FinCEN Scam Alerts Push Banks To Rethink AML Monitoring

By **Kelly Lenahan-Pfahlert and Matthew Smith** (October 30, 2026)



Kelly Lenahan-Pfahlert



Matthew Smith

On Sept. 3, the Financial Crimes Enforcement Network released two companion publications on digital asset investment scams.

The first, a financial trend analysis, reviews Bank Secrecy Act reporting filed between September 2023 and the end of 2025.[1] The second, Alert FIN-2026-Alert005, addresses money laundering associated with the transnational scam centers, concentrated in Southeast Asia, that perpetrate much of this fraud.[2]

On their face, the documents are a typology update. In substance, they mark a change in what the anti-money laundering regime is expected to do. That regime was designed to detect criminals moving their own proceeds. FinCEN now expects banks; money services businesses, or MSBs; and virtual asset service providers to detect fraud in which the customer moving the money is the victim, not the offender.

That expectation reaches three core program functions: how institutions monitor customers, when they file suspicious activity reports (known as SARs), and how they investigate digital asset flows.

The Traditional Model and Its Limits

The BSA regime developed around a familiar paradigm. The customer — or someone controlling the customer's account — is the presumptive wrongdoer. A launderer has to use the financial system, and in doing so leaves traces that diverge from what a legitimate customer would do.

Fraud has always been reportable, but the core design assumption of most monitoring programs remains that suspicious activity reflects the customer's own illicit purpose. Scam center fraud breaks that assumption.

Why Scam Center Operations Are Different

The financial trend analysis describes the dominant pattern: Scammers instruct victims to open accounts with MSBs that offer digital asset services, to purchase specific digital assets and then to send those assets to addresses the scammers control.

FinCEN observes that institutions have reported difficulty detecting this pattern "because the victim technically maintains control of funds in the accounts at the MSB before any scam proceeds are transferred to scammer-controlled addresses."

Scammers typically direct victims to reputable centralized exchanges, which means the onboarding transaction looks like what it nominally is: a customer buying cryptocurrency through a legitimate platform.

The money moves fast and across rails. The financial trend analysis adds that, regardless of

the asset used in the original investment, scammers nearly always exchanged proceeds for stablecoins, almost exclusively Tether, or USDT.

The scale is substantial. FinCEN analyzed 33,904 BSA reports from roughly 1,300 institutions, involving about $12.7 billion in reported activity. FinCEN itself cautions that growth in reporting may indicate increased adoption of its 2023 key term and does not necessarily indicate an accelerating rate of scams.

Two further features matter for program design. First, because scammers spread funds across many institutions, most filers reported only "a snapshot of different phases in a scam's lifecycle," according to FinCEN. No single institution sees the whole scheme.

Second, the data does not support treating this as primarily an elder fraud problem. Elder financial exploitation appeared in nearly 25% of the reports, roughly in line with older adults' approximately 25% share of the population under the 2020 census.

Programs that route scam detection through elder exploitation protocols alone risk missing the roughly three-quarters of the reported activity that did not involve elder exploitation.

By emphasizing these patterns and publishing detailed indicators, FinCEN is implicitly describing capabilities that it expects institutions to develop. The guidance therefore functions not only as a description of emerging risk but also as a road map for supervisory expectations.

What the Guidance Signals About SAR Expectations

The alert restates the SAR standard, including the prong that captures a transaction that "involves the use of the financial institution to facilitate criminal activity." That prong, rather than the more familiar focus on proceeds of the customer's own crime, is the natural fit for victim-initiated transfers.

The practical implication is that an institution may need to file on activity by a customer it believes is acting in good faith, and to describe in the narrative a criminal actor who is not its customer and whom it may never identify.

FinCEN's requests regarding SAR content are telling. It asks filers to include cyber and blockchain indicators such as chat logs, phone numbers, social media usernames, email addresses, transaction hashes, wallet addresses, apps used, and relevant URLs, domains and IP addresses. They are inputs for disruption: attribution, address clustering and fund recovery.

The financial trend analysis notes that some MSB filings helped law enforcement link networks of scammers and victims to common addresses, and that FinCEN's Rapid Response Program has, since its inception in 2015, facilitated the interdiction of $1.8 billion and the recovery of more than $1 billion in stolen proceeds on behalf of 5,790 U.S. victims since 2015.

The guidance also reflects a timing problem. FinCEN reports that institutions often became aware of scam activity only after the scheme had concluded or after the victim had already lost significant sums. The implicit expectation is earlier detection and filing, together with the joint SARs and Section 314(b) information sharing the alert encourages.

Institutions should also expect examiners to ask how they handled cases in which staff

identified a likely scam, warned the customer and processed the transaction anyway. Documenting the warning, the customer's response and the filing decision will matter.

At the same time, FinCEN states that no single red flag is determinative and that institutions should weigh a customer's historical activity and the presence of multiple related indicators. The guidance does not make every cryptocurrency purchase reportable, but it does ask institutions to build the capacity to recognize when an ordinary-looking purchase is part of an extraordinary pattern.

Although an alert does not create new legal obligations, it often establishes a practical supervisory benchmark. Institutions that cannot demonstrate reasonable efforts to identify and investigate scam center activity may increasingly find themselves explaining program design choices to examiners, particularly as fraud prevention becomes more central to anti-money laundering effectiveness assessments.

Implications for Monitoring and Cryptocurrency Investigations

For banks and broker-dealers, the most useful signals in the FinCEN materials are behavioral and narrative. Depository institutions detected schemes when customers sent funds to digital asset MSBs, wired money to beneficiaries with references to digital asset investments, moved large sums between their own accounts, or applied for loans and second mortgages.

Customers described an online romantic partner, friend, mentor or business partner guiding their decisions, or referred to a trusted adviser while refusing to discuss that person. Securities and futures firms most often flagged liquidation of investment accounts to fund digital asset purchases.

Detecting these patterns depends heavily on front-line staff and on escalation paths that treat a customer's explanation as data rather than as a resolution.

For virtual asset service providers, the materials point to on-chain monitoring that is oriented toward counterparties, not just customers. Some MSBs identified scam activity by observing multiple apparent victims sending funds to the same suspicious addresses.

The alert's red flags include transactions with unattributed address clusters that share blockchain infrastructure with a known guarantee marketplace, direct or indirect exposure to marketplace-attributed addresses without apparent lawful purpose, and substantial use of a stablecoin whose issuer advertises that it cannot be seized or frozen.

Notably, a separate group of red flags is aimed at the laundering side rather than the victim side. It includes customers receiving stablecoins from U.S. exchanges followed by on-chain laundering patterns, deposits from wallets aggregating suspected scam proceeds, and large volumes of offsetting transactions consistent with operating as an over-the-counter broker or peer-to-peer exchanger.

FinCEN observes that underground banking services connected to scam proceeds typically rely on liquidity from large digital asset MSBs. An exchange can therefore be both the on-ramp for a victim and the liquidity source for a launderer, and its program must address both exposures.

The Huione Group **actions** illustrate why counterparty monitoring has to be dynamic. FinCEN's Section 311 final rule, published on Oct. 16, 2025, cut the Cambodia-based group

off from the U.S. financial system, and a proposed rule, published June 25, 2026, would expand the definition of Huione Group to include H-Pay Service PLC, to which FinCEN assessed Huione Group shifted operations to evade the special measure, and to add and define the term "successor entity."[3]

The alert accordingly flags payment service providers that change names, branding or websites in an apparent effort to disguise association with a marketplace subject to enforcement or takedowns.

The Broader Enforcement Trajectory

The alert also should be understood in the context of a broader shift in enforcement priorities. Over the last several years, the U.S. Department of the Treasury and law enforcement agencies have increasingly characterized transnational fraud, cyber-enabled crime, and digital-asset-enabled scams as core illicit finance threats rather than as peripheral consumer protection concerns.

Consistent with that development, the alert cites the U.S. Department of the Treasury's 2026 National Money Laundering Risk Assessment for the proposition that fraud remains one of the largest sources of illicit proceeds in the U.S., notes that fraud and cybercrime are among FinCEN's AML and countering the financing of terrorism national priorities, and invokes Executive Order No. 14390, signed March 6, 2026, on combating cyber crime, fraud and predatory schemes against Americans.[4]

Recent enforcement activity reflects that shift. In November 2025, the U.S. Attorney's Office for the District of Columbia, together with the DOJ's Criminal Division, the FBI and the U.S. Secret Service, announced the creation of a Scam Center Strike Force.[5]

These developments suggest that fraud facilitation is moving toward the center of how regulators evaluate AML program effectiveness. The FinCEN materials do not create new legal obligations, and an alert is not a rule. But the guidance gives examiners and prosecutors a detailed, public account of what FinCEN believes institutions should be able to see.

Institutions most exposed to that benchmark are those operating at the points of conversion the materials identify: digital asset exchanges, kiosk operators, payment processors and banks serving digital asset MSBs.

FinCEN's reminder of its whistleblower program adds another potential source of scrutiny.

What Compliance Programs Should Take From This

Several adjustments follow from the guidance. Risk assessments should address fraud facilitation as a distinct risk rather than treating it as a subset of customer fraud or elder exploitation. Monitoring scenarios should combine funding-source signals, such as retirement liquidation and new borrowing, with outbound digital asset activity.

Virtual asset providers should integrate blockchain analytics into both victim-side and counterparty-side reviews and refresh attribution data frequently. SAR narratives should capture the cyber and on-chain indicators FinCEN has requested. And institutions should make active use of sharing in Section 314(b) of the USA PATRIOT Act, given that no single filer sees more than part of a scheme.

Taken together, the guidance suggests that future AML examinations and enforcement actions may focus less exclusively on whether institutions detect the movement of criminal proceeds and more broadly on whether they can identify fraud schemes before victims suffer catastrophic losses.

The institutions best positioned to meet those expectations will be those that integrate traditional AML controls with fraud detection, cyber intelligence and digital asset investigative capabilities.

The traditional AML model asks whether the customer is the criminal. FinCEN's guidance asks institutions to recognize when the customer is the instrument of someone else's crime, and to report it in a way that helps the government reach the people behind it. That is a harder question, and it is now part of the job.

Kelly Lenahan-Pfahlert is a senior staff attorney and Matthew Smith is a partner at Ballard Spahr LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Fin. Crimes Enf't Network (FinCEN), U.S. Dep't of the Treasury, Financial Trend Analysis: Digital Asset Investment Scams: 2023–2025 Threat Pattern & Trend Information 1, 4, 7, 9–12 (Sept. 3, 2026).

[2] FinCEN, U.S. Dep't of the Treasury, FIN-2026-Alert005, FinCEN Alert on Money Laundering Activity Associated with Digital Asset Investment Scam Centers 1–6, 9–12, 16 (Sept. 3, 2026).

[3] Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 48,295 (Oct. 16, 2025) (codified at 31 C.F.R. § 1010.664); Definition of Huione Group, a Financial Institution Operating Outside the United States of Primary Money Laundering Concern, 91 Fed. Reg. 38,340 (proposed June 25, 2026) (to be codified at 31 C.F.R. pt. 1010).

[4] U.S. Dep't of the Treasury, 2026 National Money Laundering Risk Assessment 1 (Mar. 2026); FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities 1 (June 30, 2021); Exec. Order No. 14,390, 91 Fed. Reg. 12,051 (Mar. 11, 2026).

[5] Press Release, U.S. Att'y's Off. for D.C., New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans (Nov. 12, 2025).