BURGHERGRAY LLP CLIENT ALERT

FINCEN RAISES RED FLAGS ON CVC KIOSKS—WHAT FINANCIAL INSTITUTIONS NEED TO KNOW NOW

by Trina L. Glass | August 11, 2025

On August 4, 2025, the Financial Crimes Enforcement Network ("FinCEN") issued an urgent notice to the financial industry urging vigilance against the misuse of convertible virtual currency ("CVC") kiosks which are rapidly becoming conduits for scams, fraud, and cross-border money laundering—particularly by drug trafficking organizations and transnational criminal networks. The notice, FIN-2025-NTC1[1] (the "Notice") comes with sharp red flag indicators, actionable compliance expectations, and a clear call to financial institutions to be vigilant and proactive.

According to the FBI's Internet Crime Complaint Center, over 10,900 fraud complaints were tied to CVC kiosks in 2024 representing nearly $247 million in losses, including a disproportionate number of elder fraud cases. Even more alarming, that figure marks a 99% spike in complaints from 2023. FinCEN's own analysis, layered with law enforcement data, confirms what many compliance professionals already suspect: these ATM-like terminals, many of them operating without proper registration or anti-money laundering ("AML") protocols, are easy targets for exploitation.

WHAT ARE CVC KIOSKS—AND WHY DO THEY MATTER?

CVC kiosks, commonly referred to as "crypto ATMs," allow users to exchange fiat currency (cash or card) for digital assets like Bitcoin, Ethereum, or stablecoins. They are typically located in convenience stores, gas stations, shopping malls and other high-traffic locations. While these machines offer convenient entry points into the digital asset ecosystem, their physical accessibility, cash-based transactions, and fragmented oversight make them ripe for abuse and a high rate of noncompliance.

Scammers exploit their simplicity. Victims are often guided step-by-step by fraudsters on how to withdraw money, locate a kiosk, and send the funds, either by scanning a QR code or depositing cash at a CVC kiosk, unknowingly sending funds directly into a scammer's crypto wallet. Once a scam payment is made, criminals often aggregate funds from multiple victims into a single CVC wallet. They then use a technique called "chain-hopping," quickly swapping the CVC into a stablecoin via cross-chain bridges. The transaction is fast, irreversible, and often untraceable.

Even more concerning is the widespread failure of many CVC kiosk operators to comply with their obligations under the Bank Secrecy Act ("BSA"). According to FinCEN, there is substantial non-compliance with both federal and state regulatory requirements, including failures to register as money services businesses ("MSBs"), implement and maintain adequate AML programs, and adhere to customer identity verification protocols. For example, some CVC kiosk operators fail to implement effective AML/CFT programs because they neglect to collect, retain, and verify customer identification. In some cases, non-compliant operators have been found to provide false information to financial institutions to acquire accounts, or they may engage in money laundering themselves by structuring transactions or using personal accounts for business.

1 FIN-2025-NTC1

RED FLAGS FOR FINANCIAL INSTITUTIONS

The Notice is more than a bulletin—it is a strategic roadmap for navigating regulatory expectations and a guide for compliance moving forward. The agency lays out clear red flag indicators for both depository institutions and CVC kiosk operators. Among the most notable:

- **Structured transactions**: Customers making multiple deposits just below the SAR ($2,000) or Currency Transaction Report ($10,000) threshold, either across machines or locations.
- **Geographically dispersed activity**: Multiple customers depositing into the same crypto wallet from different cities or states.
- **Rapid layering**: Large CVC deposits quickly transferred through several addresses, swapped into stablecoins, or moved across blockchains (a tactic known as "chain-hopping").
- **Unusual client behavior**: Elderly or inexperienced clients suddenly making large CVC-related withdrawals after contact from "support" or "government" representatives.

Financial institutions should view these patterns not as anomalies, but as indicators of elevated and immediate risk. In particular, older customers withdrawing large sums from retirement accounts for CVC transfers demand closer scrutiny. The Federal Trade Commission has identified that people aged 60 and over are more than three times as likely to report a loss using a CVC kiosk than younger adults, and they account for more than two-thirds of the total reported losses.[2]

THE REGULATORY BOTTOM LINE

Be clear, financial institutions are not insulated from the misconduct of CVC kiosk operators. If your institution services a client that operates these machines, especially one that is not registered as an MSB or shows signs of BSA noncompliance, you could be exposed to regulatory risk. FinCEN specifically highlights cases in which kiosk operators provided false information to open accounts, structured transactions to avoid reporting, or used personal accounts to obscure the nature of their business.

At least 20 states have proposed or passed laws governing crypto ATMs, e.g., recent amendment to California's Digital Financial Assets law which, among other things, restricts daily transaction limits[3] and Colorado's Vending of Digital Assets Act[4] which requires CVC owners to warn customers about potential fraud and established dollar limits on daily transactions through the machines. Iowa's Attorney General, as a result of its investigations into CVC owners, has even initiated lawsuits against CVC kiosk firms alleged to have facilitated over $20 million in fraud with the majority of the scammed victims over the age of 60.[5]

The message is clear: noncompliance is not just a regulatory misstep; it is a legal liability.

2 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers

3 Cal. Fin. Code §§ 3905, 3902

4 https://leg.colorado.gov/bills/sb25-079

5 https://www.iowaattorneygeneral.gov/newsroom/attorney-general-bird-sues-crypto-atm-companies-for-costing-iowans-more-than-20-million

ACTION ITEMS FOR COMPLIANCE TEAMS

1. **SARs and Keyword Tagging**: FinCEN requests that institutions tag any relevant Suspicious Activity Reports with the key term "FIN-2025-CVCKIOSK" in SAR Field 2 and the narrative. Reports should include all relevant account details, customer identifiers, and links to related transactions or entities. FinCEN strongly encourages information sharing under the safe harbor authorized by section 314(b) of the USA PATRIOT Act. Collaborating with other financial institutions will prove crucial for identifying and preventing these schemes. Additionally, all books and records must be preserved for five years.

2. **Conduct a Targeted Review of Client Relationships**: Identify any clients that operate CVC kiosks or provide services to entities engaged in such activity. Verify whether these clients are properly registered as MSBs with FinCEN, maintain a reasonably designed AML program, and are in compliance with all applicable federal and state licensing and regulatory requirements.

3. **Enhance KYC and Transaction Monitoring**: Implement enhanced due diligence measures for clients with exposure to CVC activity. Where feasible, leverage blockchain analytics tools to detect transaction layering, smurfing tactics, and links to wallets associated with illicit activity. Reevaluate client onboarding protocols and transaction monitoring systems to ensure they align with current risks. Robust initial and ongoing due diligence will be critical to managing exposure and ensuring regulatory compliance.

4. **Train the Frontline**: Implement targeted training for your financial professionals, including call center representatives as they will most likely be the first to notice suspicious activity. Provide them with scripts, FAQs, and escalation procedures to recognize and respond to red flags in real time.

FINAL THOUGHTS

The continued growth of CVC kiosks constitutes a significant inflection point in the ongoing expansion of cryptocurrency infrastructure across the United States. As of August 2025[6], the presence of more than 39,000 kiosks introduces heightened risk exposure within traditional banking channels. Financial institutions can no longer maintain a passive posture and must proactively assess and address these emerging vulnerabilities. Financial institutions cannot afford to take a passive stance. As the Notice makes clear, strong financial controls remain our most effective tool to disrupt fraud, protect vulnerable consumers, and reduce exposure to criminal liability.

If you'd like to discuss how these developments may impact your organization, feel free to contact Trina L. Glass.
Trina *is a seasoned securities attorney at BurgherGray LLP, focusing on regulatory compliance, cybersecurity, and privacy law. She advises financial institutions, fintech firms, and investment advisers on matters related to AML, securities regulation, and digital asset compliance.*

6 See Coin ATM Radar.

BURGHERGRAY LLP
ATTORNEYS AT LAW

www.burghergray.com

1350 Broadway | Suite 1510
New York, NY 10018
T: 646.513.3231 | F: 646.561.9866
info@burghergray.com