC action. On some occasions, we have observed the same processor providing services for multiple different entities that were defendants in FTC, [9] SEC, or state cases.

Processors control access to the financial system and unscrupulous processors can allow the underlying frauds to inflict harm on thousands of consumers. Where appropriate, challenging processors is a critical component of the FTC's efforts to fight fraud and illegal robocalls while halting hundreds of millions of dollars of consumer injury. Payment processors engaged in illegal conduct harm not only consumers; they harm legitimate industry players and undermine confidence in the financial system. This testimony will briefly summarize how the payments system works, explain the bases of the FTC's legal authority, and describe a few representative enforcement actions the Commission has filed against payment processors.

To accept credit card payments from consumers, a merchant must establish an account with an acquiring bank ("the acquirer") because acquiring banks have direct access to the credit

[9] *See, e.g.*, *FTC v. Landmark Clearing, LLC*, No. 11-cv-00826 (E.D. Tex. Dec. 29, 2011) (Stip. Perm. Inj.), https://www.ftc.gov/enforcement/cases-proceedings/1123117/landmark-clearing-inc-larry-wubbena-eric-loehr (allegedly processed payments for defendants in at least two FTC law enforcement actions); *FTC v. Edebitpay, LLC*, No. 07-cv-4880 (C.D. Cal. Jan. 17, 2008) (Stip. Perm. Inj.) (online marketers charged with deceptive sales of reloadable debit cards and unauthorized debiting of consumers' accounts); *FTC v. Direct Benefits Group*, No. 11-cv-01186 (M.D. Fla. Aug. 12, 2013) (Final Judgment) (found liable for debiting consumers' bank accounts without consent and failing to adequately disclose that financial information from payday loan applications would also be used to charge consumers for enrollment in unrelated products and services)); *FTC v. Automated Electronic Checking*, No. 13-cv-0056 (D. Nev. Mar. 11, 2013) (Stip. Perm. Inj.), https://www.ftc.gov/enforcement/cases-proceedings/122-3102/automated-electronic-checking-et-al (allegedly processed payments for Edebitpay defendants just weeks after Edebitpay entered into a stipulated permanent injunction with the FTC and processed for Elite Debit, one of the named defendants in *FTC v. I Works, Inc.*, No. 10-cv-2203 (D. Nev. Aug. 26, 2016) (Stip. Perm. Inj.) (a massive internet fraud that caused more than $280 million in harm by luring consumers into trial memberships for bogus government-grant and money-making schemes)); *see also FTC v. Your Money Access*, No. 07-cv-5147 (E.D. Pa. Dec. 6, 2007), https://www.ftc.gov/enforcement/cases-proceedings/052-3122/your-money-access-llc-et-al-ftc-state-illinois-state-iowa; *FTC v. First American Payment Processing, Inc.*, No. 04-cv-0074 (D. Ariz. Jan. 3, 2004), https://www.ftc.gov/enforcement/cases-proceedings/032-3261/first-american-payment-processing-inc-et-al; *FTC v. Electronic Financial Group, Inc.*, No. 03-cv-211 (W.D. Tex. July 7, 2003), https://www.ftc.gov/enforcement/cases-proceedings/032-3061/electronic-financial-group-inc-et-al.

card networks, such as MasterCard and VISA.[10] Acquirers commonly enter into contracts with third parties called Independent Sales Organizations ("ISOs") who solicit and sign up merchant accounts on behalf of the acquirers. ISOs, in turn, will often use other smaller ISOs ("sub-ISOs") or independent sales agents to solicit and refer prospective clients. We use the term "payment processor" to refer collectively to ISOs, sub-ISOs, and independent sales agents.

The card networks require the banks, which in turn require their payment processors, to comply with detailed rules to ensure that their system is not being used to process fraudulent transactions. These rules include requirements for payment processors to underwrite merchants before opening accounts in order to determine whether they are legitimate businesses, and to monitor existing merchants to make sure that their processing activity is not indicative of fraud. For example, merchants with high rates of transactions returned by consumers ("chargebacks") or merchants with unusual spikes in their processing volume, may be subject to further review.

The FTC has brought actions against a variety of payment processors that have assisted fraudulent merchants to help them perpetuate the fraud, avoid the scrutiny of acquiring banks and credit card networks, and cause significant harm to consumers. The FTC's law enforcement cases against payment processors advance two bases of legal liability. First, the FTC's "unfairness authority" prevents payment processors from engaging in practices: (1) that cause or are likely to cause substantial injury to consumers, (2) that could not be reasonably avoided by consumers, and (3) for which the injury is not outweighed by countervailing benefits to consumers or competition.[11] Second, the FTC brings actions against payment processors under the Telemarketing Sales Rule ("TSR") when the underlying fraudulent merchant has engaged in

[10] The FTC does not have jurisdiction over banks. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2).

[11] *See* Section 15(n) of the FTC Act, 15 U.S.C. § 45(n); *see also* FTC Policy Statement on Unfairness, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

telemarketing.[12] In these cases, the FTC uses the TSR's prohibitions on "assisting and facilitating" and "credit card laundering." Payment processors violate the TSR's "assisting and facilitating" provision when they provide substantial assistance to an entity while knowing or consciously avoiding knowledge that the entity is engaged in specified violations of the Rule.[13] Payment processors are liable for "credit card laundering" when they cause a transaction to be submitted to the credit card networks when the transaction is not the result of a transaction between the cardholder and the actual merchant.[14] One such example is where the payment processor or the merchant submits the transaction in the name of a shell corporation in order to mask the identity of the true merchant.

III. Illustrative FTC Enforcement Cases

The Commission's law enforcement actions against payment processors represent a small fraction of the cases filed,[15] but they are an integral part of the agency's robust anti-fraud program. The FTC pursues payment processors that know or consciously avoid knowing that they are facilitating fraudulent telemarketing operations; engage in tactics to evade anti-fraud monitoring measures aimed at preventing and detecting fraudulent merchants; and launder credit card transactions through the merchant accounts of shell companies.

For example, in *FTC v. E.M. Systems & Services*, the Commission and the Office of the Attorney General for the State of Florida charged a nationwide debt relief telemarketing scam

[12] 16 C.F.R. § 310 *et. seq.*

[13] 16 C.F.R. § 310.3(b).

[14] 16 C.F.R. § 310.3(c)(1)-(2).

[15] Since 2008, the Bureau of Consumer Protection has filed 639 law enforcement cases in federal district court seeking consumer redress or civil penalties for violations of the FTC Act and rules enforced by the Commission. Of those cases, 15 (or 2.35%) involved allegations that a payment processor engaged in unlawful conduct.

with violations of the TSR.[16] In the course of discovery, staff uncovered evidence of a credit card laundering scheme orchestrated by E.M. Systems' payment processor, CardReady, and CardReady's executives.[17] Staff discovered that, after E.M. Systems was unable to open merchant accounts in its own name, CardReady created shell companies, recruited "straw men" to be the officers of the shell companies, and fabricated merchant accounts in the names of these shell companies that E.M. Systems could use to process its transactions. The evidence indicated that CardReady then assisted in spreading the scam's revenues and chargebacks across at least 26 different merchant accounts, circumventing industry fraud controls and hiding the true identities of the scam's perpetrators, which allowed the scam to continue for at least two years. To settle the case, the CardReady defendants agreed to permanent injunctions, including a $12,365,371 judgment, representing the net sales volume (total sales volume less refunds and chargebacks) processed through the merchant accounts. The judgment was suspended based upon defendants' financial condition, provided they made payment of $1,800,000 for consumer redress.[18]

In *FTC v. WV Universal Management d/b/a Treasure Your Success*, the Commission charged the Treasure Your Success ("TYS") defendants with deceptively marketing credit card interest rate reduction services to consumers using illegal robocalls, outbound calls, and unlawful

---

[16] *FTC v. E.M. Systems & Servs., LLC*, No. 15-CV-1417 (M.D. Fla. June 16, 2015) (granting *ex parte* temporary restraining order, asset freeze, and appointment of receiver against defendants charged with falsely promising cash-strapped consumers that they would save consumers money and illegally charging up-front fees ranging up to $1,400). Relevant court filings are available at https://www.ftc.gov/enforcement/cases-proceedings/152-3155/em-systems-services-llc.

[17] *FTC v. E.M. Systems & Servs., LLC*, No. 15-CV-1417 (M.D. Fla. Dec. 21, 2015) (amended complaint charging payment processor defendants with violations of the TSR's prohibition against assisting and facilitating unlawful telemarketing and credit card laundering).

[18] For a complete description of settlements reached with various defendants, see FTC Press Release, *Debt Relief Defendants Agree to Telemarketing and Financial Services Ban and Payment Processors Agree to Payment Processing Ban to Settle FTC Action* (Nov. 30, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/debt-relief-defendants-agree-telemarketing-financial-services-ban.

up-front fees.[19] Here too, following discovery, the Commission amended the complaint to charge payment processors Newtek (a division of Universal Processing of Wisconsin, LLC ("UPS")), its then-president, Derek DePuydt, and sales agent, Hal Smith, with violating the TSR. The payment processors opened and approved TYS for a merchant account without performing customary reviews (such as obtaining telemarketing scripts, as required by their own procedures) and despite clear indicia of fraud (including inconsistent information on the merchant application, poor credit scores, unusually high chargeback rates, and fraud notices from MasterCard).[20] The court entered summary judgment against UPS and Smith, finding them jointly and severally liable for substantially assisting the TYS defendants while knowing or consciously avoiding knowing that TYS was violating the TSR.[21] The court awarded the Commission $1,734,972, representing the full amount processed through the TYS merchant accounts (less refunds and chargebacks).[22] On appeal, UPS did not dispute liability, and instead challenged only the court's finding of joint and several liability for $1.7 million.[23] On appeal after remand,[24] the Eleventh Circuit affirmed the monetary award, held that joint and several liability is appropriate, and

---

[19] *FTC v. WV Universal Management, LLC*, No. 12-cv-1618 (M.D. Fla. Oct. 29. 2012) (court entered an *ex parte* TRO, asset freeze, and appointment of a receiver, and later converted the TRO into a preliminary injunction).

[20] *FTC v. WV Universal Management, LLC*, No. 12-cv-1618 (M.D. Fla. June 18, 2013) (Amended Complaint). The TYS defendants, DePuydt, and other named defendants entered into settlements with the Commission. For a complete description of settlements reached with various defendants, see FTC Press Release, *Court Finds Defendants in FTC's Treasure Your Success "Rachel Robocalls" Case Liable for $1.7 Million* (May 20, 2015), https://www.ftc.gov/news-events/press-releases/2015/05/court-finds-defendants-ftcs-treasure-your-success-rachel.

[21] *FTC v. WV Universal Management, LLC, et al.*, No. 12-cv-1618, 2014 WL 6863506 (M.D. Fla. Nov. 18, 2014) (entry of summary judgment on liability against payment processor defendants for violations of the TSR).

[22] *FTC v. WV Universal Management, LLC, et al.*, No. 12-cv-1618, 2015 WL 916349 (M.D. Fla. Feb. 11, 2015) (finding of joint and several liability for $1.7 million).

[23] *FTC v. HES Merchant Services Company, Inc.*, 652 Fed. Appx. 837 (11th Cir. June 14, 2016) (vacating in part, affirming in part, and remanding for clarification the district court's finding of joint and several liability for $1.7 million).

[24] *FTC v. HES Merchant Servs. Co., Inc. et. al*, No. 12-cv-1618, 2016 WL 10880223 (M.D. Fla. Oct. 26, 2016) (decision on remand, clarifying court's determination of joint and several liability).

expressed confidence that the "requirement of a culpable mind . . . [means] that joint and several liability will not result in collateral damage to innocent third parties."[25]

Although much of the FTC's work has focused on payment processors servicing credit cards as the payment instrument, the FTC also brings action against other payment entities that help dishonest merchants obtain payments from consumers. In 2017, the FTC entered into a settlement with Western Union, alleging that massive fraud payments flowed through its money transfer system for many years, including payments in which complicit Western Union agents processed the fraud payments in return for a cut of the proceeds.[26] Even in the face of evidence that many of its agents were involved in the frauds, Western Union allegedly failed to properly address the problem, looked the other way, and even rewarded some complicit agents for their high volume of business. As alleged, many of these frauds harmed older adults. For example, from 2004 to 2015 Western Union received more than 41,000 complaints totaling nearly $75 million in losses for "emergency scams and grandparent scams."[27] Concomitant with the FTC's action, Western Union entered into a Deferred Prosecution Agreement with the Department of Justice ("DOJ") in which the company admitted to criminally aiding and abetting wire fraud and violations of the Bank Secrecy Act,[28] and agreed to settle related civil charges brought by the

[25] *FTC v. WV Universal Management, LLC,* 877 F.3d 1234, 1242 (11th Cir. Dec. 13, 2017), cert. denied by *Universal Processing Services of Wisconsin, LLC v. FTC*, --- S.Ct. ----, 2018 WL 1367543 (2018).

[26] *FTC v. The Western Union Co.*, 17-cv-00110 (M.D. Pa. Jan 19, 2017), https://www.ftc.gov/enforcement/cases-proceedings/122-3208/western-union-company.

[27] Grandparent scams involve a scammer calling other adults and pretending to be a grandchild who has a desperate need for immediate financial help, such as to pay medical bills or bail.

[28] *United States v. The Western Union Co.*, No. 17-cr-0011 (M.D. Pa. Jan. 19, 2017), https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million.

Financial Crimes Enforcement Network.[29] The separate FTC and DOJ settlements resulted in $586 million in redress for consumer victims.[30]

The overwhelming majority of payment processors abide by the law and provide substantial benefits to the marketplace. But, as the cases above highlight, when unscrupulous payment processors violate the law, they also cause significant economic harm to consumers and legitimate businesses. In such circumstances, Commission action, including law enforcement action, ensures consumers are protected and the nation's payment system continues to operate effectively and efficiently. When a payment processor helps a fraudulent merchant take money from consumers–either by actively helping the merchant hide its fraudulent conduct from the acquiring banks and payment networks or by turning a blind eye to the merchant's fraud–the Commission will pursue appropriate law enforcement, to protect consumers and competition.

---

[29] *In the Matter of Western Union Financial Servs., Inc.*, No. 2017-01 (Jan. 19, 2017) (assessment of civil money penalty), https://www.fincen.gov/sites/default/files/enforcement_action/2017-01-19/WUFSI%20Assessment%20of%20Civil%20Money%20Penalty-%201-19%20-%202017.pdf.

[30] The Commission's cases frequently provide a foundation for actions brought by its law enforcement partners. *See, e.g., United States v. First Bank of Delaware*, Civ. No. 12-6500 (E.D. Pa. Nov. 19, 2012) (settlement of case alleging defendant bank originated more than 2.6 million remotely created check transactions totaling approximately $123 million on behalf of payment processors, including payment processing defendants in *FTC v. Landmark Clearing*, No. 11-cv-00826 (E.D. Tex. Dec. 15, 2011) (Stip. Perm. Inj.) and *FTC v. Automated Electronic Checking*, No. 13-cv-00056 (D. Nev. Feb. 5, 2013) (Stip. Perm. Inj.) that were actively facilitating fraudulent internet and telemarketing merchants sued by the FTC).

Andrew Smith

Director, Bureau of Consumer Protection

BIOGRAPHY

Andrew Smith is Director of the FTC's Bureau of Consumer Protection. He came to the FTC from the law firm of Covington & Burling, where he co-chaired the financial services practice group. Earlier in his career, Mr. Smith was a staff attorney at the FTC, where he led the agency's efforts to make several rules under the Fair Credit Reporting Act. Mr. Smith has written extensively on consumer protection and financial services issues, served as the Chair of the American Bar Association's Consumer Financial Services Committee, and is a Fellow of the American College of Consumer Financial Services Lawyers and the American Bar Foundation. He earned a bachelor's degree in history from Williams College, and a J.D. from William & Mary Law School, where he served as Professional Articles Editor of the William & Mary Law Review.

Mr. DESANTIS. I thank the gentleman.

Mr. Oxman, you are up for 5 minutes.

STATEMENT OF JASON OXMAN

Mr. OXMAN. Thank you, Mr. Chairman.

I am here representing ETA, the Electronic Transactions Association. We are the trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services to merchants.

ETA supports the enforcement of existing laws and regulations by Federal agencies, including the Federal Trade Commission, to stop fraud. But what we are deeply troubled about is the FTC's use of Operation Chokepoint-style tactics to hold payment processors responsible for fraud committed by bad merchants.

The Department of Justice ended Operation Chokepoint in 2017 following congressional scrutiny and criticism. That scrutiny demonstrated that holding payment processors liable for merchant fraud has serious adverse consequences, including processors abandoning lawful categories of merchants disfavored by the government as well as higher prices for consumers.

Now, again, the payments industry is dedicated to fighting fraud and ensuring that consumers have access to safe, convenient, and affordable payment services. Consumers choose electronic payments, indeed, because they have zero liability for fraud.

ETA has worked hard as an industry representative to develop guidelines on merchant and ISO underwriting and risk monitoring. These guidelines provide more than 100 pages of best practices to detect and halt fraudulent actors. ETA has shared these draft guidelines with the Federal Trade Commission, which has encouraged us to strengthen anti-fraud efforts.

The FTC's targeting of the payments industry actually predates Operation Chokepoint and, indeed, exceeded the Department of Justice's efforts in scope but somehow has managed to fly under the radar until today.

Many of our member companies receive what are called civil investigative demands, CIDs, from the FTC asking for dozens of categories of information about dozens of different merchants. Many of our payment processor members receive multiple CIDs a year, often part of a broader fishing expedition around a particular industry.

Now, even though processors do their part to fight fraud through robust underwriting and monitoring, payment processors simply are not law enforcement. The fact is that sometimes processors miss red flags or make unintentional mistakes. But it is a big leap to suggest that a processor was intentionally aiding and abetting a merchant in fraud and should be left to cover the total cost of consumer injury caused by the merchant. And that is exactly what the Federal Trade Commission does.

Specifically, the FTC seeks to hold payment processors and even individual owners and employees financially responsible for the total volume of sales transactions processed for a bad merchant, even where the processor made just a penny on the dollar for such transactions.

Emboldened by a recent but misguided decision in the 11th Circuit entitled "Universal Processing," the FTC's aggressive use of joint and several liability threatens to put targeted processors out of business or even to bankrupt individuals based on the conduct of a single bad merchant out of a processor's entire portfolio.

It is important to understand that the FTC uses the same aggressive tactics in all cases, even where a processor cooperates with the FTC to assist law enforcement activities. The FTC's insistence on joint and several liability for payment processors makes it financially impossible for a processor to try to defend itself in court. A small processor that earns a few thousand dollars processing for a merchant can't take the risk of litigating a case where the FTC seeks to hold the processor liable for millions of dollars.

When the FTC sends a CID to a processor regarding a merchant, it tells the processor to maintain confidentiality and to continue processing for the merchant. But then the FTC inevitably turns on the processor and seeks to hold it financially liable for all of the volume processed and all of the merchant's sales, including those after the CID was issued.

Similarly, where a court appoints a receiver to manage a merchant's assets, the FTC pressures the receiver to take possession of a processor's reserves for the merchant, even though those reserve accounts belong to the processor, not the merchant. The processor is then forced to cover consumer charge-backs out of its own funds.

The FTC refuses to discuss settlement of a case against a processor until the processor or its individual owner provides financial information.

The FTC also engages in aggressive prosecution of individual officers and employees for assisting and facilitating the conduct of a merchant employee, even where they had no control over that conduct.

And the FTC regularly uses its CID process to request information from third parties, when that information is regularly available to the FTC itself.

The results of this enforcement approach is that payment processors will have no choice but to increase prices for services to merchants and, even worse, restrict access to payment systems to certain categories of merchants to avoid exposure for liability.

There is, however, a better path forward. Congress should encourage the FTC to review and reconsider its overly aggressive use of CIDs and questionable discovery and enforcement tactics. Former FTC Chairman Ohlhausen in 2017 announced just such an effort. That effort should continue.

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 actually an active part of a common enterprise with merchants.

Congress should direct the FTC to halt enforcement actions against processors until they engage in a public discussion of Operation Chokepoint.

And Congress should support the FTC to encourage additional industry self-regulation.

Thank you for the opportunity to appear here before you today, and I look forward to your questions.

[Prepared statement of Mr. Oxman follows:]

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's") 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

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

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 taking jobs overseas and often leaving 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.

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

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 its 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 then 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

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

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).

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

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 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 CIDs from the FTC asking for dozens of categories of information about dozens of different merchants. 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 make 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

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

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 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

[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

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

because the FTC aggressively seizes any reserves that a processors 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 has and continues to press against the payments industry. It is important for Congress to

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

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

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

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 up 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,

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

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 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

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

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 targeted 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, and other clients. In March 2017, a federal judge in North Dakota dismissed the CFPB's lawsuit

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

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 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 make 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

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

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 processing 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.

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

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 cardholders 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:

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

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 work shop 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.

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

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 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 now ask that Congress take a closer look at the FTC's enforcement practices and the aggressive tactics outlined in this testimony. The FTC's actions, just like Operation Choke Point, are harming the payments industry, merchants, and consumers. We believe that 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 before the Subcommittee.

Mr. MEADOWS. [Presiding.] Thank you, Mr. Oxman.
Ms. Saunders, you are recognized for 5 minutes.

STATEMENT OF LAUREN SAUNDERS

Ms. SAUNDERS. Thank you.

Chairman DeSantis, Ranking Member Lynch, Chairman Meadows, Ranking Member Connolly, and members of the subcommittees, thank you for inviting me to testify today. I am Lauren Saunders, associate director of the National Consumer Law Center, which works for economic justice for low-income and other vulnerable consumers across the United States.

Fraud takes billions of dollars from people every year, often from seniors and other vulnerable communities. Fraud also imposes costs on businesses and many other people in the country.

Fraudsters often do not act alone. Many fraudsters rely on payment processors to take money out of consumers' accounts. Responsible payment processors can stop fraud or make it more difficult. Unfortunately, a very few outliers sometimes willingly enable fraud.

The FTC's cases against payment processors are part of its traditional bipartisan law enforcement work, unanimously supported by both Republican and Democratic chairs and commissioners. These cases go back over two decades and are independent at the Department of Justice's former Operation Chokepoint.

For example, in 1996, under Chairman Steiger, who was appointed by the first President Bush, the FTC sued Windward Marketing, which used remotely created checks to help a magazine subscription scam bilk consumers of over $12 million.

In 2007, under Chairman Majoras, appointed by the second President Bush, the FTC sued Your Money Access, which processed more than $200 million on behalf of numerous fraudulent telemarketers and internet-based merchants, accepting merchants with facially false sales scripts and ignoring extremely high return rates.

More recently, last year the FTC sued the payment processor iStream Financial Services for processing discount club transactions despite numerous fraud indicators, including recommendations from the iStream's sister bank, independent compliance auditors, and iStream's own compliance and risk officers that the processing relationship be terminated due to the high return rates and likelihood of fraud.

The FTC's work has been approved by courts, as in the recent case against WV Universal Management, the credit card processor for a fraudulent credit card interest rate reduction scheme. The processor's president had personally approved merchant accounts despite several glaring red flags, including charge-backs so high that they came to the attention of Mastercard, which noted the potential fraud risk.

The 11th Circuit Court of Appeals affirmed a position of joint and several liability on the defendants but only after observing that it was undisputed that Universal had violated the telemarketing sales rule by providing substantial assistance to the scammers despite knowing or consciously avoiding knowing about the fraud.

The testimony from the Electronic Transaction Association today criticizes the FTC's use of joint and several liability but does not attempt to defend the conduct of the processor in the Universal case.

And, indeed, as Mr. Smith pointed out, I haven't heard anybody criticizing the cases they have brought. These are not close cases. There is extensive evidence of complicity of the payment processors in the very few cases that they bring.

The FTC targets bad apples and provides incentives for the industry to police itself, spurring efforts like those of the Electronic Transaction Association to help its members prevent fraud and make enforcement unnecessary in most cases.

Vague and unsubstantiated claims have been made that the FTC may be targeting entire classes of legal businesses, but the evidence is that the FTC targets fraudulent activity, plain and simple.

While I disagree with the characterizations of DOJ's Operation Chokepoint, there is a key difference between that operation and the FTC, and that is the FTC starts with the scammer and then, like any good investigator, follows the money.

Most of FTC's 600 fraud cases do not have a companion case against a payment processor. But if the FTC finds evidence that a payment processor was a willing participant and enabler, it brings an enforcement action, which is especially important because consumers cannot do this kind of investigation on their own, and they rely on government to prevent this type of fraud.

The FTC's fraud work is especially important today, with growing problems of identity theft, data breaches, and online scams. Everyone, from individual consumers to legitimate businesses benefits, when fraudsters and their collaborators are held accountable.

Thank you for inviting me to testify today. I would be happy to answer your questions.

[Prepared statement of Ms. Saunders follows:]

Testimony of Lauren K. Saunders

Associate Director, National Consumer Law Center

On

"The Federal Trade Commission's Enforcement of Operation Chokepoint-Related Businesses"

Before the

Subcommittee on Government Operations and

Subcommittee on National Security

Of the

Committee on Oversight and Government Reform

U.S. House of Representatives

July 25, 2018

Chairmen Meadows and Desantis, Ranking Members Connolly and Lynch, and Members of the subcommittees:

Thank you for inviting me to testify today. I am the Associate Director of the National Consumer Law Center. NCLC works for economic justice for low-income and other disadvantaged people in the U.S. through policy analysis and advocacy, publications, litigation, and training. One of our publications is Consumer Banking and Payments Law, for which I am the lead author.

I am here today to testify in support of the Federal Trade Commission's work to stop payment fraud, including its enforcement actions against payment processors that knowingly or recklessly facilitate fraud.

Fraud takes billions of dollars from Americans each year. Grandparent scams, IRS imposters, fake credit cards, lottery scams, unwanted membership clubs, work-at-home schemes, and many other variations prey on people across the country. Often, the victims are elderly, immigrants with limited English proficiency, or other vulnerable populations.

Fraudsters often need help scamming people. Many fraudsters rely on third party payment processors to take money from consumers' accounts. Responsible payment processors can stop fraud or make it more difficult, but a very few outliers sometimes willingly enable fraud.

It is only the rare payment processor that that knowingly participates in fraudulent schemes or willfully ignores blatant signs of illegal activity, and these are the payment processors that the FTC pursues. No one is defending the egregious conduct of any of the payment processors that the FTC has sued.

The FTC's cases against payment processors are part of its traditional law enforcement work. That work has been bipartisan and unanimously supported by both Republican and Democratic commissioners. The FTC's work in this area goes back over two decades and is independent of the Department of Justice's Operation Choke Point, which started much later and has now ended.

The FTC targets fraudulent activity, not any category of legal business. It is most often through the investigation of a fraudulent scheme that the FTC finds evidence that a payment processor was a willing participant and enabler.

Everyone, from individual consumers to legitimate businesses, benefits when fraudsters and their collaborators are held accountable. Anyone who cares about protecting Americans

from fraud should support the FTC's work to against payment processors that consciously enable scams.

Fraudsters Use Banks and Payment Processors to Take Money from Consumers

Many scams, frauds and illegal activity could not occur without access to consumers' bank or credit card accounts. Fraudsters who obtain consumers' account numbers can take payments from consumers in several ways. Sometimes they con people into leaving their homes to send money by wire transfer or through gift cards or prepaid card reload packs. But sometimes, using information obtained on the phone or online, they submit a preauthorized electronic debit through the ACH system; create a remotely created check drawn on the consumer's account and deposit it[1]; or process a fraudulent charge against the consumer's credit or debit card through the relevant card network (Visa, MasterCard, American Express or Discover).[2]

Many scams and other forms of unlawful activity rely on the ability to access the payment system to get the consumer's money. The FBI estimates that mass-marketing fraud schemes cause tens of billions of dollars of losses each year for millions of individuals and businesses.[3] Estimates of the costs of fraud targeted at seniors alone start at $3 billion and go much higher than that.[4]

---

[1] Amendments to the Telemarketing Sales Rule now ban use of RCCs in telemarketing transactions.
[2] For example, the FTC recently brought a case against a third party payment processor that contributed to a massive $26 million internet scam by helping its fraudster clients evade the credit card networks' fraud monitoring programs. FTC, Press Release, "FTC Charges Payment Processors Involved in I Works Scheme" (Aug. 1, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-charges-payment-processors-involved-i-works-scheme.
[3] Federal Bureau of Investigation, International Mass-Marketing Fraud Working Group, "Mass-Marketing Fraud: A Threat Assessment" (June 2010), available at http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment/mass-marketing-threat.
[4] *See* Tobie Stanger, Consumer Reports, "Financial Edler Abuse Costs $3 Billion a Year. Or Is It $36 Billion?" (Sept. 29, 2015), https://www.consumerreports.org/cro/consumer-protection/financial-elder-abuse-costs--3-billion-----or-is-it--30-billion-;The MetLife Study of Elder Financial Abuse (June 2011), available at https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf.

How Payment Processors Can Prevent or Enable Payment Fraud

The term "payment processor" can refer both to the entity that packages payments for processing by a financial institution and also the independent sales organizations and independent sales agents that help merchants arrange processing by financial institutions.

The payment processor's obligations arise through several sources. Payment system rules, such as NACHA rules,[5] may impose direct obligations on payment processors. Processors may have obligations that arise through their relationships with financial institutions, which are bound by Bank Secrecy Act, know-your-customer, anti-money laundering and fraud prevention rules. Payment processors are also covered by general laws, such as laws against unfair or deceptive conduct and the FTC's Telemarketing Sales Rule, which prohibits persons from consciously providing substantial assistance to support a violation of the rule.

Some payment processors perform due diligence functions for financial institutions or vouch for their merchants. Payment processors that handle transactions must also monitor the accounts for signs of fraud or unlawful activity.

One of the clearest signs of a problem is a high return rate – the percentage of payments that are rejected or challenged, i.e., because the payment was unauthorized, was subject to a stop payment order, bounced because of insufficient funds, or was rejected because the account does not exist or was closed.

Not every rejected payment is a sign of fraud. But if return rates are high, processors have a duty to determine why, and to investigate if the account is being used for improper purposes. If large numbers of consumers are challenging a customer's payments as unauthorized, clearly the payment processor's customer—the merchant whose transactions the

[5] Effective January 1, 2015, NACHA rules impose direct obligations on payment processors to the extent that the payment processor is performing the financial institution's obligations. 2018 NACHA Operating Rules § 2.15.3.

payment processor is handling--is doing something wrong. If an unusually high number are rejected because the account has been closed, that may reveal that consumers are closing their accounts in response to fraud or that the fraudster is buying lists of account numbers that contain older accounts long since closed. Even high rates of payments rejected for insufficient funds, especially when combined with returns for other reasons, may reveal that consumers are not expecting the payments and have been defrauded. Depending on the type and level of the return rate, a high return rate can be a per se rule violation or it may trigger a duty to investigate.

In the ACH system, the average rate of transactions returned as unauthorized is 0.03%.[6] NACHA rules prohibit unauthorized return rates higher than 0.5% (over sixteen times higher than the average rate).[7] The average total rate at which ACH debits are returned for any reason is about 1.42%. Under NACHA rules, and a total return rate above 15% (over ten times higher than the average rate) requires scrutiny, though not the same absolute obligation to reduce the rate.[8] Average return rates in other payment systems are in the same ballpark, and, similarly, abnormally high return rates are strong evidence of fraud.[9]

Payment processors can hide high return rates and help scammers avoid scrutiny by spreading questionable transactions among different merchant accounts. "Nested" payment processors – a processor that processes payments for other payment processors – can launder signs of unlawful activity, and nesting is itself a warning signal. For this reason, regulators have

---

[6] NACHA, ACH Network Risk and Enforcement Topics, Topic 1- Reducing the Unauthorized Return Rate Threshold (effective date September 18, 2015), https://www.nacha.org/rules/ach-network-risk-and-enforcement-topics.

[7] *Id.*

[8] NACHA, ACH Network Risk and Enforcement Topics, Topic 2- Establishing Inquiry Process For Administrative and Overall Return Rate Levels (effective date September 18, 2015), https://www.nacha.org/rules/ach-network-risk-and-enforcement-topics.

[9] *See, e.g.,* FTC, Press Release, "FTC Sues Payment Processor for Assisting Credit Card Debt Relief Scam" (June 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/06/ftc-sues-payment-processor-assisting-credit-card-debt-relief-scam?utm_source=govdelivery (noting that the average credit card chargeback rate is well below one percent).

advised financial institutions to be especially careful of processor customers whose clients include other payment processors.[10]

Other signs of fraud are obvious. The consumer, the consumer's bank, state attorneys general, or other government officials may complain to or tip off the payment processor.

Payment processors are not expected to verify the legality of every payment they process, and they are not always aware that they are being used to facilitate illegal activity. But those that take their duties seriously can be an important bulwark depriving criminals of access to the payment system.

The FTC Typically Pursues Scammers First, Then Follows the Money to Payment Processor Conspirators

The prosecution of fraudsters is an important part of the FTC's work. The FTC has brought numerous cases against scammers over the years. In recent years, these cases have included:

- *FTC v. Hornbeam:* Defendants deceived consumers into thinking they were applying for payday loans but instead registered them in online discount clubs without the consumers' consent. The defendants debited more than $40 million from consumers' bank accounts by using electronic remotely created checks (RCCs).[11]

[10] *Id.*

[11] FTC, Press Release, FTC Says Operators of Bogus Discount Clubs Took Tens of Millions of Dollars From Consumers' Bank Accounts without Their Consent (Aug. 16, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/ftc-says-operators-bogus-discount-clubs-took-tens-millions.

- *FTC v. Money Now Funding, LLC.* Money Now Funding cheated consumers out of $7 million through false promises of business or work-at-home opportunities.[12]

- *FTC v. The Tax Club, Inc. et al.* The Tax Club's telemarketing operation took more than $200 million from consumers trying to start home-based businesses. The defendants falsely claiming affiliation with companies that the consumers did business with, made false claims that their products and services were essential, and failed to provide the promised services.[13]

- *FTC v. Innovative Wealth Builders, Inc., et al.* The defendants operated a credit card interest rate reduction scam using telemarketers to pitch phony debt relief services. The defendants later consented to over $9.9 million in equitable monetary relief.[14]

Each of these scams relied on a payment processor to take the money from consumers.

Most of the FTC's fraud cases do not result in a companion case against a payment processor. But in its investigations of fraudulent conduct, the FTC at times uncovers evidence that the payment processor knew or consciously disregarded evidence that it was processing fraudulent transactions.

The FTC has brought cases against payment processors under both Republican and Democratic Chairpersons, with the unanimous consent of the FTC's commissioners of both

---

[12] FTC, Press Release, FTC Stops Elusive Business Opportunity Scheme (Aug. 20, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/ftc-stops-elusive-business-opportunity-scheme.
[13] FTC, Press Release, FTC and New York and Florida Attorneys General Charge The Tax Club's Telemarketing Scheme with Bilking Consumers Who Were Trying to Launch Home-Based Businesses (January 17, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/ftc-new-york-florida-attorneys-general-charge-tax-clubs.
[14] FTC, Press Release, FTC Shuts Down Fraudulent Debt Relief Operation (Sept. 11, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/ftc-shuts-down-fraudulent-debt-relief-operation.

parties. These cases have been brought for more than 20 years, and have no relationship to the U.S. Department of Justice's Operation Choke Point, which began in 2013 and ended in 2017.

In 1996, under Chairman Steiger, who was appointed by the first President Bush, the FTC sued *Windward Marketing*, which used victims' banking information obtained over the phone and illegitimately created remotely created checks that debit accounts for over $12 million in magazine subscriptions that consumers did not realize they were purchasing. [15]

In 2002, under Chairman Muris, who was appointed by President George W. Bush, the FTC obtained a stipulated order against *Hyperion, LLC*, which helped telemarketers launder credit card receipts through offshore companies and books for telemarketing scams including lottery tickets, British bonds, and consumer benefits packages.[16]

In 2007, under Chairman Majoras, also appointed by the second President Bush, the FTC sued *Your Money Access*, which processed more than $200 million on behalf of numerous fraudulent telemarketers and Internet-based merchants, accepting merchants with facially false sales scripts and ignoring extremely high return rates.

As in these older cases, in more recent years, the FTC has brought enforcement cases against payment processors only when there is convincing evidence of the processor's culpability. Examples include:

- The payment processor *Global Marketing Group* aided Canada-based advance-fee credit card schemes to debit bank accounts on behalf of clients whose sales scripts plainly indicated that they intended to violate the FTC's Telemarketing Sales Rule and industry rules that prohibit processing electronic banking transactions for

[15] FTC v. Windward Marketing, Ltd., 1:96-CV-615-FMH (N.D. Ga. 1996).
[16] FTC, Pres Release, Consumers Duped by Telemarketers Claiming To Provide Identity Theft Protection Defendants Allegedly Pitched Worthless Credit Card "Protection"; Laundered Credit Card Purchases for Products Sold by Others (Oct. 1, 2002), https://www.ftc.gov/news-events/press-releases/2002/10/consumers-duped-telemarketers-claiming-provide-identity-theft.

outbound telemarketers. The FTC alleged that the payment processor drafted, edited, reviewed, and approved sales scripts and processed transactions without first obtaining adequate information about the clients and their business practices.[17]

- The defendants in the *Your Money Access* case processed more than $200 million in debits and attempted debits, with more than $69 million of the debits returned or rejected by consumers or their banks for various reasons, indicating the lack of consumer authorization. Joined by the Attorney Generals of Illinois, Iowa, Nevada, North Carolina, North Dakota, Ohio, and Vermont, the FTC charged that the defendants, an interrelated group of payment processors, accepted clients whose applications contained signs of deceptive activity, including sales scripts with statements that were facially false or highly likely to be false.[18]
- *Capital Payments* (now known as Bluefin) enabled The Tax Club telemarketing scheme to process consumers' credit card payments. Capital Payments ignored red flags of fraud including high rates of chargebacks, claims of fraudulent or unauthorized charges, and alerts from financial institutions.[19]
- *Electronic Payment System of America* and related defendants provided Money Now Funding access to credit card networks by submitting and approving

[17] FTC, Press Release, FTC Stops Payment Processor Who Aided Cross-Border Telemarketing Fraud (Dec. 20, 2006), https://www.ftc.gov/news-events/press-releases/2006/12/ftc-stops-payment-processor-who-aided-cross-border-telemarketing.
[18] FTC, Press Release, FTC And Seven States Sue Payment Processor that Allegedly Took Millions from Consumers Bank Accounts on Behalf of Fraudulent Telemarketers and Internet-based Merchants (Dec. 11, 2007), https://www.ftc.gov/news-events/press-releases/2007/12/ftc-and-seven-states-sue-payment-processor-allegedly-took.
[19] FTC, Press Release, Payment Processor Involved in The Tax Club Telemarketing Scheme Settles FTC Charges (Feb. 11, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/payment-processor-involved-tax-club-telemarketing-scheme-settles.

fraudulent applications in the names of more than 40 fictitious companies, evading the anti-fraud monitoring efforts of the credit card networks.[20]

- *iStream Financial Services* repeatedly disregarded the high return rates generated by the Hornbeam discount club and disregarded other fraud indicators, including recommendations from iStream's sister bank, independent compliance auditors, and iStream's own Compliance and Risk Officers to terminate the processing relationship due to the high return rates and the likelihood of fraud.[21]

One case that has gained attention recently is *FTC v. WV Universal Management, LLC*, 877 F.3d 1234 (11th Cir. 2017). The FTC sued a credit card payment processor, Universal, its sales agent and others for assisting a telemarketing company in a fraudulent credit card interest reduction scheme. The FTC's evidence was so compelling that a court granted summary judgment to the FTC, finding that the payment processor knew or consciously avoiding knowing of the fraudulent activities. The payment processor did not appeal the merits. The uncontroverted facts are that the payment processor's president had personally reviewed and approved the merchant accounts despite several glaring red flags, including serious credit delinquencies. Chargebacks later became so high that MasterCard took notice of the potential fraud risk but, undeterred, the president approved a second merchant account for the telemarketer. The Eleventh Circuit Court of Appeals, noting that "it has been established as a matter of law that Universal violated the [Telemarketing Sales Rule]," affirmed joint and several

[20] FTC, Press Release, FTC Files Charges Against Independent Sales Organization and Sales Agents (Aug. 7, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/ftc-files-charges-against-independent-sales-organization-sales.

[21] FTC v. Hornbeam Special Situations, LLC, No. Case 1:17-cv-03094-TCB (N.D. Ga. Aug. 15, 2017). https://www.ftc.gov/system/files/documents/cases/savings_makes_money_complaint_file_stamped_8-16-17.pdf.

liability against the defendants, including the payment processor, following well established standards in similar tort and securities cases.[22]

These payment processor cases, though few and far between, can be a more efficient use of government resources than scammer-by-scammer prosecutions. Scammers shut down by the FTC often pop up again somewhere else. A payment processor that is aiding one scammer often has developed a business of processing payments for multiple fraudsters, so a single enforcement action can help identify and shut stop multiple scam.

Beyond the impact of the individual cases, the FTC's enforcement cases serve as an important reminder to all payment processors about the importance of taking their due diligence duties seriously.

Indeed, the most important impact of the FTC's enforcement actions may be to spur industry efforts to police itself and avoid the need for government enforcement. Trade associations like the Electronic Transaction Association play an important role in these self-policing efforts by helping their members comply with the law and to be vigilant against fraud.

The vast majority of payment processors have no desire to help scammers. These institutions are important partners with law enforcement when they deny criminals access to the payment system. It is much better to deny fraudsters access to consumers' accounts in the first place than to prosecute them after the fact.

Payment Fraud Hurts Everyone

Wrongdoers who access the payment system inflict harm on everyone. In addition to the direct victims of fraud:

- Retailers and online merchants lose business if consumers are afraid to shop online;

[22] FTC v. WV Universal Management, LLC, 877 F.3d 1234 (Dec. 13, 2017).

- New and improved payment systems will not gain consumers' confidence if consumers fear fraud;
- Payments fraud causes the general public to spend millions of dollars on identity protection products and lose faith in the security of the payment system;
- Consumers' banks bear the customer friction and the expense of dealing with an unauthorized charge – at an average cost of $100 and up to $509.90 for a smaller bank, according to NACHA;
- The fraudsters' banks and payment processors may suffer regulatory or enforcement actions, lost customers, private lawsuits, and adverse publicity; and
- American security is put at risk when banks and processors that lack know-your-customer controls are used for money laundering.

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. Work against payment fraud is especially important today with growing problems of identity theft, data breaches, and online scams.

I urge you to support the FTC's work against payment processors that willfully enable fraudulent activity. Everyone must do their part to protect the integrity of the payment system and to prevent fraudulent activity that harms millions of Americans and American businesses.

Thank you for inviting me to testify today. I would be happy to answer any questions.

Mr. MEADOWS. Thank you all for your testimony.

And the chair recognizes the gentleman from the 11th District of Virginia, my good friend, Mr. Connolly, for his opening statement.

Mr. CONNOLLY. I thank the chair, and I thank our witnesses for coming here today. I am a little late today because we had a vote, and we are going to have some more votes very shortly.

Two days ago, during a full committee hearing on election security in this very room, I made a motion for the Oversight and Government Reform Committee to subpoena the Office of the Director of National Intelligence to inform the committee and the public about the extent of the Russian threat to our country. That subpoena unfortunately was tabled by a vote of 17 to 15.

This morning, two Oversight and Government Reform subcommittees are teaming up to discuss the urgent problem of Operation Chokepoint, a program that no longer exists and a program that the full committee conducted extensive oversight of 4 years and two chairmen ago.

What is, one wonders, the urgent need for this hearing now, when the administration is under legal compulsion to reunite children that have been separated from their parents as part of a zero tolerance policy at the border; when the deaths of perhaps as many as 4,600 U.S. citizens in Puerto Rico have been attributed to Hurricane Maria and the Federal Government's inadequate response to it; when the Secretary of Commerce apparently misled this committee on why a divisive question on citizenship was hastily added to the 2020 census; when a member of this committee, full committee, forthrightly wrote an op-ed in The New York Times saying that the President of the United States has been manipulated by Vladimir Putin?

These are all worthy of committee examination and open hearings. So what could possibly be the reason for this hearing today?

Congress conducted lengthy oversight of Operation Chokepoint in 2013 and 2014. Congressional Republicans then alleged that DOJ and the FDIC intentionally conspired—intentionally—to mislead Congress about their partnership and inappropriately targeted a list of high-risk merchants and industries to conduct Operation Chokepoint.

The Committees on Financial Services and Judiciary also held oversight hearings. The Oversight and Government Reform Committee conducted an investigation under then-Chairman Darrell Issa that produced not one but two staff reports.

Republicans got what they wanted. The two principal agencies involved in Chokepoint, the DOJ and the FDIC, have both ended their work on the operation. The FDIC ended its involvement in Operation Chokepoint in January of 2015.

The DOJ issued a letter to the chairman of the House Judiciary Committee in August that stated, and I quote, "All of the Department's bank investigations conducted as part of Operation Chokepoint are now over. The initiative is no longer in effect, and it will not be undertaken again," unquote. Pretty definitive.

Yet here we are questioning the Federal Trade Commission, an agency that played no role in Operation Chokepoint. And here we are because the FTC has a broad mandate to protect consumers from unfair, deceptive, or fraudulent practices in the marketplace.

Some have concluded that this must mean a continuation of Operation Chokepoint. That, it seems to me, is not the case. As part of its work to protect consumers, the FTC works to stop payment fraud, including taking action against payment processors that knowingly or recklessly facilitate fraud. That is their job. The FTC's cases against payment processors goes back two decades and is not related to Operation Chokepoint, which started much later and, as we have heard, no longer exists.

Enforcement action against payment processors who knowingly participate in fraudulent schemes or willfully ignore signs of illegal activity has historically received bipartisan support. These schemes often prey on vulnerable populations, such as seniors, immigrants with limit English language, or families of Active Duty military.

According to a survey by True Link, a company that provides account monitoring software for elders and families, projected that financial elder abuse costs families more than $36 billion a year, of which $17 billion is linked to exploitation and scams such as work-from-home schemes, misleading financial advice, or reverse mortgages.

I can't speak for my colleagues, but I have to say: We ought to be having hearings, it seems to me, about some of the pressing issues of the day. And we could start with the list of subpoena requests the Democrats have submitted to the full committee and the full chairman. I think there are now 62 of them outstanding. That would be some work worthy of our enterprise.

I thank my friend from North Carolina for letting me have this time for my opening statement and will try my best to participate before we call votes.

Mr. MEADOWS. I thank the gentleman from Virginia. And, as he well knows, on some of those items I am willing to advocate in a bipartisan fashion to deal with some of those.

I would like to ask unanimous consent that my opening statement be made part of the record without doing it. Any objection?

Mr. CONNOLLY. No objection.

Mr. MEADOWS. All right. So ordered.

Mr. MEADOWS. Also, I would like to recognize Charlie Kirk, who is here.

Thank you for being here. You have done some work on this particular issue, and we appreciate your work.

And so, with that, I will recognize the gentleman from Florida, Chairman DeSantis.

Mr. DESANTIS. Thank you, Mr. Chairman.

Thanks to the witnesses. I appreciate the work that you guys do.

Mr. Smith, fraud is just a cottage industry, particularly in my State of Florida. You know, you have seniors. And I think we are by far, I think, the number-one State for complaints. So I think it is very, very important. And the issues you site where people are knowingly involved in fraud, I think that is a no-brainer.

How would you respond to Mr. Oxman? Because there seems to be a discrepancy here about how innocent processors are treated by the FTC. Because I would say, if the people who are committing fraud, that's where you would want to do the government action. If people are simply processing this stuff without being a part of it, then putting some of these investigative demands on them

raises the cost of doing business, and that hurts consumers, too, because people don't have access, the ability to do that.

So how would you respond to some of the things Mr. Oxman pointed out?

Mr. SMITH. Right. So in the 15 cases that we have brought, I don't think there is any disagreement about complicity by the payment processor. So there are issues raised by Mr. Oxman about what I understand to be compulsory process issued by the FTC to payment processors as a part of a broader investigation.

So we do this kind of third-party discovery, like any litigant does and like any law enforcement agency does. We do it routinely. We send third-party CIDs, civil investigative demands, to telephone companies, to banks, to payment processors, to internet registrars in order to gather information for our investigations of——

Mr. DESANTIS. Is there a threshold that is required before you initiate that?

Mr. SMITH. So any CID that we issue, whether it is to a target or to a third party, has to be approved by a commissioner and it has to articulate specific allegations of a law violation in order for us to issue the CID. So we can't do fishing expeditions to, you know, we want to investigate the business opportunity industry and so this CID, we are sending it to 100 companies as a part of that. We don't do that, because we are not permitted to do that under our rules of practice and our statute.

So we do send third-party process, though. All law enforcement agencies do. And we are sensitive to the fact that it is expensive to respond, and we appreciate that. And, as Mr. Oxman noted, in 2017 the FTC undertook an effort to streamline its CID processes to make them more manageable for businesses.

But the fact remains that we really need to get this information from third parties. We frequently can't get it anyplace else, either because the investigation is confidential and we don't want to tip the target or because we get better information from third parties than we get from the target. We have frequently found instances where—remember, we are talking about fraudsters here—where they have given us bad responses to our CIDs and we have gotten better information from third parties.

But we understand and respect that that presents an expense for legitimate businesses, and we appreciate that and try to factor that in to our targeting.

Mr. DESANTIS. The idea of holding the person processing the transaction responsible for the entire amount of the transaction, unless there is evidence that they knowingly were participating in the fraud, that would not be something that you would support?

Mr. SMITH. Right. So, in the 11th Circuit case that was mentioned by Ms. Saunders, the court held that—and there are a couple of other court decisions that have similar holdings—that, in order to impose joint and several liability on a payment processor, the FTC has to show that they knew of the fraudulent scheme or they consciously avoided knowing it and they actively facilitated the fraudulent scheme.

So, in that 11th Circuit case, what happened was that the company president was complicit in sort of fast-tracking these fraudulent transactions through, circumventing the underwriting process

and the monitoring process. And the company essentially admitted liability. The question was, was there enough knowledge, was there enough intent, in order to satisfy that joint and several standard? And the court held that there was.

Mr. DESANTIS. So, Mr. Oxman, how would you respond? Because I think that, you know, Mr. Smith is saying, hey, there are rare instances where there is active participation. And, look, I mean, that is a totally different issue, if they are actively engaged in fraud. You are raising concerns about kind of just the normal course of business and having, you know, government action really hurt the industry. So how would you respond to what Mr. Smith has said?

Mr. OXMAN. That is exactly right. And I think the reason that both Mr. Smith and Ms. Saunders focus on those 15 cases is we have no dispute with those cases, and we are not here to discuss that.

What we are here to discuss and what we are raising concerns about is what is happening at the FTC in all the cases we don't know about.

So our member companies are telling us that there are an unrelenting number of CIDs coming out of the FTC in cases where the Commission appears to be looking—I call it a fishing expedition—at particular merchant categories. They are sending these CIDs out, sometimes dozens at a time, looking blanketly across multiple industries and using the information gathered to build cases.

And, as Mr. Smith noted, those CIDs don't need the approval of the entire Commission. They need one commissioner. And what we are looking for is a process where, as in those 15 cases, the entire Commission is making sure that these actions are justified and that the burden is not placed on processors to take these actions in support of law enforcement where they are legitimately going against bad merchants. That is the concern that we have.

Mr. DESANTIS. Great.

I am out of time, so I will yield back.

Mr. MEADOWS. The chair recognizes the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman.

At this time, I would defer to my colleague, the brilliant gentlelady from New York.

Mrs. MALONEY. Thank you so much, Ranking Member and Chairman, for holding this important hearing on consumers and protection for them.

I want to commend and thank Ms. Saunders and the organization she represents, the National Consumer Law Center, for the initiatives that you have taken to protect disadvantaged people, poor people, and, particularly, elderly people from financial scams.

So, first, I would like to ask you, in your own words, at the NCLC, what types of financial scams targeting the poor, the elderly, or other vulnerable people have you seen and come across?

Ms. SAUNDERS. You know, the variation is really incredible.

We see a lot of "grandparent scams." In fact, my own father was subject to one of these that the FTC actually did a little profile blog on. Somebody called up—and my father, who is very competent, 88 years old, but he got a call, you know, "Hi, this is Ben, and I've

been arrested, and I need some money to get out on bail." And even my own father, who, you know, thought it didn't sound like his voice, you know, called me up and said, "Where is Ben?" And, you know, I mean, he was very scared, and the scammer wanted him to go and send the money.

Mrs. MALONEY. Wow.

Ms. SAUNDERS. We see romance scams. We see lottery scams. We see fake interest credit card reduction scams. And often these scams do target seniors and people with limited English proficiency and other—IRS scams. I get these calls all the time, you know, "I'm the IRS, I'm going to arrest you." Now, I don't owe the IRS, so I'm not too scared when I get those calls, but there are, you know, people who have trouble with their back taxes, don't realize it is not the IRS on the other end.

There are all sorts of scams. And a lot of these scams require a method to take the money from consumers, to take the money out of their pockets. And most payment processors, you know, do their best to stop being willing participants, but those who do are appropriately subject to enforcement. And the FTC needs to investigate to figure out who is culpable and who is not.

Mrs. MALONEY. Okay. You have given some examples of people. Could you give some examples of how the FTC is important in protecting consumers against predatory third-party payor processors, which Mr. Oxman seems to feel are being unfairly targeted?

Ms. SAUNDERS. Right. Well, you know, I mentioned the iStream Financial Services case. This is a case where people were signed up for discount clubs that they really didn't want and money was taken out of their bank account. And——

Mrs. MALONEY. They signed them up without their knowledge and then took the money out of their account?

Ms. SAUNDERS. Exactly.

Mrs. MALONEY. How in the world can you do that? Isn't the bank there to—how could they get into their accounts?

Ms. SAUNDERS. Because people often provide their information because they think they are signing up for something else. They may think they are signing up for a payday loan. They may think that they are getting a one-time, you know, purchase of something. But once they have their bank account information, they can use that. Maybe sometimes in the fine print, in deceptive terms, you know, they sign them up for something else.

Mrs. MALONEY. Is this usual, that payment processors participate in scams like this?

Ms. SAUNDERS. Payment processors are often essential to move the money, in order to take a credit card, a debit card, to do an electronic payment. Now, again, they aren't all complicit, but they are often a key part of how the scam works and how the money gets from the consumer to the scammer.

Mrs. MALONEY. Now, what would happen if consumers were helpless, if there was no FTC there to help them in payment scams or other scams?

I talked to some of the prosecutors in New York, and they say a lot of their work in the district attorney's office is just trying to protect people from scams all the time.

Ms. SAUNDERS. Right. Absolutely.

Mrs. MALONEY. So, if you didn't have the FTC, would there be any protection for consumers in this area?

Ms. SAUNDERS. You know, consumers do have some protection against unauthorized charges, and they can go to their bank if they can show that the charge is unauthorized.

And it actually imposes costs on banks, as well, especially small banks. They are the ones who end up having to deal with these things, and it costs them money to have to deal with the consumer and reverse the charge. And sometimes they can't get them reversed.

Mrs. MALONEY. Now, I want to get to some of the other witnesses.

Mr. Smith, how many enforcement actions has the FTC pursued since 1996? And how many of these enforcement actions have involved a third-party processing payment system?

Mr. SMITH. Right. So we looked back 10 years to 2008, and we counted up 639 enforcement actions. We decided just to focus on the last 10 years because it would have taken us a long time to count up until 1996. But in that 10 years, we have 639 enforcement actions generally and 15 against payment processors.

And one quick thing I wanted to add is that we are focusing a lot on the complicit payment processors, but the payment processing industry—trillions of dollars of transactions happen without event, right? So consumers should feel safe that the payment processing industry is looking after their best interests. It is just in these very few cases where we found a need to drill down and hold the payment processor responsible.

Mrs. MALONEY. Uh-huh.

May I just, Mr. Chairman, ask a question related to what he just said?

Mr. MEADOWS. Very succinctly.

Mrs. MALONEY. Okay.

So what is the estimated amount of financial harm consumers have suffered in these 639 cases and 15 with—so we get a sense of what is the economic impact on people and the economy.

Mr. SMITH. Right.

Mr. MEADOWS. So you can answer briefly. The gentlewoman's time has expired.

Mr. SMITH. Okay. In the 15 cases, we had $700 million of harm and we recovered $620 million for consumers.

Mrs. MALONEY. Wow.

Mr. MEADOWS. Okay.

Mrs. MALONEY. Uh-huh.

Mr. MEADOWS. The chair recognizes the gentleman from Georgia.

Mr. HICE. Thank you, Mr. Chairman.

Mr. Smith, what was the role of the FTC in developing Operation Chokepoint?

Mr. SMITH. So I wasn't at the Commission at the time, but I have spent a lot of time reviewing the OGR prior investigations, and I have also spent a lot of time talking to staff. And the FTC was a part of the Financial Fraud Enforcement Task Force established by President Obama, along with something like 30 other agencies—Securities and Exchange Commission, the IRS, et cetera.

We also were a leader of the Consumer Protection Working Group of that FFETF. And as the Nation's primary consumer protection agency, that would only make sense. And there were maybe another dozen agencies on the Consumer Protection Working Group. So we communicated with DOJ and all of our law enforcement partners regularly about fraud cases.

In terms of specific Operation Chokepoint activity, the FTC, as I understand it, wasn't involved in that. It wasn't involved in targeting, to the extent that there was any, of particular industries. But I don't want to say that there wasn't information being exchanged by the FTC with its law enforcement partners, because we do that all the time pursuant to our rules and approval by our general counsel.

Mr. HICE. Right. According to the memos about Chokepoint, as I understand it, the FTC provided the DOJ with potential leads for Operation Chokepoint investigations.

Mr. SMITH. Don't—well, we provided the DOJ with names of banks.

Mr. HICE. Right.

Mr. SMITH. Don't know if that was for Chokepoint or for something else.

One thing that is important to remember is that the FTC doesn't have any jurisdiction over banks. That is specifically carved out from our statute. DOJ does. So, to the extent that there might be banks that have information or that may be problematic, then that is a DOJ——

Mr. HICE. But as you came up with suspicious information, that information was passed on as a potential lead, according to memos, as I understand it.

So my question from that would be: How would the FTC determine a particular companyor institution, whether or not they should be investigated? What are they looking for?

Mr. SMITH. So a particular company, we were looking for strong evidence of fraud, and we would investigate the merchant, right? So we would investigate the business opportunity scam or the robocalling scam.

And in the course of that investigation, as Ms. Saunders said, we follow the money, as all investigators do. So you go to the payment processor, you go to the acquiring bank, you go also to other third parties, like the telephone company and the internet registrar, to gather up information.

And so, in the course of those investigations, there is a process between the FTC and other law enforcers to share information that we get——

Mr. HICE. So did the FTC actually participate in Operation Chokepoint?

Mr. SMITH. No, not as far as I know. I mean, there was—so if you think of Chokepoint as the—it was defined earlier in the hearing as these 60 subpoenas that were sent out, that is not us.

Mr. HICE. All right.

Now, before your appointment to the FTC, you worked for a law firm that represented companies against Operation Chokepoint. Is that correct?

Mr. SMITH. Yes.

Mr. HICE. Okay. I am curious of some of your experiences with that. Did any of your clients have assets seized as a result of Operation Chokepoint?

Mr. SMITH. So my involvement with Operation Chokepoint—and this is a matter of public record. I was a partner at the law firm of Covington & Burling, and I represented a trade association for online lenders who were impacted negatively by Operation Chokepoint.

So the work was primarily on a policy level, working with the agencies to determine how we can resolve Operation Chokepoint. Because the problem was that legitimate companies were losing their banking relationship——

Mr. HICE. Right. That is what I am aware of.

Mr. SMITH. Right.

Mr. HICE. So, with that—and that was the whole problem with this. So I take it that you did represent some companies that had some assets seized. What——

Mr. SMITH. No, not so much companies, but more this trade association. So I don't know——

Mr. HICE. Okay. Were the seizures justified?

Mr. SMITH. I don't know of any asset seizures for Operation Chokepoint. The problem was the loss of the banking relationship.

Mr. HICE. You don't know of any seizures as a result? Because I certainly do.

Mr. SMITH. Of Operation Chokepoint? No. I mean, I know that the FTC—and, I mean, in the course of our law enforcement, we will seize assets in order to return money to consumers. As far as Operation Chokepoint is concerned—so at the top of the hearing, it was defined as these 60 subpoenas, resulting in 3 actions against banks. And as far as asset seizures, that I don't know. I think the banks were exposed to penalties, perhaps for anti-money-laundering issues, but I don't know.

Mr. HICE. Well, so were companies.

And, unfortunately, my time has expired, Mr. Chairman, so I will yield back.

Mr. MEADOWS. I thank the gentleman from Georgia.

The gentleman from Virginia is recognized.

Mr. CONNOLLY. Thank you.

Ms. Saunders, I understand from your testimony you certainly believe, in this context, consumers need some protection.

Ms. SAUNDERS. Absolutely.

Mr. CONNOLLY. You need to speak closer to that microphone. You can move it to you.

Ms. SAUNDERS. Okay. Yes, absolutely. I think fraud would be far, far worse if we didn't have the FTC and other law enforcement agencies, you know, looking at this fraud and finding everybody who is culpable.

Mr. CONNOLLY. Right.

Now, one of the practices that has concerned me for a long time: Certain payday lenders, for example, not all but some, prey on vulnerable families of Active Duty military, especially those who kind of ship overseas and their families are left behind. They tend to be lower-income folks, and making ends meet can be a real challenge.

Is that a problem, in your experience?

Ms. SAUNDERS. Well, the Military Lending Act today does prohibit high-cost loans to servicemembers. Certainly, payday loans have been a problem with servicemembers and their families and loved ones.

You know, that is not anything related at all to, you know, the FTC's enforcement work against payment processors, but, separately, we have pushed for protections for servicemembers and all families against predatory lending, and payday lenders are a big problem.

Mr. CONNOLLY. Yeah. I guess the point I was just trying to make is that, when we look at, sort of, financial predation, it covers all kinds of classes of people—seniors, ordinary consumers, and even our Active Duty military families who can be taken advantage of in times of need. And they all need someplace to go for protection.

Ms. SAUNDERS. Right. Absolutely. And, certainly, servicemembers and veterans are targets of fraud, you know, like any other American, and they need the vigorous work of government to stop those kinds of scams and to cut off these scammers from the ability to take the money, as long as we, you know, are going after the payment processors who are willing participants.

Mr. CONNOLLY. Right.

Now, you gave the example of your dad.

Ms. SAUNDERS. Uh-huh. Who's a veteran.

Mr. CONNOLLY. I'm sorry?

Ms. SAUNDERS. Who is a veteran.

Mr. CONNOLLY. Who is a veteran. Served this country.

I think all of us know the stories of sort of the unwitting compliance—unwitting in that people are sometimes too trusting or don't have their guards up. And none of us want to sort of become, you know, jaundiced and cynical as a society, but, on the other hand, trying to help folks who maybe are more vulnerable to those kinds of schemes and threats and manipulation.

And I mentioned that the best estimate we had was that elder crime in this kind of category was $36 billion a year. Sound right to you?

Ms. SAUNDERS. I have heard that number, yes.

Mr. CONNOLLY. So do you want to expand just a little bit in terms of why senior citizens are maybe more vulnerable than some others in society and more susceptible to this kind of consumer fraud?

Ms. SAUNDERS. Right. Well, seniors, you know, are often more trusting. You know, those of us here in Washington tend to be very cynical, but they do tend to be more trusting——

Mr. CONNOLLY. Not on this committee, Ms. Saunders.

Ms. SAUNDERS. Okay.

Mr. CONNOLLY. Yeah.

Ms. SAUNDERS. They are often lonely, and somebody who calls them on the phone and is friendly and talks to them, you know, can be very persuasive.

I have an uncle who was subject to a romance scam, and I could not convince him that this woman, who—he was so lonely, and this younger woman befriended him. I could not convince him that, even after he wrote $30,000 worth of checks to her, that she was a scammer. I could not convince him to go to the police. He was

later subject to identity theft as part of the same, you know, problem.

Mr. CONNOLLY. Yeah.

Ms. SAUNDERS. And, you know, I had to go to a number of banks who were innocent, you know, who had fraudulent accounts created there, but I had to enlist their help.

Mr. CONNOLLY. To what extent are some of these fraudsters offshore, overseas? And does that complicate our ability to regulate that?

Ms. SAUNDERS. It does. I mean, they are often in boiler rooms offshore, and sometimes the money is moved offshore. That is why our anti-money-laundering laws and know-your-customer rules are especially important, to stop this kind of fraud and other movements of money overseas.

Mr. CONNOLLY. Yeah. I think that is really important to note, as well. Because I know of one, in particular, headquartered in the Caribbean, and that scheme was to call you up and say, you've won the lottery, the Jamaican lottery or whatever lottery, and all you have to do is send us, you know, your credit card number and $200 for processing and you're going to be rich. And I couldn't believe how many people, unfortunately, were prey to that scheme. So that is a whole different dimension.

Thank you, Mr. Chairman.

Mr. MEADOWS. The gentleman from Kentucky is recognized, Mr. Massie.

Mr. MASSIE. Thank you, Mr. Chairman.

Mr. Smith, in 2011, FDIC Quarterly Journal published a list of 30 merchant categories that were high-risk endeavors. Among these categories included what I consider to be very legitimate commerce: ammunition sales, firearms sales, pharmaceutical sales, surveillance equipment, and tobacco sales.

Does the FTC use this list or does the FTC have their own list of high-risk categories? And is that publicly available?

Mr. SMITH. We don't target our—we don't have a list of high-risk merchants. We don't target our enforcement activity based on high-risk merchants.

I will tell you, in all of the cases that we have brought that we outlined here, the fraud cases where there have been payment processors involved, involved telemarketing boiler rooms essentially, you know, real hardened scams, situations where merchants were debiting consumers' accounts without even any authorization.

Mr. MASSIE. Okay. I just want to make sure you weren't targeting firearms sales, ammunition sales, pharmaceutical sales——

Mr. SMITH. No. None of our cases have been brought against——

Mr. MASSIE. I am not talking about cases that have been brought but the things that are initiated in the way you look for cases.

Mr. SMITH. Right. We don't—okay. So, in terms of case targeting, we look at things like consumer complaints, consumers who have been defrauded. We conduct consumer surveys to determine whether or not there are companies that are engaged essentially in deceptive conduct.

Mr. MASSIE. Okay.

Mr. SMITH. So that's our guide.

Mr. MASSIE. So when you think you've found it, do you have a standard formula to fine or penalize the processing companies, or do you just sort of ad hoc make it up as you go?

Mr. SMITH. Well, we are looking for complicit—evidence that these processors were complicit in the underlying fraud. And, typically, what we—well, in fact, in every case that I reviewed in preparing for this testimony, every case, we have a situation where the payment processor was actively hiding the misconduct from its banking partner and——

Mr. MASSIE. Right, right. But I'm assuming you've found somebody who's guilty of something. Do you have a standard formula for the penalty?

Mr. SMITH. So, with respect to the underlying merchant, we look for unfair——

Mr. MASSIE. Or the processor.

Mr. SMITH. Okay. So our cases, we start with the underlying merchant, and we typically, you know, prove up or allege fraud, get a settlement sometimes with that merchant. So real fraud, deceptive conduct that hurts consumers.

And then we follow the money. And in those couple of cases where we've thought that the payment processor went, sort of, beyond the pale—I mean, we're not pushing the envelope here. We're talking about really bad conduct by payment processors. In those cases, we've brought action.

Mr. MASSIE. But my question is, is there a standard policy that guides when you're going to do that or what the penalty is going to be?

Mr. SMITH. We don't have a written——

Mr. MASSIE. Okay.

Mr. SMITH. —policy for when we bring an action.

Mr. MASSIE. My next question is, I heard you say, I think—and this is encouraging—that you acknowledge that the civil investigative demands are a burden on the merchant. Is that——

Mr. SMITH. On all third-party recipients. So the payment processors aren't unique in this regard or uniquely burdened. But any company, we routinely in the course of our investigations—and this is true for all law enforcement agencies, State, Federal, local—we will have to seek information from third parties unconnected from the fraud. And responding to that compulsory process is going to be expensive, and we understand that and appreciate it and do our best to——

Mr. MASSIE. So it's almost like a tax, this added regulatory compliance. So, given that, I think it's important to know how many of these CIDs have been initiated. Can you tell us—I think Mr. Oxman has alluded to an increased amount or activity of CIDs. Can you give us the number of CIDs?

Mr. SMITH. I don't have the number of third-party CIDs that we've——

Mr. MASSIE. Are they going up or down or——

Mr. SMITH. My guess is that they're going to be flat, because I think that our enforcement activity is generally, you know, a fairly steady pace. So, as an example, if you just look at cases——

Mr. MASSIE. Instead of guessing, could you just give us those numbers, like, how many CIDs? Could you give us that later? I'm not asking for it today.

Mr. SMITH. Yes. I'll ask the staff if we can get those numbers.

Mr. MASSIE. Thank you.

I've got one last question in the last 30 seconds. I'm glad to hear that you recovered money for people who have been defrauded. But can you guarantee us that all the assets that are seized by the FTC go to victims or consumers, that none of it gets diverted to other things?

Mr. SMITH. Well, there are severe legal limitations on our ability to divert money. There's a——

Mr. MASSIE. So it never happens?

Mr. SMITH. So there are cases where are administering a redress program and there is money left over. And, in those cases, sometimes——

Mr. MASSIE. So you've remunerated all of the victims and they've all become whole and you've got money left over?

Mr. SMITH. Sometimes, because not every victim——

Mr. MASSIE. Every victim has always been compensated?

Mr. SMITH. We can't always find every victim. But what I'm talking about here is a small amount of money, typically, in the tens of thousands, and we disgorge that to the Treasury Department.

Mr. MASSIE. So you can——

Mr. SMITH. Because it's very difficult——

Mr. MASSIE. Do you know what they do with it? Just goes back into the general——

Mr. SMITH. It goes into the general fund.

Mr. MASSIE. So it's not diverted to any type of projects or anything?

Mr. SMITH. We're prohibited from that. I think it's called the Miscellaneous Receipts Act. And we're prohibited from using money that we recover for consumers for our own purposes.

Mr. MASSIE. All right.

My time has expired. Thank you, Mr. Chairman.

Mr. MEADOWS. I thank the gentleman for his insightful questions.

The gentleman from Kentucky, Mr. Comer, is recognized.

Mr. COMER. Thank you, Mr. Chairman.

I have two questions for Mr. Smith.

First of all, has the Federal Trade Commission performed any studies or research on whether holding processors responsible for all alleged harm caused by a merchant will result in higher processing costs for merchants and ultimately consumers?

Mr. SMITH. Well, so, first, I disagree with the premise that we're holding all processors liable for all fraud. We're bringing, as we said a couple of times, very few cases here. But in answer to your question, no, we haven't conduct a study.

Mr. COMER. Does the FTC have a standard approach to settlements?

Mr. SMITH. To settlement with payment processors?

Mr. COMER. To settlements.

Mr. SMITH. To settlement.

Mr. COMER. Yes.

Mr. SMITH. So most of the cases that we bring we settle, particularly in the fraud area. In some cases, the bad guys don't show up for court, and so we get a default judgment. And in the course of following the money to try to return money to consumers, if we go to a payment processor, then most of those cases are settled too. Of the however many that I mentioned, I think four have been litigated.

Mr. COMER. What are ways in which the FTC can improve its tactics to be less burdensome to law-abiding and legitimate businesses?

Mr. SMITH. Well, last year, the Commission undertook an effort to streamline its CID process, and we've heard back from industry that that's helpful. Of course, more always needs to be done, and we are, you know, open to additional suggestions about how to streamline the process.

Then the other aspect of that would just be to send fewer third-party CIDs and try to get information from the targets themselves. We sometimes have difficulty doing that because the investigation is confidential or because the targets aren't forthcoming, so we have to go to third parties. But we appreciate that this imposes a burden on businesses, and we are always looking for ways to lessen that burden.

Having said that, we badly need this information for our law enforcement program. We badly need information from third parties, whether it's payment processors, banks, telephone companies, internet registrars, other folks who provide services to the companies that are defrauding consumers.

Mr. COMER. Thank you, Mr. Chairman. I yield back.

Mr. MEADOWS. I thank the gentleman.

The chair recognizes himself for a series of questions.

Ms. Saunders, listen, I think all of us up here want to make sure that consumers are protected. And the horrible stories you hear—actually, I've been one that—you know, it's interesting because occasionally I get these phone calls where I've won unbelievable amounts of money, and they just want me to call back, and so I do. And it's very interesting when we have these dialogues with a Member of Congress. And so I've called the FTC. So we want to protect it. And so I want to say thank you for being an advocate for those consumers.

But there is an equal protection that has a concern, as a business guy, as a small-business guy. And, Mr. Smith, you've talked about only bringing a few small actions. But is it not true that you many times will freeze assets and force companies to settle without ever bringing them to trial?

Mr. SMITH. So I think you're talking here about the issue——

Mr. MEADOWS. Well, you cast a wide net—so you get a complaint. You cast a very wide net. And, literally, you freeze their assets, so they don't have the ability to actually endure long-term. Because you don't bring the case—actually, you don't ever bring the case, but they holler, "Olly, olly, oxen free, please let me go"——

Mr. SMITH. Right.

Mr. MEADOWS. —and so they settle the case.

Mr. SMITH. We don't have the ability to freeze assets without a court order. So here is how an asset freeze would work. And typically we would——

Mr. MEADOWS. Yeah, but the power of the FTC is well-known. And so you get a court order, and you cast a very wide net. Do you not cast a wide net?

Mr. SMITH. So we get a court order against a bad guy——

Mr. MEADOWS. Right.

Mr. SMITH. —a temporary restraining order——

Mr. MEADOWS. And everybody that touches the bad guy.

Mr. SMITH. —and a receiver-appointed—no. The money of the bad guy, right? So we find the bad guy's accounts—or, more appropriately, the receiver finds the bad guy's accounts and freezes them. It is the receiver's job, who is appointed by the court.

And within those accounts, when those accounts are held by other people, then what the law says is that a constructive trust is established over that money because it's money that is being held for the merchant by its service providers. And so the receiver may reach out to those other accounts that are being held on behalf of the merchant by others.

Mr. MEADOWS. So, Mr. Oxman, maybe help clarify my question, so Mr. Smith can understand it a little bit better.

Mr. OXMAN. Yeah. Thanks, Mr. Chairman.

So this enforcement strategy that Mr. Smith calls "follow the money," here's how it works. So they'll go after a legitimate fraudster. And, as you noted, Mr. Chairman, it's very important that they do so. It's an important law enforcement function.

Once they've established a case against the fraudster or bad merchant, they then turn their sights on the payment processor and say: Okay, you processed $40 million in transactions for this merchant. They were bad, so we're going to go after $40 million of your money.

And the processor says: Well, wait a minute, I only made $5,000 off that, you know, less than a penny on the dollar from that transaction.

And the FTC says: Well, no, you processed that money for them, and you have a reserve account—which, by the way, is a reserve account——

Mr. MEADOWS. To pay this.

Mr. OXMAN. —to pay consumers.

Mr. MEADOWS. Right.

Mr. OXMAN. "Charge-backs" they're called.

Mr. MEADOWS. Right.

Mr. OXMAN. And instead of allowing the processor to take those funds and reimburse consumers, the FTC says or directs a receiver to say: No, we're going seize that money, we're going to use it.

That is the "follow the money" strategy. And, as you've noted, Mr. Chairman, that strategy punishes processors who weren't even implicated in the process at all. It's like holding a cash register responsible for taking money and going after the manufacturer of the cash register, or holding AT&T responsible if you and I have a phone call plotting a crime.

Going after the processor might seem easy because that's where the money is. But when you're following the money to a party that

had nothing to do with the fraud, that's where the problem comes. And that's where the issue of payment processors, you know, having to shut off merchants unfairly, having to raise their prices because of this FTC enforcement strategy.

So what we would like to see the FTC do is follow the money to the fraudster, don't bring in innocent parties like payment processors and hold them financially responsible essentially as an insurer for bad merchant behavior.

Mr. SMITH. This is not——

Ms. SAUNDERS. Could I respond?

Mr. SMITH. —an issue of holding payment processors liable for the full amount of the fraud. This is an issue of marshaling the assets of the fraudster and freezing them. So these reserve accounts are——

Mr. MEADOWS. So you're saying what he just said, freezing the $40 million in his example——

Mr. SMITH. We're not freezing $40 million.

Mr. MEADOWS. Well, hold on.

Mr. SMITH. Reserve accounts don't have the full amount of the fraud in them. The reserve accounts have whatever the payments that the merchants or the processors——

Mr. MEADOWS. So are you saying there's not enough money in the reserve accounts to pay the consumers? Is that your sworn testimony here today?

Mr. SMITH. What I'm saying is——

Mr. MEADOWS. No, I—yes or no, is there enough money in the reserve accounts, like Mr. Oxman said, if you had the reserve account, that would actually go to her father or whomever if it was done improperly, is there enough money in the reserve accounts——

Mr. SMITH. There's never enough money in the reserve accounts because it represents a fraction of the fraud. It's just whatever money the payment processor is holding back for the last 60, 90, 180 days, whatever the contract is between the payment processor and the merchant.

Mr. MEADOWS. Okay. So why, then, if it's frozen, why would you freeze that?

Mr. SMITH. We would freeze it——

Mr. MEADOWS. Freeze the reserves.

Mr. SMITH. We would freeze the reserve account so that we can marshal all of the assets of the fraudster and make as close to full recompense as we can to all of the customers.

Mr. MEADOWS. So let's assume that you're following the money and the FTC follows the money and you freeze the assets. What happens when they're innocent?

Mr. SMITH. Well, we're not freezing the assets of anyone who's innocent. We're freezing the assets of the fraudster that are being held——

Mr. MEADOWS. So how do you know that they're guilty?

Mr. SMITH. I'm sorry?

Mr. MEADOWS. How do you know that they're guilty?

Mr. SMITH. Because a court has entered a temporary restraining order——

Mr. MEADOWS. You've got a court order. That's different than having an actual case.

Mr. SMITH. Well, no, we have to make a strong showing to the court—look, a TRO, an asset freeze——

Mr. MEADOWS. Right. Okay.

Mr. SMITH. —the appointment of a receiver, these are extraordinary remedies, and courts don't enter them lightly. We go into court without giving an opportunity for the other side to respond because the fear is that, if we do, the money, the evidence, the people will be——

Mr. MEADOWS. Gotcha. Okay. That makes sense. That makes sense.

So here's what I would ask of you, Mr. Smith, because you've got a long career not just in your new job but at the FTC, and, actually, I have found the people of the FTC to be very capable Federal servants. I mean, they actually are a great group. I actually, when I was a freshman, had a hearing with the FTC and found the engagement to be delightful.

Here is the concern that we're hearing. So, just as awful as some of those stories that Ms. Saunders has shared with us, we're hearing some stories from people who believe that they've had a disproportionate amount of attention based on through no fault of their own. And so it'd be like me processing something, and all of a sudden I find that I processed, through millions of different people, I had one bad actor, and then all of a sudden my entire business operation gets constrained. And we've got to find a way to deal with that too.

Because what happens—and whether it's additional reserves, whether it's actually looking at a more targeted approach. Because if we're not dealing with that, Mr. Smith, what we're doing is we're having a chilling effect on a number of different small businesses. And as a small-business guy, that's something that I'm not going to stand for.

And so I can tell by the way you're nodding that you're willing to help us work through this. This is not my issue. This is not one that, honestly, when I heard about it originally, I said, well, how could that be going on? If you're willing to come in and brief, you know, our staff or me personally, I am willing to look at that.

And I think, as a small-business guy, hopefully what I can do is help mediate the distance between Mr. Oxman, Ms. Saunders, and you, Mr. Smith, where we can come together and say, well, this is some good policy that we can change, and figure out what part is legislative and what part of it is administrative. Does that sound fair?

Mr. SMITH. Yes.

And I would add that, in most instances where we're talking about reserve accounts, that there is some sort of an accommodation that's agreed to by the parties. The ultimate issue over whether the receiver owns the reserve accounts is one for the court, but it doesn't usually get there, and we're able to reach some sort of an accommodation.

Mr. MEADOWS. So let me tell you what you may be getting a little bit of side benefit. Obviously, Operation Chokepoint was an issue that had a political agenda in some shape or fashion. The

other part that you're getting from me is seeing the FDIC do similar things when it comes to banking regulations and what they do. And so you may be getting a little bit of spillover, because I have seen the long arm of the FDIC, at times, do things that have an unbelievable chilling effect, that make absolutely no business sense whatsoever, in the name of protecting consumers.

And so I want to be fair to you. And so if—I see some of your staff nodding that they're willing to come in, so I assume that you're willing to bring your staff in to help, where we can work through that.

And, Mr. Oxman, I would ask you to give me a few more examples.

Ms. Saunders, if you will do the same from a consumer standpoint.

Hopefully, we can come together and we can fix this without another hearing. How about that? Does that sound good?

Mr. SMITH. We'd be happy to work with your staff.

Mr. MEADOWS. All right.

So, with that, I'd like to thank all of you for appearing today.

I think they're—well, they did call votes, and so hopefully I'll make it.

The hearing record will remain open for the next 2 weeks for any member who wants to submit an opening statement or questions.

So you may get followup questions from some of the those members.

Mr. MEADOWS. And if there's no further business before the subcommittee, it stands adjourned.

[Whereupon, at 11:39 a.m., the subcommittees were adjourned.]

○