2025

MEKONG CLUB

RECOMMENDATIONS FOR FINANCIAL INSTITUTIONS TO AVOID EXPLOITATION BY ONLINE SCAM OPERATIONS

The Mekong Club | September 2025

2025

RECOMMENDATIONS FOR FINANCIAL INSTITUTIONS 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 FINANCIAL INSTITUTIONS 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 victims of scams.

Traditional financial systems, like banks, can become victims or rather, unwitting facilitators of online scam operations. These operations have evolved into sophisticated networks that exploit both individuals and financial systems

Criminal syndicates frequently use cryptocurrencies like Bitcoin or stablecoins (e.g., Tether) to collect funds from scamming victims worldwide, leveraging the speed and pseudo-anonymity of cryptocurrencies. However, to integrate these illicit profits into the traditional financial system, scammers must convert crypto into fiat currency—often relying on banks to facilitate this process.

Detecting suspicious financial activities tied to online scam operations require increased vigilance and a sophisticated understanding of money laundering techniques.

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

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

Scammers often exploit banks with weak CDD controls to open accounts using fake identities, allowing them to bypass basic KYC checks. These fraudulent accounts serve as a bridge between crypto exchanges and the banking system, facilitating cross-border fund movements and enabling deposits into banks with weaker KYC frameworks and oversight.

To mitigate these risks, banks should take proactive measures to fortify their KYC/CDD systems and prevent becoming an unwitting conduit for illicit funds, including:

> 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. Southeast Asian scam centers rely on stolen or forged documents, which biometrics can flag.
- Use tools for automated ID verification and document authentication.
- Apply stricter scrutiny to accounts opened in or linked to high-risk jurisdictions (e.g., Myanmar, Cambodia, Laos, or border regions like Thailand's Mae Sot) and cross-reference IP addresses and phone numbers with physical locations.
- Screen against global sanctions lists (e.g., OFAC, UN), watchlists, and politically exposed persons (PEPs).
- 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.

- Screen for signs of coercion or scripting during account setup (e.g., rehearsed answers, third-party influence), as trafficking victims are often forced to open accounts.
- Prioritize CDD on accounts receiving funds from Southeast Asian countries or sending to known cash-out hotspots (e.g., ATMs near scam compounds like KK Park).

Conduct regular KYC reviews and risk assessments to identify anomalies and shifts in customer behavior. During these reviews, proactively inquire about cryptocurrency usage and flag accounts linked to unregistered exchanges. Pay close attention to inconsistencies or implausible explanations for crypto-related transactions during KYC/CDD checks.

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 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 crypto 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. Organized crime groups, often linked to human trafficking and operate scam compounds.
- 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 Philippine offshore gaming operators (POGOs) that double as fronts for fraud.
- Russia is frequently cited for hosting crypto 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 scam center exploitation regarding 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.

- Cryptocurrency Exchanges and Virtual Asset Service Providers (VASPs)

  Scam centers use crypto to collect funds from victims (e.g., relationship investment scams) and convert them to fiat via exchanges, which then deposit into bank accounts. Weakly regulated or offshore exchanges (e.g., Cambodia, Philippines) are prime laundering points.

- Online Gaming and Gambling

  These platforms provide a veneer of legitimacy for moving large sums, often accepting crypto payments that scammers use to launder money. Fake gambling sites also double as scam fronts (e.g., Scammers in Laos might funnel victim's funds through fake poker sites, then withdraw fiat to bank accounts).

- Investment and Trading Firms (Especially Crypto-Focused)

  Relationship investment scams and Ponzi schemes promise high returns on crypto or foreign exchange investments, tricking victims into transferring funds that scammers later transfer to banks (e.g., a fake trading app promoted by a Cambodian scam ring might direct victim funds to a bank account under a shell investment firm). Scam centers often target this sector due to its high-profit potential.

- Remittance and Money Transfer Services

  Scammers use these services to move money across borders quickly, often converting crypto profits into fiat via remittance firms that deposit into banks. (e.g., funds from a Thai scam call center might be remitted to a bank account in the Philippines via a crypto-funded agent).

- Real Estate and Property Development

  Large transactions in real estate provide a way to "park" scam proceeds, with crypto often converted to fiat to buy property through banks. Shell companies are used as common fronts. Source of funds for property purchases should be investigated, especially if tied to crypto conversions or Southeast Asian entities (e.g., scam profits from KK Park might fund luxury condos in Bangkok, with banks processing the fiat payments).

- Import/Export and Trade-Based Businesses

  Scammers use fake invoices or over/under-invoicing to launder money through trade payments, often involving crypto-to-fiat conversions that hit bank accounts. It is recommended that trade documentation is examined for inconsistencies (e.g., mismatched goods values) and payments to crypto exchanges or high-risk jurisdictions like border towns in Myanmar are traced.

- Charity and Crowdfunding

  Fake charities collect "donations" from scam victims or launder proceeds under humanitarian pretexts, with funds often transferred to banks after crypto conversion.

- Adult Entertainment

  Scammers exploit adult entertainment and dating 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 Transaction Monitoring

Scammers exploit both traditional financial systems and cryptocurrencies to move illicit funds, often using banks as intermediaries. To combat this, financial institutions must enhance their transaction monitoring capabilities by integrating blockchain analytics alongside traditional fraud detection methods. By leveraging AI-driven tools, behavioral analytics, and real-time monitoring, banks can identify suspicious fund flows, detect layering attempts, and uncover links to illicit entities. Strengthening these controls will help prevent banks from being unwittingly used in scams, whether through fraudulent fiat transactions or crypto-related money laundering schemes.

> 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, helping banks identify fraudulent transactions and money laundering attempts.
- SAS Institute offers SAS Fraud Management, a real-time platform using predictive analytics to spot fraud patterns, including layering, across large datasets, strengthening banks' ability to combat illicit financial activities.
- NICE Actimize delivers its Fraud & Authentication Management suite, powered by AI and machine learning, which can be tailored to monitor transactions for suspicious behaviors and prevent fraud with real-time alerts, enhancing detection of scam-related activities.
- LexisNexis provides Bridger Insight and ThreatMetrix, which combine identity verification with transaction risk scoring, helping banks detect synthetic identities, fraudulent accounts, and suspicious fund movements linked to money laundering and scams.
- FICO offers the Falcon Platform, renowned for its AI-driven fraud detection, which can analyze payment streams to identify anomalies and layering attempts with over 100 patented models.

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

- Transactions linked to scam-heavy regions (e.g., Cambodia, Laos, Myanmar) or routing through local banks with weak AML controls.
- Funds deposited from known or unregistered cryptocurrency exchanges, especially those flagged for lax KYC (e.g., past issues with Binance or Huobi in Southeast Asia).
- Vague or generic payment descriptions (e.g., “consulting,” “investment”) that don’t match the customer’s profile or history.

- Customers unable to provide clear source-of-funds details for crypto-related deposits (e.g., no wallet history or exchange records).
- Direct transfers from crypto wallets to bank accounts, followed by quick cash-outs or onward transfers.
- Large, irregular transfers from personal accounts to cryptocurrency exchanges, often paired with customer claims of "investment" without documentation (potential indicator or pig-butchering)
- High frequency- small transfers from crypto-linked sources, potentially testing AML thresholds or aggregating scam proceeds.
- Deposits tied to blockchain addresses that used mixing services (e.g., Tornado Cash) to obscure origins, detectable via analytics tools.
- Transactions heavily involving stablecoins like Tether (USDT), a favorite for Southeast Asian scammers due to its stability and liquidity.
- Elderly or inexperienced customers suddenly engaging in high-value cryptocurrency activity, a hallmark of social engineering scams.
- Rapid conversion of cryptocurrency to fiat via bank accounts, then immediate movement offshore or to cash.
- Accounts with minimal personal use (e.g., no utility payments or regular spending) but high volumes of third-party transfers.

Use behavioral analytics to differentiate legitimate transactions from potential scam-related laundering. For example:

- Large transfers to newly created accounts with no prior activity.
- Frequent transfers from bank accounts to convert into cryptocurrency.

- Unusual peer-to-peer transactions with inconsistent justifications might be indicators of romance scams.
- Customers unable to provide clear source-of-funds details for crypto-related deposits (e.g., no wallet history or exchange records).

- Conduct network analysis to uncover links between accounts suspected of being part of scam operations.

- Monitor transactions involving cryptocurrency exchanges with weak AML controls.

- Integrate machine learning models to analyze transaction metadata (e.g., timing, recipient, device) and flag crypto-related transfers matching scam profiles (e.g., rapid movement to exchanges).

- 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.

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.

Partner with cryptocurrency exchanges for data sharing to flag accounts or transactions linked to scam-related crypto wallets before fiat hits bank accounts.

- Collaborate with cryptocurrency exchanges on KYC alignment, ensuring exchanges report suspicious withdrawals (e.g., large USDT cash-outs) that may flow into banking systems.
- Work closely with policymakers to establish clearer guidelines on crypto-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.
- Update the industry on crypto-specific red flags, like stablecoin-heavy transactions or mixer use, observed in scam-to-bank pipelines.

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

Educating both employees and customers is a crucial component of preventing fraud and exploitation by scammers. 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 fraud 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. 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 crypto 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

Financial institutions should introduce clear internal goals and key performance indicators (KPIs) to ensure the effectiveness of security enhancements. These metrics help measure the success of scam 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.
- 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, financial institutions 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

Financial institutions 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 financial systems against exploitation and reinforce trust and integrity within the global economy.

MEKONG
CLUB