Joint Chiefs of Global Tax Enforcement

Crypto Assets Risk Indicators for Financial Institutions

Introduction:

The Joint Chiefs of Global Tax Enforcement (J5) would like to bring attention to crypto assets risk indicators that may be indicative of money laundering, cybercrime, tax evasion, and other illicit activities.

The J5, a collaborative partnership among tax authorities and law enforcement from five countries, has identified several risk indicators that financial institutions should be aware of. Risk indicators play a pivotal role in enhancing the ability of financial institutions to detect and report money laundering and illicit activities involving crypto assets. To counteract these risks, timely identification allows institutions to intervene and to report to the relevant authorities contributing to the overall integrity of the financial system and ensure compliance with anti-money laundering (AML) regulations.

Detecting signs of money laundering and tax evasion requires the gathering, analysis and reporting of financial data. By disseminating the risk indicators to the financial institutions, valuable insights from law enforcement can be relayed to the financial sector and reporting agencies. This exchange enhances the abilities of reporting entities to detect and report suspicious activity necessary to disrupt illicit financial flows. While risk indicators may vary and not all are covered, the details in this advisory note are commonly observed.

Identifying Crypto Asset Layering

The following risk indicators involve transactions that are designed to conceal the illicit origin of funds, posing a major risk to the financial sector. Financial institutions should prioritize the detection of layering involving crypto assets, the phase in money laundering where transactions are intentionally made intricate to conceal illicit origin of funds, throughout their relationship with their customers. For example, unusually high volumes with rapid movement of funds between digital wallets, especially across multiple jurisdictions can signal potential layering.

To counteract these risks, financial institutions are advised to reference the following risk indicators and behaviors on evolving money laundering techniques.

- Rapid movement of funds between accounts held at crypto exchanges without apparent business rationale.
- The customer is sending or receiving in volumes inconsistent and larger than expected from private wallet addresses.
- Conversion across different crypto assets exploiting the wide range of digital assets to complicate the tracing of funds.
- The customer is sending/receiving in high volumes from peer-to-peer (P2P) platforms which enables a direct transfer between parties but bypasses traditional financial institutions.
- The customer is sending/receiving from crypto mixers.
- The customer is sending/receiving from gambling platforms.
- A disproportionate amount of the customer's account activity involves the buying and selling of privacy coins or maintains a large portfolio of privacy coins. These crypto assets are designed for enhanced privacy and are commonly employed to conceal transaction details and the identities of the parties involved.

- The customer is sending/receiving cryptocurrency from darknet marketplaces, fraud shops, or high-risk exchanges.
- High volume and frequency of transfers between different types of crypto assets.
- The customer is transacting in round dollar and/or structured amounts to avoid bank reporting requirements.
- The customer's cryptocurrency transactions flow through several intermediate addresses in a very short period of time prior to being added to a client's wallet, or just after being withdrawn.
- The customer transfers Bitcoin in large volumes in exchange for privacy coins.

Geographical Risk Indicators

FIUs need to exercise vigilance when dealing with cryptocurrency transactions tied to jurisdictions known for weak regulatory frameworks, inadequate AML controls, or heightened levels of corruption. The following geographical risk indicators may indicate that there is sending and receiving exposure between high-risk exchanges that lack in customer identity verification measures, transactional due diligence, and legal/regulatory compliance measures, or may be in offshore jurisdictions with a history of tax havens and banking secrecy, or foreign countries known for public corruption.

- Transactions involving exchanges operating out of high-risk jurisdictions identified as non-cooperative for AML purposes.
- Changing IP addresses, which also change telephone providers. This could indicate identity concealment through technology.
- Customer accounts being accessed with IP addresses from high risk-jurisdictions. The shared use of an account or access login from devices tracked to IP addresses in high-risk jurisdictions may indicate that the account is part of a larger network of accounts.
- Crypto addresses that match addresses on recognized watch lists such as the list of the Office of Foreign Assets - Control (OFAC) or law enforcement information.

High Risk Counterparties

Customer counterparties and transaction beneficiaries and senders can serve as significant risk indicators for potential money laundering and illicit activities in the realm of crypto assets. Unusual counterparties, particularly if they involve high-risk entities with obscure ownership structures may warrant closer scrutiny. Moreover, transactions where the beneficiary and sender information is obscured or has multiple layers of intermediaries may be indicative of attempts to conceal the true source or destination of funds. Financial institutions and crypto exchanges should closely monitor their customer's transactions and parties they engage with in the cryptocurrency space.

- The client's crypto assets originated from an over-the-counter trade broker that advertises its services as privacy-oriented/anonymous.
- Direct sending and receiving from high-risk crypto exchanges which operate in jurisdictions with inadequate AML and regulatory framework.
- Funds or crypto currencies that are added or withdrawn from crypto addresses or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (for example, ransomware) and/or theft reports.
- Interaction with financial institutions or individuals subject to sanctions or based in sanctioned states.

New Client Onboarding Risk Indicators

Robust know your customer (KYC) practices enable crypto asset exchanges to identify potential risks associated with crypto asset transactions and ensure compliance with regulatory measures to strengthen the integrity of the financial system. By collecting and maintaining a comprehensive customer profile, financial institutions and crypto exchanges can verify source of crypto assets and transaction history to better establish a baseline understanding of their clients' crypto exposure and activities.

- Customer attempts to provide as little identity information as possible, including incomplete or insufficient identification information.
- Company beneficial ownership is difficult to establish.
- Customer is difficult to contact, responds only via email or web chat, and at unusual hours.
- The level or volume of transactional activity is inconsistent with the client's apparent financial profile, their usual pattern of activities, occupational information, or declared business information.
- Clients who register with the exchange within a short period using a shared address, mobile device, phone number, IP addresses and other common identity indicators.
- The customer's use of an anonymity-oriented email provider.
- A customer's crypto address appears on public forums related to illegal activities.
- Carrying out transactions with crypto addresses that are connected to public investigations.
- The customer has access to multiple accounts used to purchase crypto. The account set-up access can also be done as an authorized representative or if the customer carries out the transactions himself.
- The client provides an anonymous email address obtained through an encrypted email service.
- Multiple changes to an account's contact information that could indicate a customer account takeover.
- Account set up where the client has access to multiple bank accounts and/or other people's accounts may indicate money mule activity.
- The customer's email address used in the transaction is linked to advertisements for the sale of crypto assets on P2P exchange platforms. These advertisements may suggest that the client is buying and selling crypto assets on a commercial scale through a business as a non-registered money services business.
- An account number in a country other than the customer's nationality/residential address. This could indicate that the customer is hiding who the true owner of the account is.
- The client is unwilling or unable to provide supporting information about the source of crypto assets or the reasoning behind holding privacy coins.

Ransomware and Cybercriminal Risk Indicators

Crypto exchanges have an important role to detect and report financial flows related to ransomware and stop ransomware payments, because they are a key point where criminals interact with the legitimate financial system. Cybercriminals use many methods to try and conceal the origin and destination of ransomware payments before the digital currency arrives at the final wallet or bank account under their control. Cybercriminals will use sophisticated methods to try and obscure their flow of funds. These risk indicators are to assist financial institutions in identifying potential bad actors or accounts associated with organizations that perpetrate ransomware and cybercrime.

- The customer's unusual high usage of privacy coins. Privacy coins are digital currencies that provide enhanced anonymity by obscuring the amount, destination, and origin of transactions.
- The customer's transactions exhibit chain-hopping. This is where one digital currency is exchanged for another. The digital currency is moved from one blockchain to another, hence the term 'chain-hopping'.
- The account and customer transact with a mixer. Cybercriminals direct ransomware payments through intermediary digital currency addresses, exchanges, and mixers. Mixers increase anonymity by mixing the customer's digital currency with the transactions of others before being redirected back to the customer.
- Use of mule accounts. A mule account is created using a stolen or fake identity or, a legitimate account held by another party who is complicit in its use.
- Following an initial large digital currency transfer, a customer has little or no further digital currency activity.
- Customer's digital currency account is linked to or funded by multiple bank accounts at several different institutions.
- A newly on-boarded customer wants to make an immediate and large purchase of digital currency, followed by an immediate withdrawal to an external digital currency address.

Final Remarks

The J5 has listed these crucial red-flags risk indicators indicative of money laundering, sanctions evasion, cybercrime, tax evasion, and other illicit activities within the realm of crypto assets. These indicators serve as tools for financial institutions where they can proactively detect and respond to financial crimes.

Observing one of these indicators may not suggest illegal activity on its own. However, if one sees a combination of indicators or observe other activity that raises suspicion, please include the term "J5-Cyber" in the financial reporting.

As the financial landscape continues to evolve, the partnership among the J5 countries in developing and sharing these indicators underscores the collective commitment to mitigating the risks associated with crypto assets related cybercrime, money laundering, and tax evasion.

Sincerely,

[Joint Chiefs of Global Tax Enforcement]

Contact – J5Cyber@ci.irs.gov or jmlit.mailbox@hmrc.gov.uk