UNITED STATES OF AMERICA

Federal Trade Commission

WASHINGTON, D.C. 20580

Office of the Chairman

Joint Statement of Chairman Andrew N. Ferguson and Commissioner Mark R. Meador
In the Matter of Nuvei
Matter Number 2223153

September 4, 2026

American citizens are inundated by foreign scams. Foreigners barrage our phone lines, text messages, emails, and social media with an infinite variety of scams designed to move money out of the pockets of hardworking, honest American citizens and into the hands of dishonest, cheating foreign criminals. This flood of foreign scam attacks on American citizens is a crisis. In just one year, Americans lost at least ten billion dollars to Southeast Asian scam networks alone.[1] And there is no reason to believe the torrent will stop any time soon, the foreign scammers continue to enrich themselves and their countries by impoverishing Americans. In 2023, for example, the equivalent of forty percent of the combined gross domestic product of Laos, Burma, and Cambodia came from scam centers in those countries. These scam operations also fuel human trafficking, which the scammers use to obtain their scam-center labor force.[2]

The Commission has limited tools to confront foreign scammers directly. These scam operations often violate our federal and state criminal laws, as well as those of the scammers' own countries. Experience shows that the threat of civil enforcement by the FTC in federal court does little to deter scammers many thousands of miles away who are comfortable running operations that violate countless criminal laws.[3] But the Commission has other tools to protect American

[1] H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, Crime, Corruption, and Power 10 (May 19, 2026), https://chinaselectcommittee.house.gov/media/press-releases/moolenaar-khanna-release-investigation-exposing-billion-dollar-china-linked-scam-centers-targeting-americans; see also Statement of Gregory Herb (Deputy Assistant Director, Criminal Division, Federal Bureau of Investigation) on *The Rising Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters* Before the Joint Econ. Comm. (Mar. 25, 2026), https://www.jec.senate.gov/public/_cache/files/2f5ca5c1-44c9-4e23-944e-8008293856f7/sfr-gregory-heeb.fbi.pdf.

[2] China's Exploitation of Scam Centers in Southeast Asia, U.S.-China Econ. & Sec. Rev. Comm'n (July 18, 2025), China's_Exploitation_of_Scam_Centers_in_Southeast_Asia_July_18_2025. "The explosive growth of scam centers in Southeast Asia has also fueled large-scale human trafficking." *Ibid.*

[3] Prepared Statement of the Federal Trade Commission on *The Rising Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters* at 6–7, Before the Joint Econ. Comm. (Mar. 26, 2026), https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf.

consumers, especially when foreign scammers have domestic accomplices providing them access to the U.S. financial systems and facilitating their fraudulent activities.

Across more than two decades,[4] the Commission has been working to "cut off foreign scammers' use of American companies to prey on American families"[5] by bringing actions against payment processors for their violations of the FTC Act and the Telemarketing Sales Rule's (TSR) prohibition on assisting and facilitating merchant fraud.[6] Payment processors are crucial intermediaries between consumers and merchants. A consumer cannot use their credit or debit card to purchase goods or services from a merchant unless that merchant has a relationship with a third party that gives them access to the card networks. Some merchants are specifically approved by banks to access the networks directly. But most merchants are forced to go through payment processors that have been approved by the banks to provide derivative access.[7]

As a condition of access, the card networks require banks and the banks' approved payment processors to implement policies designed to protect the networks and the consumers who depend upon them. The basic idea is that it is the bank's, and thus the payment processor's, job to prevent, identify, and address merchant misconduct. Payment processors must, for example, perform underwriting before agreeing to process payments for a merchant, and must monitor existing merchants for deceptive or otherwise illicit conduct. Accordingly, payment processors must learn about the merchant's identity, location, and offered products or services, and check the merchant against a list of merchants that the card networks have previously excluded for misconduct. It may also require looking at the merchant's "chargeback rate"—the proportion of transactions submitted by a merchant that consumers dispute as fraudulent. If red flags indicate that the merchant is deceiving consumers or engaging in other illegal conduct, the card network requires the bank, and

---

[4] See, e.g., Press Release, FTC, *Payment Processor for MOBE Business Coaching Scheme Settles FTC Charges* (June 1, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/06/payment-processor-mobe-business-coaching-scheme-settles-ftc-charges; Press Release, FTC, *FTC Action Bans Payment Processor from Using a Novel Payment Method to Debit Accounts* (Jan. 5, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/01/ftc-action-bans-payment-processor-using-novel-payment-method-debit-accounts; Press Release, FTC, *FTC Sues Electronic Payment Processors for Facilitating Fraudulent Telemarketing Schemes* (Feb. 11, 2004), https://www.ftc.gov/news-events/news/press-releases/2004/02/ftc-sues-electronic-payment-processors-facilitating-fraudulent-telemarketing-schemes (discussing *FTC v. First Am. Payment Processing, Inc.*, No. 04-cv-0074 (D. Ariz. Jan. 3, 2004)).

[5] Statement of Chairman Andrew N. Ferguson, joined by Comm'rs Melissa Holyoak & Mark R. Meador, *In re Paddle.com*, Matter No. 2223154, at 2 (June 16, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/paddle-anf-statement.pdf.

[6] See Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and the FTC's Telemarketing Sales Rule, 16 C.F.R. § 310.3.

[7] See Global Digital Payments Market Statistics 2026, MerchantSavvy (last accessed July 13, 2026) (showing that the vast majority of U.S. merchants use payment processors like Stripe and Square to accept credit- and debit-card payments), https://www.merchantsavvy.co.uk/digital-payment-market/.

thus the payment processor, to deny or terminate access and, in the latter circumstance, to report the fact of, and reason for, termination to the card networks.

Because payment processors control most merchants' access to the debit- and credit-card ecosystem, they are well-positioned to protect and reinforce the integrity of the payments system against dishonest or fraudulent merchants. The entire American debit- and credit-card ecosystem depends on processors guarding this access responsibly and in good faith. When they do so, Americans enjoy the convenience of a trusted payments system that lets them spend their money as they wish and receive the goods and services that they want. Payment processors that engage in unfair payment-processing practices or other law violations (such as violation of the TSR), on the other hand, put Americans at risk by providing a tool for scammers to reach consumers they otherwise could not. This sort of misconduct undermines the payments system and harms American consumers.

Section 5 of the FTC Act is the Commission's most useful tool for confronting payment processors who facilitate foreign scams. It prohibits "unfair or deceptive acts or practices."[8] As a general matter, a practice is unfair if it (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or competition.[9] The general principles motivating our enforcement against unfair practices are the protection of free markets and consumers' ability to make informed choices as participants in those markets.[10] We have applied these principles to payment processors by treating as unfair processing payments for a merchant after being made aware of fraudulent activity[11]; directly facilitating merchants' avoidance of fraud-prevention measures through, for example, "credit card laundering" or "load balancing"[12]; and ignoring a

---

[8] 15 U.S.C. § 45(a)(1).
[9] *Id.* § 45(n).
[10] *In re Int'l Harvester Co.*, 104 F.T.C. 949, 1060 n.47 (1984) ("The principal focus of our unfairness policy is on the maintenance of consumer choice or consumer sovereignty, an economic concept that permits specific identification of conduct harmful to that objective."); *Am. Fin. Servs. Ass'n. v. FTC*, 767 F.2d 957, 976 (D.C. Cir 1985) ("[C]ertain types of seller conduct or market imperfections may unjustifiably hinder consumers' free market decisions and prevent the forces of supply and demand from maximizing benefits and minimizing costs. In such instances of market failure, the Commission may be required to take corrective action.").
[11] See, e.g., Press Release, FTC, *Payment Processor for MOBE Business Coaching Scheme Settles FTC Charges* (Jun. 1, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/06/payment-processor-mobe-business-coaching-scheme-settles-ftc-charges; Press Release, FTC, *Payment Processor and its Former CEO Pay $1.5 Million to Settle FTC Charges They Facilitated Fraud* (Dec. 10, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/payment-processor-its-former-ceo-pay-15-million-settle-ftc-charges-they-facilitated-fraud.
[12] See, e.g., Press Release, FTC, *FTC Takes Action Against BlueSnap and its Former CEO and Senior VP for Credit Card Laundering, Processing Payments for Known Scammer* (May 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-takes-action-against-bluesnap-its-former-ceo-senior-vp-credit-card-laundering-processing; Press Release, FTC, *Worldwide Payment Processor and Payments Industry Executive to Pay $40.2 Million to Settle FTC Charges of Assisting Fraudulent Schemes and Credit Card Laundering* (May 19, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/05/worldwide-payment-processor-payments-industry-

processor's own written or governing policies that would ordinarily require them to stop processing for merchants engaged in fraud.[13] Such practices allow scammers, often continents away, to reach their hands into American pockets, degrading consumers' trust in the payments system and, more importantly, exposing American consumers to injuries from which they would be insulated but for the decision to unlock and open the door for scammers.

Last year, the Commission brought an action against a payment-processing company alleged to have knowingly assisted foreign scammers in accessing the American debit- and credit-card ecosystem.[14] Today's case builds upon that effort. In a complaint filed in the United States District Court for the District of Arizona, the Commission alleges, among other things, that Nuvei opened and maintained payment-processing accounts for merchants it knew, or should have known, were engaging in unlawful conduct and otherwise assisted those merchants in avoiding the card networks' fraud-monitoring systems. The FTC's complaint also charges Nuvei with violating the TSR by providing substantial assistance and support to foreign merchants—namely Restoro and Reimage—that Nuvei knew, or consciously avoided knowing, were engaged in deceptive telemarketing. Nuvei's alleged practices injured American consumers by eluding the anti-fraud defenses intended to prevent malicious actors from defrauding American citizens and funneling hard-earned dollars to foreign scammers.

According to the Commission's complaint, Nuvei had written policies prohibiting the onboarding of:

- Merchants from certain industries plagued by foreign fraudsters, such as computer anti-virus software that is "sold via inaccurate advertisements";
- Merchants that were "previously identified by any Card Brand for deceptive practices";
- Merchants with "a history of excessive chargebacks or fraud"; and

---

executive-pay-402-million-settle-ftc-charges-assisting; Press Release, FTC, *FTC Adds Latvian Financial Institution, CEO to Case against Apex Capital Group* (May 31, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/05/ftc-adds-latvian-financial-institution-ceo-case-against-apex-capital-group; Press Release, FTC, *FTC Acts to Block Payment Processor's Credit Card Laundering for Tech Support Scammers* (Apr. 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-acts-block-payment-processors-credit-card-laundering-tech-support-scammers.

[13] See Complaint ¶¶ 46–58, *FTC v. Qualpay*, No. 20-cv-00945 (M.D. Fla. Jun. 1, 2020), https://www.ftc.gov/system/files/documents/cases/qualpay_complaint.pdf; Complaint ¶¶ 42, 52, *FTC v. Complete Merchant Solutions*, No. 20-cv-00864 (D. Utah Dec 9, 2020), https://www.ftc.gov/system/files/documents/cases/ftc_v._cms_-_complaint_for_posting.pdf.

[14] See Press Release, FTC, *Paddle Will Pay $5 Million to Settle FTC Allegations of Unfair Payment-Processing Practices and Facilitation of Deceptive Tech-Support Schemes* (June 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/06/paddle-will-pay-5-million-settle-ftc-allegations-unfair-payment-processing-practices-facilitation.

- Merchants whose "true beneficial ownership is not clear or is masked."[15]

But the complaint alleges that Nuvei ignored these policies when it was profitable to do so. Nuvei allegedly processed over $30 million for the infamous Reimage tech support scam[16] through multiple channels despite knowing that Reimage was actively funneling money from American consumers to foreign scammers.[17] Even though Nuvei had received many complaints about Reimage, and even though its own underwriters flagged the scam as "very bad," Nuvei allegedly processed the transactions anyway and helped the scammers avoid detection by banks and the card networks because it "kn[e]w reimage (and the owner [smiley face emoji])" and because it was profiting handsomely from the business.[18] Nuvei allegedly assisted other scammers in similar ways.[19] These allegations about Nuvei's practices easily satisfy the elements of unfairness set out in Section 5(n) of the FTC Act.[20]

To resolve these allegations, Nuvei has agreed to: (1) a ban on processing payments for tech-support providers who engage in telemarketing or use pop-up advertisements and for merchants on Mastercard's high-risk-merchant list; (2) a prohibition on making or assisting others in making false or misleading statements; (3) a prohibition on helping merchants circumvent fraud-monitoring systems; and (4) an injunction requiring defendants to implement and adhere to strict underwriting and monitoring requirements. Nuvei additionally agreed to pay $4.85 million in redress to consumers.

Payment processors may be liable indirectly for injuries directly caused by bad-actor merchants if they process payments for which the "injury was a predictable consequence."[21] And it is predictable that any payment processor willing to process payments for unproven merchants will eventually provide services to a bad actor and will thus process a fraudulently induced payment. That is true even for payment processors that faithfully apply every industry-standard anti-fraud measure; some bad merchants will inevitably slip through the nets. If that fact alone were sufficient to impose liability under Section 5, payment processors would either abandon the

---

[15] Compl. ¶¶ 50–53.
[16] See Press Release, FTC, *FTC Sends More than $25.5 Million to Consumers Impacted by Tech Support Firms' Scam* (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/ftc-sends-more-255-million-consumers-impacted-tech-support-firms-scam; Press Release, FTC, *Paddle Will Pay $5 Million to Settle FTC Allegations of Unfair Payment-Processing Practices and Facilitation of Deceptive Tech-Support Schemes* (June 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/06/paddle-will-pay-5-million-settle-ftc-allegations-unfair-payment-processing-practices-facilitation.
[17] Compl. ¶¶ 63–158.
[18] *Id.* ¶¶ 91–92.
[19] *Id.* ¶¶ 159–83.
[20] 15 U.S.C. § 45(n).
[21] See *FTC v. Neovi*, 604 F.3d 1150, 1156 (9th Cir. 2010).

practice of processing payments for all but the most tried-and-true merchants, or be left to hope for a consistently favorable exercise of prosecutorial discretion.

Fortunately, Section 5 does not put payment processors to that choice. Section 5 does not impose liability for an allegedly unfair act or practice solely on the basis of a consumer injury. The Commission must also show that the injury was substantial, that the injury was unavoidable, and that the act or practice does not have countervailing benefits to consumers or competition. Processing a payment for a merchant engaged in fraud clearly satisfies the injury, substantiality, and unavoidability requirements. The Commission therefore must balance the injury caused by the act or practice against any countervailing benefits of the act or practice.

For payment processors, we think the balance cuts decisively in favor of a knowledge requirement and against strict liability. The injuries being inflicted on Americans by scammers are grave and far-reaching.[22] The payment processor who knows, should know, or is consciously avoiding knowledge that it is granting bad actors engaged in scamming American consumers access to those consumers is a scourge. And there are no countervailing benefits to offset consumers' resultant injuries. By contrast, the good-faith payment processor working to grant small businesses, startups, and other risk-taking enterprises access to America's consumers serves a critical role in maintaining our envy-of-the-world payments network, providing immense countervailing benefits to both consumers and competition.

Without a knowledge requirement, good-faith payment processors would be on the hook for all their merchant clients' fraudulent conduct even when they deployed industry-standard anti-fraud measures to protect consumers and had no basis to know (and did not consciously avoid knowing) of any merchant wrongdoing. If simply opening a payment-processing account for any merchant that engages in any unlawful practice violated Section 5, irrespective of how thorough the processor's underwriting or compliance procedures were, payment processors would be forced to exclude legitimate merchants from the payments system, hindering those merchants and eliminating significant benefits to consumers. Strict liability for merchant fraud would deprive Americans of the massive, convenient payment networks that make the modern economy possible. Section 5's prohibition on unfair acts or practices does not require that.

The Commission has never brought an unfair-payment-processing action in the absence of evidence that the payment processor knowingly helped scammers.[23] Yet we have never formally

---

[22] See *supra* n.1.

[23] See Prepared Statement of the Federal Trade Commission on *The Federal Trade Commission's Enforcement of Operation Chokepoint-Related Businesses* at 10, Before the Subcomms. on Nat'l Sec. and Gov't Oversight of the H. Comm. on Oversight and Gov't Reform (July 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395770/p180101_commission_testimony_re_operation_chokepoint-related_businesses_07262018.pdf ("When a payment processor helps a fraudulent merchant take money from consumers—either by actively helping the

taken the position that an unfair-payment-processing claim requires that the payment processor have actual or constructive knowledge of a merchant's wrongdoing.[24] Indeed, despite pleading allegations sufficient to demonstrate such knowledge, we have never actually pleaded that a defendant had it. Today, however, we plead that Nuvei knew of the merchants' wrongdoing because we have concluded that Section 5 imposes a knowledge requirement in unfair-payment-processing claims. That is, we read Section 5 to require the Commission to plead, and eventually to prove, that the processor knew, should have known, or consciously avoided knowing that the merchant's transactions involved unfair or deceptive acts or practices or otherwise unlawful conduct.

Of course, actual or constructive knowledge may be adduced or inferred from a wide range of evidence. There is no single fact that demonstrates a lack of knowledge. Nor can a payment processor bury its head in the sand to avoid learning the truth about what its existing or prospective merchants are doing. The mere fact that a merchant's chargeback rates were low, for example, does not mean that a payment processor did not know, from other facts it was or should have been aware of, that the merchant was engaged in unlawful behavior. For example, we will attribute to a payment processor knowledge of those facts which it would have uncovered had it engaged in the sort of fraud-prevention practices and investigations that the card networks require.

* * *

Today's complaint shows that the FTC under President Trump is committed to protecting American consumers from scammers and fraudsters of all types, while also being mindful of the limits on our broad unfairness authority. Payment processors are crucial intermediaries between businesses and consumers that must take their role seriously and operate in good faith to screen out bad actors; they should be able to do so without fear that they will become responsible whenever an associated merchant behaves poorly. But if payment processors do not take their fraud-prevention role seriously, the Commission will move swiftly to compel them to do so.

---

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.").

[24] See 15 U.S.C. §§ 45(b), 57a(1)(B).