Crypto: Identifying Suspicious Behavior

Overview

In light of events in 2022, cryptoassets have been in the spotlight regarding major collapses, hacks, and fraud. ACAMS has been monitoring each case and has identified some common typologies and red flags. These typologies demonstrate the crossovers and similarities between traditional money laundering through financial institutions and the crypto ecosystem.

Suspicious Behavior

To further understand suspicious activity related to the laundering of cryptoassets, these behaviors should be monitored during investigations:

"Create your own" token scheme

Use of bank accounts for an on and off ramp to fiat

Use of crypto ATMs, specifically in a high-risk jurisdiction

Co-mingling of funds with a potentially connected company

Multi-customer cross wallet activity

Layering of funds through the potential use of a peel chain technique

Use of money mules

Quick transaction movement

Use of a non-compliant exchange

Red Flags

- Customer is using an exchange that only requires basic information, such as an email and password
- Exchange specifically advertises cash for crypto services
- Discussion forums on the dark web reference the exchange the customer is using
- Exchange is located in a high-risk jurisdiction with no compliance (KYC/AML) policies in place
- Multiple customers sending transfers to a common account(s) with no apparent purpose
- Cryptoasset ATMs are listed at a physical address, with further OSINT data indicating it may be a front company
- Multiple crypto wallets send funds via ATMs to a single recipient over a short period of time
- A customer receives newly issued tokens and immediately wishes to exchange a large volume, unconcerned with fees and/or losses

Considerations for Compliance Professionals

Consider your direct, indirect, and customer exposure to cryptoassets and adjust your risk appetite accordingly. Where appropriate, deploy a cryptoasset analytic solution to mitigate risk as part of a anti-financial crime control framework.

Evaluate transaction monitoring programs to ensure the red flags identified would be identified within the institution's systems.

Several red flags show crossovers between cryptoasset providers and conventional financial sector activity. Compliance professionals focused on cryptoassets should evaluate which red flags overlap with their risk mitigation controls.

It is requisite on the cryptoasset sector to understand its broader exposure to predicate criminality, including money laundering, fraud, corruption, market abuse, and wider thematic issues. Professionals in this space can learn from the evolving threat landscape and volume of analysis issued by regulators, law enforcement, and thought leaders in the field.

ACAMS will continue to monitor crypto financial crime trends and typologies. Visit the **ACAMS Insights Hub** to find more of our publications covering cryptoassets and financial crime.

Red flags derived from the 2022 Elliptic Typologies Report

V30012023