TRM GUIDE

Part I

Wires to Wallets: Understanding and Investigating Wire Exposure to Crypto

CRYPTO COMPLIANCE PROGRAM GUIDE
FOR FINANCIAL INSTITUTIONS

TRMLABS.COM

In the fall of 2022, the US Secret Service (USSS) began an undercover investigative operation to disrupt an international money laundering syndicate. The syndicate was operating a particular type of virtual currency investment scam[1] that is oftentimes thought to take place solely within the crypto ecosystem. However, the reality is that these scams are often more nuanced.

In the course of the USSS's operation, an undercover agent began communicating with a fake customer service department run by the perpetrators. Syndicate operatives directed the agent to wire funds to an account in the name of a shell company called, "Sea Dragon Remodel Inc,"[2] at a US banking institution. In the course of their investigation, law enforcement ended up uncovering over 60 shell accounts like this account — held at various banking institutions that were being used to launder the scam proceeds — and identified over 150 victims who had lost money to just this one criminal syndicate. The USSS also uncovered other fund transfers that were part of the scheme and were affected through cryptocurrency accounts.

Two truths emerge upon examining this and dozens of similar law enforcement cases like it.

First, criminals don't exclusively use one type of asset to carry out a scheme and launder funds. The "Sea Dragon Case" involved not only the use of wire transfers and crypto, but checks and credit cards, too. Ultimately, criminals will use any and all financial instruments available to them to exploit our financial systems. **This multi-asset laundering approach necessitates a multi-asset compliance defense.**

Second, since the early days of Bitcoin, there has been an indirect relationship between traditional financial institutions (FIs) and crypto. For FIs, that point of connectivity often arises through wire transfers to or from crypto-linked entities. The crypto nexus via wire transfers may stem from any number of sources, such as customers:

- Wiring funds to exchanges
- Wiring funds to accounts held for custodians or stablecoin issuers
- Purchasing hardware for crypto mining equipment
- Transferring money to asset management firms investing in blockchain technology platforms or crypto assets

[1] This type of scam has been referred to in the industry as "pig butchering," yet this terminology focuses on the exploitative process of these particular scams rather than the critical need to safeguard victims and educate financial institutions about prevention. FinCEN refers to these scams as virtual currency investment scams (https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf).

[2] https://storage.courtlistener.com/recap/gov.uscourts.vaed.539729/gov.uscourts.vaed.539729.1.1.pdf, and https://coingeek.com/us-seizes-45-million-in-fraud-proceeds-from-tether-ftx-bank-deltec/

It's important to keep in mind that from a risk tolerance perspective, not all wires with crypto-linked entities are part of illicit schemes. Bitcoin is currently on a meteoric rise, pricing close to USD 100,000[3] at the time of this writing — and investors are taking note. In addition to growing institutional adoption, a recent Pew Research Center survey found that 17% of US adults (approximately 58 million people) had invested in or used cryptocurrency. Among men aged 18 to 29, this figure was notably higher, exceeding 40%.

Such significant activity doesn't happen without wire transfers. Banks will be increasingly linked to crypto, and wire transfers have long been the primary nexus point between the two. Moreover, banks that have historically derisked and blocked customer transactions with these entities will find it increasingly difficult to continue on that path as both retail and institutional involvement expand.

The duality facing banks and their compliance teams is clear: **What do we do about wire transfers with crypto-linked entities?** How should we balance the risks that dominate the headlines and are inherent to that space, while simultaneously managing growing interest from both Main Street and Wall Street? The question for banks is no longer if they should scrutinize these transactions but how.

Understanding crypto-linked entity activity

When learning about crypto and digital assets, one of the most important lessons is that this technology and its applications are not monolithic.

"Crypto" is not a single entity or activity — and it is far from uniform. Bitcoin is not the same as USDC. And NYDFS registered exchanges are not the same as overseas OTC services. In recent TRM Talks episodes, thought leaders from Standard Chartered, Fidelity, and Citi have all spoken not only about the dynamic nature of this ecosystem, but how financial institutions are building within that ecosystem.

The same applies with wire transfers involving crypto-linked entities. This sprawling ecosystem includes many types of entities, applications, and varied business purposes for the underlying wire transfers — many of which go beyond mere speculative trading.

Mainstream news headlines often focus on activity that takes place with crypto exchanges (e.g. Coinbase, Binance, FTX, etc.) , but there are many other types of

[3] https://www.wsj.com/livecoverage/stock-market-today-dow-sp500-nasdaq-live-11-25-2024/card/bitcoin-prices-aren-t-far-off-100-000-here-s-the-recent-runup-in-perspective--7t15tI5F5fOokCUzOUM0

entities and activities – a fact that was also noted by the Wolfsberg Group in their recent digital asset FAQs. These include:

- Over the Counter (OTC) services for institutional investors that serve as digital asset market makers
- Venture capital and other private investment activity funding digital asset startups
- Subscription and/or redemption activity from digital asset Exchange-Traded Funds (ETFs) and/or Exchange-Traded Products (ETPs)
- Blockchain technology computing equipment use for mining or staking services

Customers may use these and other crypto-linked entities and wire transfers for various legitimate purposes, such as:

- **Investment:** Seeking exposure to digital assets as part of a diversified portfolio
- **Trading:** Accessing crypto markets for short-term speculation or arbitrage
- **Payments:** Using dollar-backed stablecoins to facilitate remittances or corporate financial needs
- **Inflation hedge:** Converting fiat into digital currencies like stablecoins to preserve value in uncertain economic conditions
- **Private funding:** Using cryptocurrencies for personal or business transactions, especially across borders
- **Business expansion:** Institutional clients exploring blockchain technology or integrating crypto solutions into their operations

Red flags in wire transfers with crypto-linked entities

Of course, this space is not without its share of risks. And not all wire transfers to crypto-linked entities are benign.

A recent bank enforcement action, in which FinCEN noted specific instances of large volumes of wire transfer flows to crypto-linked entities that were insufficiently

investigated, serves as a gripping reminder that these interactions cannot be ignored. Banks must remain vigilant and use a variety of controls and investigative techniques to ascertain the legitimate from the illicit, and evolve along with changing typologies.

When investigating specific wire transfers and customer activity, here are some of the primary red flags to look out for.

> Note that some of these typologies will help identify non-compliant and risky crypto-linked entities, and others will help identify higher-risk transactions with legitimate crypto-linked entities. These typologies can also be used to help configure more programmatic transaction monitoring rules to flag at scale.

Rapid multi-exchange exposure

Though different exchanges may offer different assets and spreads, multiple wires to multiple crypto exchanges within a short timeframe can be indicative of layering and splintering tactics.[4]

Unusual "For Further Credit" (FFC) instructions

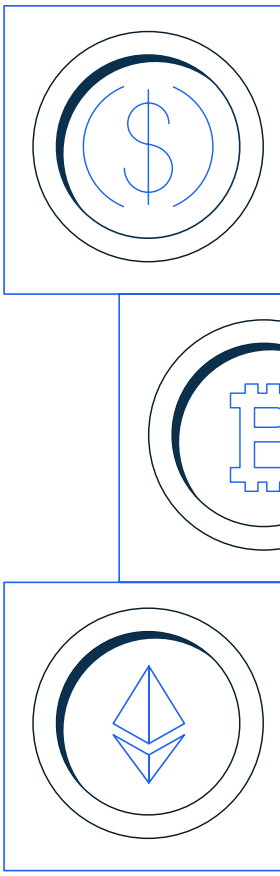
Unusual FFC instructions can indicate routing funds to unrelated or unexpected beneficiaries, potentially obscuring the ultimate recipient. This is a common tactic in money laundering schemes, including the case referenced above.

Multi-product rapid movement of funds

Rapid movement alone is often not enough to identify illicit activity. Rapid movements coupled with multiple products (e.g. check deposit followed by wire to crypto exchange) in a single account is often a sign of atypical account activity.

Increasing ramping amounts

A consistent theme heard from scam victims is that they transact with legitimate exchanges. Their investments start small, but then quickly increase over several weeks and months — eventually reaching significant sums.



[4] Layering is when multiple wires and transactions are structured to obscure the path of the funds. Splintering is when funds are divided and sent to various exchanges to fragment the total amount and reduce the visibility of any single large transaction.

Outsized exposure vs. assets under management (AUM)

Customers wiring funds to crypto-linked entities much larger than their disclosed AUM or expected activity is indicative of money laundering risks, as recently seen in the cited FinCEN enforcement action.

Inconsistent cross-jurisdictional exposure

Customers wiring funds with crypto-linked entities that have a jurisdictional profile that doesn't align with the customer's background (e.g. retail company based in US, sending wires to exchanges in multiple other jurisdictions).

Inconsistent business purposes

Business purposes that don't align with the counterparty's services (e.g. a "crypto investment" to a crypto payment processor service) indicate suspicious intentions behind the transfer.

Unregistered intermediaries

For example, FTX customers were told to wire funds to an unregistered money services business (MSB) that was not in the name of FTX, and which did not have any apparent connection to FTX. This could itself be a red flag. And even if it is a benign investment, there are still AML/CFT risks associated with transacting with a non-compliant exchange.

Conducting due diligence on crypto-linked entities

Anti-money laundering (AML) investigators may well recognize that these red flags are similar to traditional transaction monitoring red flags. Still, determining whether a single or group of wire transfers with a crypto-linked entity is legitimate requires context, nuance, customer background information, and a wider look at the account activity.

While similarities exist, the transactional red flags analysis should be coupled with conducting counterparty due diligence on the crypto-linked entity itself — as this space presents some unique risks and unique risk mitigation techniques for crypto-linked entities. Evaluating the risk profile of crypto-linked entities is an essential component of monitoring wire transfers with these entities.

Six key considerations for risk assessing crypto-linked entities involved in wire transfers

1. Where is the crypto-linked entity's jurisdictional footprint?
Determine where the crypto exchange operates, and whether it services customers or entities in high-risk jurisdictions like Russia — as threat actors (and thus suspicious wire transfers) have concentrated financial flows to these jurisdictions.

A recent report from TRM Labs found that Russian-speaking threat actors from across the former Soviet Union consistently drive most types of crypto-enabled cybercrime, from ransomware to illicit crypto exchanges and darknet markets. And from a sanctions exposure perspective, inflows to just one Russia-based crypto exchange, Garantex, accounted for 82% of crypto volumes belonging to all sanctioned entities internationally.

2. What is the crypto-linked entity's licensing and regulatory posture?
Confirm whether the entity, where relevant, holds appropriate licenses and registrations consistent with their jurisdictional footprint.

For example, ascertain whether the entity meets the US regulatory definition of a money services business (MSB) if it operates inside the US or has US customers, and if so, whether it is registered with FinCEN. Does it comply with licensing requirements in jurisdictions such as Canada (under the Financial Transactions and Reports Analysis Centre of Canada), the United Arab Emirates (via the Abu Dhabi Global Market), or the European Union (through the Markets in Crypto-Assets Regulation)?

3. What is the risk appetite of the crypto-linked entity's crypto asset offering?
Assess the range of assets and services provided by the exchange, and consider whether it supports assets that are subject to greater exploitation by bad actors and scrutiny by regulators, such as privacy coins and mixing services.

Does it have standards for onboarding new assets? A large and unvetted asset offering can signal an exchange with a higher risk appetite, as well as a lack of stringent controls (and therefore a higher likelihood of being favored by threat actors).

4. What parts of the crypto ecosystem does the crypto-linked entity service?
Analyzing the products and services a crypto-linked entity serves can provide signals about the levels of risk of any particular wire transfers with that entity.

For instance, consider crypto-linked entities that only serve institutional clients based in the US. These entities would naturally carry much less risk than one that services only retail customers from all over the world.

5. Who are the crypto-linked entity's counterparties?
Similarly, you can ascertain a great deal about a crypto-linked-linked entity by identifying who its primary counterparties are. Blockchain technology's transparency makes many of these connections visible and subject to analysis.

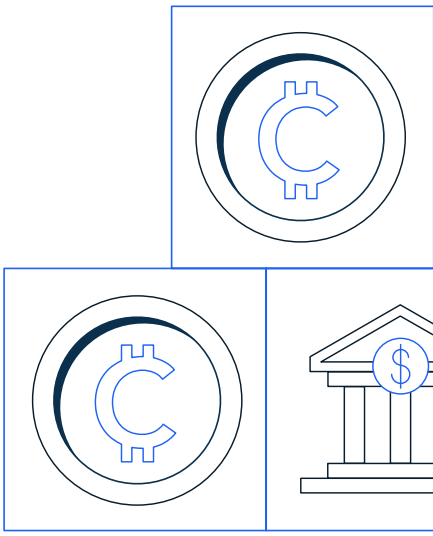
Consider, for instance, a crypto custodian whose major counterparties include high-risk exchanges, gambling shops, payment processors, retail OTC services, and other peer-to-peer services that can be more susceptible to being exploited by bad actors at scale. These connections can be a useful indicator to determine whether wire transfers with such entities might actually be problematic from a regulatory or reputational risk perspective.

6. What is the effectiveness of the crypto-linked entity's AML/CFT and KYC controls?
Strong anti-money laundering (AML) and Know Your Customer (KYC) controls are non-negotiable indicators of a crypto-linked entity's compliance maturity. But outside of reaching out to these entities, how can a compliance or risk professional get a sense of what a crypto-linked entity's internal controls are like?

Certainly the historical presumption has been that these entities operate on little to no controls. And while that may be true in select instances and countries, it may surprise traditional financial compliance officers how much their crypto compliance counterparts do to detect and prevent illicit activity. Additionally, blockchain technology provides unique ways to analyze the relative amounts of illicit risk flowing through a crypto-linked entity's pipes, which can serve as one indicator of the robustness of their AML controls.

Weak controls, such as insufficient transaction monitoring or limited KYC processes, are more likely to lead to systemic exposure to Child Sexual Abuse Material (CSAM) vendor cashouts, sanctioned exchange exposure from Iranian exchanges, or large scam networks – all issues made visible by blockchain intelligence solutions and insights.

While the data needed to assess these factors may seem daunting to obtain, blockchain intelligence tools actually aggregate each of these data points and risk factors in a single solution, enabling compliance teams to incorporate this data into their investigative and diligence processes.



A balancing act: Vigilance and openness

Global cryptocurrency adoption is at unprecedented rates, driven by a myriad of economic, regulatory, and political forces.

This adoption comes with several key benefits for developing nations – including greater financial inclusion for unbanked and underbanked populations, accelerated cross-border transactions, economic protection in countries experiencing high inflation or currency volatility, and support for vibrant tech and entrepreneurial ecosystems. Meanwhile, factors like the recent US election, fintechs like PayPal and Stripe embracing stablecoins, and traditional financial institutions like BlackRock and Fidelity offering crypto exposure are all factors that could significantly reshape and accelerate the future of cryptocurrency regulation globally.

The growing adoption of crypto-related services will inevitably increase banks' exposure to digital assets. Navigating the intersection of wires and wallets is a complex but increasingly critical task for financial institutions. Balancing vigilance with openness requires informed frameworks that can adapt to the ever-evolving financial landscape.

By leveraging robust due diligence practices, clear criteria for evaluating transactions, and cutting-edge blockchain tools, banks can confidently facilitate legitimate financial activity while mitigating risks this space presents. Collaboration between banks, regulators, and the crypto industry will be key to ensuring a safe and transparent ecosystem for the future.

About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com