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).