HUDSON COOK

Enforcement Alert from Hudson Cook: FTC Settles with Two Payment Processors Over Alleged Unfair and Deceptive Processing Practices

September 18, 2026 | Webb McArthur and Tracy Wang

HIGHLIGHTS:

- The FTC announced settlements with two payment processors, one for $4.85 million and the other for $12 million.
- The FTC alleged that a Canada-based payment processor processed payments for merchants it knew or should have known were engaged in deceptive practices, including tech support scams. The company neither admitted nor denied the FTC's allegations except as specifically stated in the settlement agreement.
- The FTC alleged that an Arizona-based payment processor processed payments for merchants engaged in unauthorized billing schemes and maintained merchant accounts for more than 1,000 shell entities allegedly used to facilitate fraud. The company neither admitted nor denied the FTC's allegations except as specifically stated in the settlement agreement.
- Statements by FTC officials in both matters underscore the agency's view that payment processors serve as critical gatekeepers in the payments ecosystem and may face enforcement scrutiny when they allegedly ignore red flags of fraud, deceptive practices, or consumer harm.

CASE SUMMARY:

On September 4, 2026, the Federal Trade Commission ("FTC") announced that a global payment processor based in Canada agreed to pay $4.85 million to settle claims that it opened and maintained payment processing accounts for merchants that it knew or should have known were engaged in deception, including tech support scams. The company neither admitted nor denied any of the allegations in the complaint except as specifically stated in the settlement agreement.

In its complaint, the FTC alleged that the company violated Section 5 of the FTC Act for engaging in unfair or deceptive acts or practices in or affecting commerce, including unfair payment processing practices. The FTC also alleged that the company violated the Telemarketing Sales Rule ("TSR") by providing substantial assistance and support to sellers or telemarketers that it knew, or consciously avoided knowing, were violating the TSR through misleading statements designed to induce the purchase of goods or services.

The Company operated a global payment processing business and allegedly facilitated a tech-support scam known as Reimage. According to the FTC, the Company opened numerous merchant accounts for Reimage and distributed Reimage's transactions, including chargebacks from allegedly deceived consumers, across multiple accounts. This practice purportedly helped conceal Reimage's excessive chargeback rates from card network fraud-monitoring programs. The FTC further alleged that, despite receiving a warning from Visa that Reimage was impersonating Microsoft, the Company increased its payment processing services for Reimage. In addition, the Company allegedly opened and maintained merchant accounts for Reimage despite knowing that the merchant account applications contained false information regarding Reimage's ownership and business location, which obscured Reimage's offshore telemarketing operations. According to the complaint, the company's payment processing practices enabled the scheme to obtain over $30 million from consumers.

The FTC also alleged that the company opened and maintained merchant accounts for merchants engaged in deceptive practices, including tech support providers, business opportunity sellers making false or unsubstantiated earnings claims, entities impersonating government tax authorities, and merchants that had previously been terminated by payment processors or acquiring banks for excessive chargebacks, fraud, or other misconduct.

Under the proposed order, the company will pay $4.85 million in monetary relief and will be prohibited from engaging in certain unfair or deceptive payment processing practices. The order also imposes extensive compliance obligations, including restrictions on providing payment processing services to certain high-risk merchants, prohibitions on practices designed to evade fraud and risk-monitoring programs, and enhanced merchant screening and monitoring requirements.

In announcing the settlement, Christopher Mufarrige, Director of the FTC's Bureau of Consumer Protection, stated that the action demonstrates the FTC's commitment to ensuring that the payments system operates "free of fraud" and reinforces the transparency and trust on which consumers and businesses rely. According to Mufarrige, consumers deserve a payment system that is "competitive, transparent and fortified against fraud," and the FTC will take action when those standards are threatened.

On September 8, 2026, the FTC announced a second settlement agreement, this one with an Arizona-based payment processor. The company agreed to pay $12 million to settle allegations that it processed payments for merchants that defrauded consumers through unauthorized billing schemes. The company neither admitted nor denied any of the allegations in the complaint, except as specifically stated in the settlement agreement.

In its complaint, the FTC alleged that the company violated Section 5 of the FTC Act by engaging in unfair payment processing practices. According to the FTC, the company opened and maintained merchant accounts for more than 1,000 shell entities that served as fronts for undisclosed third parties engaged in fraudulent online marketing and unauthorized billing schemes. The FTC alleged that the company processed more than $100 million in transactions through these sham merchant accounts.

The FTC further alleged that the company opened and maintained these accounts despite numerous indicators of fraud, including excessive chargeback rates, signs of credit card laundering, the use of shell companies and straw signers, and warnings from Mastercard and the company's personnel regarding widespread load balancing and transaction-laundering activity. The FTC also alleged that the company attempted to increase transaction volume through these accounts by placing them on a lower-risk bank identification number ("BIN") associated with an affiliated entity, thereby increasing the likelihood that transactions would be approved by card issuers.

According to the FTC, many of the shell merchant accounts were connected to unauthorized billing schemes and other deceptive online marketing operations, including entities associated with an unauthorized billing and credit card laundering operation that the FTC had shut down in 2024.

Under the proposed order, the company will pay $12 million in monetary relief and will be prohibited from engaging in or assisting credit card laundering. The order also prohibits the company from processing payments for certain high-risk merchants, including straw companies, certain merchants on Mastercard's MATCH list, and merchants previously subject to law enforcement actions. In addition, the order imposes enhanced merchant screening, monitoring, and sales agent oversight requirements, and prohibits tactics designed to evade fraud and risk monitoring programs, including load balancing.

Katherine White, Deputy Director of the FTC's Bureau of Consumer Protection, stated that the company allegedly continued processing payments despite red flags indicating that certain merchants were engaged in fraudulent activity. White noted that the case underscores the FTC's commitment to holding companies accountable when they knowingly support fraudulent businesses.

RESOURCES:
You can review all of the relevant court filings and press releases at the FTC's Enforcement page.

Against Cananda-Based Payment Processor:

- Press Release
- Complaint
- Consent Order

Against Arizona-Based Payment Processor:

- Press Release
- Complaint
- Consent Order

Enforcement Alerts by Hudson Cook, LLP, written by the attorneys in the firm's Government Investigations, Examinations and Enforcement and Litigation practice groups, are provided to keep you informed of federal and state government enforcement actions and related actions that may affect your business. Please contact our attorneys if you have any questions regarding this Alert. You may also view articles, register for an upcoming CFS Bites monthly webinar or request a past webinar recording on our website.

HUDSON
COOK

Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

hudsoncook.com