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.