2025

MEKONG CLUB

RECOMMENDATIONS FOR CRYPTOCURRENCY COMPANIES TO AVOID EXPLOITATION BY ONLINE SCAM OPERATIONS

The Mekong Club | September 2025

2025

RECOMMENDATIONS FOR CRYPTOCURRENCY COMPANIES TO AVOID EXPLOITATION BY ONLINE SCAM OPERATIONS

Author: Balki Aydin
Editor: Sebastián Arévalo Sánchez

This publication was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the author[s] and do not necessarily reflect those of the United States Department of State.

RECOMMENDATIONS FOR CRYPTOCURRENCY COMPANIES TO AVOID EXPLOITATION BY ONLINE SCAM OPERATIONS

An online scam operation is an organized scheme, often run by criminal networks, that uses deceptive tactics to carry out fraudulent activities such as online scams, phishing, or investment fraud. These highly coordinated operations lure vulnerable individuals with false promises of legitimate employment and instead force them into situations of human trafficking where they engage in fraudulent investment and romance schemes. According to the U.S. Institute of Peace, the funds stolen by these criminal networks in Southeast Asia through the scamming industry exceeds an estimated $43.8 billion annually, exploiting both trafficked individuals and unsuspecting victims of scams.

Detection of suspicious financial activities linked to online scam operations require heightened vigilance and a sophisticated understanding of money laundering techniques.

The following recommendations can help strengthen the detection and prevention of scam-related activities within the cryptocurrency ecosystem:

01 Enhance Customer Due Diligence (CDD) and Know Your Customer (KYC) Measures

Require all new users to complete a thorough KYC process before accessing services:

- Collect government-issued ID (e.g., passport, driver's license), and biometric data (e.g., facial recognition or liveness checks) to verify identity.
- Use tools for automated ID verification and document authentication.

- Screen against global sanctions lists (e.g., OFAC, UN), watchlists, and politically exposed persons (PEPs).
- Reject or flag applications with inconsistencies—e.g., IP addresses from high-risk jurisdictions (like those on the FATF grey list) mismatching stated residency.
- Identify ultimate beneficial owners.
- Leverage compliance screening databases like Dow Jones Risk & Compliance or Refinitiv World-Check to cross-reference customer data against adverse media and scam-related databases.
- Conduct KYC and CDD on users operating under pseudonyms (e.g., anonymous usernames or wallet addresses), as online scam operations often exploit pseudonymity to conceal their identities while laundering funds.
- Monitor for rapid account creation, particularly when multiple accounts are registered in quick succession from the same IP address or device.

Conduct periodic KYC reviews and risk assessments to identify anomalies and changes in customer behavior.

Strengthen onboarding procedures for customers in high-risk jurisdictions.

These jurisdictions may not necessarily be high-risk for traditional banking transactions but can serve as hubs for cryptocurrency scam operations due to factors like corruption, weak enforcement of financial regulations, limited law enforcement capacity and government oversight, or the presence of organized crime networks exploiting decentralized technologies. Below is a list of some of the jurisdictions often associated with elevated risks for cryptocurrency scam activities, based on patterns observed in recent news, expert analyses, and trends in cryptocurrency crime:

- Cambodia has emerged as a notable hub for crypto-related scam operations, particularly relationship investment

scams, where victims are lured into fake investment schemes via romantic or social engineering tactics.

- Myanmar political instability and lack of regulatory control, especially in border regions like the Golden Triangle, have made it a hotspot for scam centers.
- Laos has been implicated in hosting scam operations, particularly in the Golden Triangle Special Economic Zone, a semi-autonomous area along the Laos–Myanmar–Thailand border known for lax oversight and a history of illicit activities.
- North Korea uses cryptocurrency scams, hacks, and thefts to fund illicit programs. Its isolation from global financial systems makes it a unique high-risk jurisdiction for crypto-related crime.
- Nigeria has a robust crypto adoption rate but also a reputation for scams, including advance-fee frauds that have adapted to cryptocurrency.
- Philippines has seen a rise in crypto scam operations, often linked to illicit operations that previously operated under the guise of Philippine offshore gaming operators (POGOs) before a national ban in 2024 and despite the ban, illegal POGO-like activities reportedly continue to operate underground.
- Russia is frequently cited for hosting cryptocurrency exchanges and services involved in illicit activities, such as money laundering and ransomware payments.

Enhance customer onboarding protocols for industries that may not traditionally be considered high-risk but are particularly vulnerable to scams.

High-risk industries susceptible to online scam operations via crypto scams are those that inherently involve significant financial transactions, trust-based interactions, or vulnerabilities that scammers can exploit using cryptocurrency's pseudo-anonymity and irreversibility.

- ### Online Gaming and Gambling

  Crypto-based gaming and gambling sites often operate in regulatory grey zones, making them susceptible to scams like rigged games, fake token offerings, or exit scams where operators disappear with funds.

- ### Online Investment Platforms

  These platforms are frequently used for Ponzi schemes and fraudulent crypto trading. Fraudulent wealth management services lure victims with promises of guaranteed returns. Scam centers often target this sector due to its high-profit potential.

- ### Social Media and Influencer Marketing

  Scammers exploit influencers or fake accounts to promote fraudulent Initial Coin Offerings (ICOs), tokens, or giveaways. Relationship investment scams often start with social media outreach.

- ### Call Centers and Tech Support

  Scammers pose as tech support or customer service agents contact victims, often claiming issues with crypto wallets, exchanges, or devices, tricking them into sending funds or revealing private keys. These operations may use cold calls, pop-up ads, or spoofed numbers to appear legitimate. The technical complexity of crypto intimidates many users, making them reliant on "support" and prone to trusting fraudulent outreach. Irreversible crypto transactions amplify losses from these scams.

- ### Charity and Crowdfunding

  Fake charities or crowdfunding campaigns solicit crypto donations for nonexistent causes, exploiting donors' goodwill. Scammers often mimic legitimate platforms. Emotional appeals and the difficulty of tracing crypto donations make this sector ripe for abuse.

- Adult Entertainment

  Scammers exploit adult entertainment services through blackmail schemes and fraudulent subscription platforms. The stigma associated with these services often discourage victims from reporting the fraud. As a result, these platforms have become attractive targets for financial exploitation and abuse.

02 Strengthen Blockchain Analytics and Strengthen Transaction Monitoring

Cryptocurrency companies are prime targets for scammers who exploit digital assets to launder illicit funds and bypass traditional financial controls. Strengthening transaction monitoring with advanced blockchain analytics is crucial to detecting suspicious activities, such as layering, rapid fund movements, and connections to illicit entities. By leveraging AI-driven tools, behavioral analytics, and real-time monitoring, cryptocurrency companies can identify fraudulent patterns, flag high-risk transactions, and enhance compliance with regulatory expectations. A proactive approach to monitoring transactions will help mitigate risks and protect the integrity of the crypto ecosystem.

Utilize AI-driven tools to detect anomalies and patterns linked to scam centers, improving proactive risk mitigation. Examples of the scam detection and prevention vendors are as follows:

- IBM Corporation provides IBM Safer Payments, which leverages AI and cognitive computing to profile entity behaviors and detect anomalies in payment streams, adaptable for cryptocurrency transactions with integration into broader financial ecosystems.
- SAS Institute offers SAS Fraud Management, a real-time platform using predictive analytics to spot fraud patterns, including layering, across large datasets, making it suitable for cryptocurrency exchanges handling high transaction volumes.

- NICE Actimize delivers its Fraud & Authentication Management suite, powered by AI and machine learning, which can be tailored to monitor crypto transactions for suspicious behaviors and prevent fraud with real-time alerts, enhancing detection of scam-related activities. including layering, across large datasets, making it suitable for cryptocurrency exchanges handling high transaction volumes.
- LexisNexis provides Bridger Insight and ThreatMetrix, which combine identity verification with transaction risk scoring, helping crypto firms detect synthetic identities and layered fund movements tied to scams.
- FICO offers the Falcon Platform, renowned for its AI-driven fraud detection, which can analyze cryptocurrency payment streams to identify anomalies and layering attempts with over 100 patented models.

Set tailored red flags for scam-related activities, such as:

- Large and frequent cryptocurrency transactions without a clear economic purpose.
- Transfers to privacy services (e.g., Tornado Cash), often used to launder proceeds from phishing or ransomware scams.
- Transactions tied to known darknet addresses, indicating potential scam center involvement in illicit sales.
- Frequent small transactions to mixers (which suggest layering—a common scam tactic).
- Rapid multi-hop transactions, where funds move through within 24 hours, indicate a layering tactic used to obscure the origins of scam-related funds.
- High volume, low-value transactions to mixers or unverified wallets, a layering method to fragment scam proceeds.

- Wallet activity linked to known scam addresses (e.g., phishing campaigns, fake exchanges), hidden by pseudonymity.
- Unusual activity surges, (e.g., 50+ transactions per day from a previously dormant pseudonymous account).
- Utilization of privacy coins (e.g., Monero, ZCash) followed by conversion into mainstream cryptocurrencies like Bitcoin or Ethereum, suggesting attempts to obscure transaction origins.

Use behavioral analytics to detect scam-related laundering patterns. For example:

- Large and frequent cryptocurrency transactions without a clear economic purpose.
- Frequent transfers from bank accounts to convert into cryptocurrency
- Unusual peer-to-peer transactions with inconsistent justifications might be indicators of romance scams.
- Transfers to known scam-associated wallets or Ponzi scheme addresses, repeated small transactions followed by large lump sum withdrawals, or deposits followed by rapid fund transfers to high-risk jurisdictions might be indicators of investment scams.

Conduct network analysis to uncover links between accounts suspected of being part of scam operations (e.g., money mule accounts that are often used to wash funds through).

Monitor transactions involving cryptocurrency exchanges with weak AML controls.

Leverage blockchain forensic tools to detect and prevent fraudulent transactions.

Advanced forensic tools can bolster the defenses of cryptocurrency companies against exploitation by scam centers by monitoring and analyzing transaction flows on blockchain networks and enabling them to identify suspicious activities such as the movement of illicit funds and sophisticated money laundering techniques. These tools provide real-time tracking, transaction visualization, and risk assessment capabilities to uncover such patterns. Some of the examples for blockchain forensics tools are as follows:

- Chainalysis offers a suite of solutions like Chainalysis Reactor, which allows companies to trace the flow of funds across blockchain networks, attribute wallet addresses to real-world entities through clustering techniques, and detect layering by analyzing multi-hop transactions.
- Elliptic provides real-time monitoring and risk-scoring features, helping businesses identify connections to high-risk entities (e.g., darknet markets or scam addresses) and visualize fund flows to spot layering attempts.
- CipherTrace, excels in cross-chain analysis and compliance, enabling companies to track funds as they move between blockchains (e.g., Bitcoin to Ethereum) and detect anomalies indicative of layering or illicit activity. By integrating these tools into their compliance and security frameworks, cryptocurrency companies can proactively identify and block transactions linked to scam centers, ensuring they remain ahead of evolving laundering tactics.

03 Improve Cybersecurity Measures

- Implement stronger security protocols, multi-factor authentication, and protection against phishing, malware, and hacking attempts linked to scam centers.
- Provide cybersecurity training for employees to recognize and report potential scams.
- Flag and terminate sessions originating from high-risk IPs (e.g., VPNs in Southeast Asia) or showing signs of automation (e.g., bot-driven logins).
- Deploy AI-driven email and SMS filters to block phishing attempts that trick customers into revealing bank credentials, a common tactic in relationship investment scams.

04 Collaboration & Intelligence Sharing

- Report suspicious activities to financial crime units and relevant authorities promptly.
- Participate in public-private partnerships to combat evolving scam methodologies.
- Enhance collaboration between law enforcement, financial intelligence units (FIUs), and cryptocurrency exchanges to trace illicit fund flows and dismantle organized networks.

- Work closely with policymakers to establish clearer guidelines on cryptocurrency-related scams and enforce stricter compliance requirements for unregulated exchanges.
- Collaborate with cybersecurity experts to share threat intelligence and best practices.
- Distribute detailed reports on evolving scam methods (e.g., synthetic identity creation, social engineering scripts) with peers, based on internal incidents or customer complaints.

05  Training and Awareness: Empowering Staff and Customers to Prevent Scams

Educating both employees and customers is a crucial component of preventing cryptocurrency related fraud and exploitation. To effectively combat these risks, it is essential to implement targeted training programs that equip employees with the skills to detect suspicious activities and empower customers with the knowledge to recognize and avoid scams.

Employee Training

Frontline employees, including customer support and compliance teams, must be equipped with the knowledge to identify potential threats and guide users in safeguarding their assets. Examples include:

- Establish clear procedures to handle customer reports of fraud for assisting customers who suspect they are being targeted by scammers.
- Implement scenario-based training to help staff recognize red flags, suspicious transaction patterns, and customer behaviors indicative of scams.

- Continuously update internal protocols to adapt to evolving fraud techniques and respond to emerging scam trends.
- Conduct regular audits of internal systems and cross-reference customer reports of suspicious activity with transaction data to detect vulnerabilities and improve scam detection measures.
- Utilize simulated exercises and case studies to strengthen employees' ability to identify and mitigate risks in real-world situations.

Customer Training

Raising awareness among customers is essential, as they are often the first targets of scammers. Providing clear educational resources —such as fraud prevention guides, warning alerts, and interactive webinars—helps users recognize phishing attempts, fraudulent investment schemes, and social engineering tactics. By fostering an informed customer base, cryptocurrency companies not only mitigate fraud-related losses but also enhance user trust and loyalty. Key education topics include:

- Phishing Attempts – Recognizing suspicious emails, messages, or fake websites designed to steal user credentials:
  - Alert customers to be cautious of unsolicited emails, social media messages, or phone calls claiming to be from your cryptocurrency provider—legitimate companies rarely initiate contact this way. Scams often promise unrealistic returns ("double your funds in 24 hours") or create urgency ("limited-time offer") to pressure victims.
  - Encourage customers to always verify communications through official channels, such as the company's verified website or support line.
- Security Best Practices – Encourage customers to enable 2FA, use hardware wallets, and verify transaction details before approving transfers.

- Educate customers on the warning signs of romance and investment scams through targeted awareness campaigns, emails, and in-app notifications. Provide clear examples of common scam tactics, such as fraudsters building emotional connections to solicit money (romance scams) or promising high, risk-free returns on cryptocurrency investments (investment scams).
- Provide guidance on how to report scams, including where to seek help if they suspect fraudulent activity.

06  Establishing Internal Goals and KPIs for Scam Prevention

Cryptocurrency companies should introduce clear internal goals and key performance indicators (KPIs) to ensure the effectiveness of security enhancements. These metrics help measure the success of fraud prevention strategies and drive continuous improvement. Key recommendations include:

- Customer Awareness Metrics – Measure engagement with scam education initiatives, such as webinar participation rates, completion of security training, or response rates to phishing simulations (e.g., emails, tutorials, in-app notifications) monthly—target 80% reach.
- Phishing Report Rate: Track the number of customer-reported phishing attempts or suspicious messages per quarter.
- Security Adoption Rate - Monitor the percentage of users enabling 2FA and using hardware wallets.
- Training Completion: Ensure all relevant employees complete scam detection training—(e.g., target 100% within 3 months, with quarterly refreshers).

- KYC Compliance Rate: Track adherence to KYC/AML checks (e.g., aim for 100% verification of new accounts within 48 hours of sign-up).
- Response Time: Monitor average time to escalate and resolve scam alerts.
- Transaction Block Rate: Measure the percentage of high-risk transactions blocked in real time.

Business Imperatives: The Financial and Strategic Benefits of Proactive Cryptocurrency Risk Management

Adopting proactive risk management strategies is not just about regulatory compliance—it's a strategic investment that enhances long-term business value. By proactively detecting fraudulent activities, cryptocurrency companies can mitigate financial losses, avoid costly legal penalties, and reduce operational risks. Strengthening security measures also fosters greater customer trust, leading to higher user retention and market credibility. Moreover, compliance with evolving regulations ensures smoother business operations and minimizes the risk of enforcement actions that could damage reputation and investor confidence. On the other hand, the cost of inaction is steep—companies that fail to address financial crime risks face regulatory scrutiny, hefty fines, and irreparable reputational damage, which could ultimately threaten their viability in an increasingly regulated industry.

Conclusion

Cryptocurrency companies play a pivotal role in dismantling scam networks, protecting vulnerable individuals, and mitigating the broader economic impact of fraudulent activities. By strengthening monitoring systems, enhancing cross-border collaboration, and fostering regulatory partnerships, they can stay ahead of evolving threats. A proactive, data- driven, and cooperative approach will fortify cryptocurrency industry against exploitation and reinforce trust and integrity within the global economy.


MEKONG
CLUB