TRM GUIDE

Part IV

Source of Wealth Analysis for High-net-worth Crypto Prospects

CRYPTO COMPLIANCE PROGRAM GUIDE FOR FINANCIAL INSTITUTIONS

TRMLABS.COM

For financial institutions operating under strict anti-money laundering (AML) requirements, verifying a customer's source of wealth (SoW) from cryptocurrencies demands a combination of traditional due diligence and modern blockchain intelligence. This process goes beyond standard Know Your Customer (KYC) and Customer Identification Program (CIP) checks, often requiring enhanced scrutiny of on-chain wallet activity.

This guide outlines factors that will be helpful in conducting SoW and/or source of funds (SoF) analysis. From gathering evidence of legitimate ownership and transaction histories to spotting early indicators of obfuscation techniques, we will explore how AML teams can augment their existing SoW and SoF processes using blockchain intelligence tools.

Asking the right questions and establishing the narrative

Banking customers with crypto-linked sources of wealth may fall into one of two categories:

1. Prospects whose source of wealth stems from traditional compensation or investment returns involving a crypto entity. This may be an executive of a crypto exchange, a partner who works at a venture capital firm that invests in crypto, or a founder of a blockchain-linked company.
2. Prospects whose source of wealth stems from trading, investing, or otherwise transacting more broadly with direct crypto assets on-chain.

In the first instance, presuming the prospect was paid in traditional currencies, an on-chain analysis is likely not necessary – though it may be prudent to assess the risk of the crypto entity itself.

In the second instance, before delving into detailed on-chain analysis or requesting formal documentation or wallet addresses, it's crucial to ask targeted questions upfront that clarify how the prospect accumulated their crypto-related wealth – and the means by which they may liquidate it and bring dollars to your institution. **This narrative you collect from the prospect becomes invaluable as you look to ultimately verify whether their on-chain activity is consistent with their story.** These questions may include:

- What cryptocurrencies are you liquidating?
- How did you acquire your cryptocurrencies? (e.g. mining, ICOs, trading on a licensed exchange, staking, inheritance, etc.)
- Over what time period did you accumulate these assets?
- Which platforms or exchanges have you used to trade or transact, and can you provide account statements or records if necessary?

- Do you control or utilize unhosted wallets? What specific wallet addresses do you use to conduct transactions, deposit funds at exchanges, trade in DeFi services, or make any transfers to other wallet addresses?
- Can you demonstrate that you control any private wallets holding this crypto?
- What proportion of your total net worth stems from crypto assets?
- Which crypto service are you using to liquidate your crypto assets?
- Have you reported your crypto gains for tax purposes?

Some prospects may push back on not wanting to provide this type of information. Here are some helpful tips for approaching those conversations.

- With some forms of wealth, we can validate the source through publicly available information (e.g. if someone sold a company, we may verify that through open source information). Depending on the specifics in this case, **an on-chain analysis may be the only way to actually verify the narrative we've been given.**
- **Regulatory expectations** require customers' source of wealth be verified.
- FATF guidance and some **regulatory statutes** (e.g. the US PATRIOT Act) require enhanced due diligence be conducted where there may be additional risk, and those steps often require the request of documentation.
- There is an emerging **industry standard** as many institutions already do this today.

Gathering evidence of source of wealth

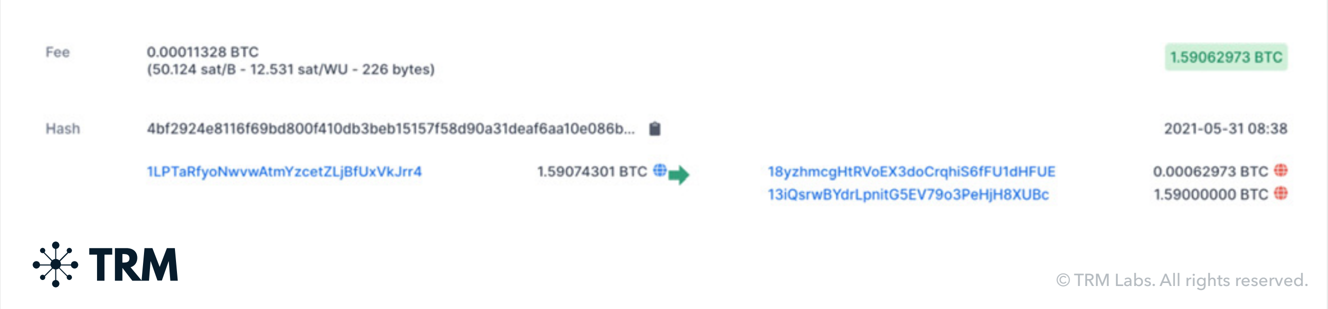
Once a narrative is collected and established, the next step is to collect verifiable evidence that supports the customer's narrative of generating wealth from cryptocurrency. **Since crypto assets and transactions often exist on public blockchains or exchange platforms, banks can leverage both traditional documentation and blockchain intelligence tools to bolster their source-of-wealth assessment.**

Note: Depending on the facts and circumstances of the narrative, not all of these data points may be necessary.

Transaction records and wallet history

On-chain evidence

Ask for wallet addresses and on-chain transaction hashes that support the relevant transfers of the activity (e.g. if a customer is liquidating funds at an exchange and maintained assets in a private wallet, ask for the transaction hash that facilitated the transfer of funds from the private wallet to the exchange).



```
Fee     0.00011328 BTC                                                                                1.59062973 BTC
        (50.124 sat/B - 12.531 sat/WU - 226 bytes)

Hash    4bf2924e8116f69bd800f410db3beb15157f58d90a31deaf6aa10e086b...                                 2021-05-31 08:38

        1LPTaRfyoNwvwAtmYzcetZLjBfUxVkJrr4     1.59074301 BTC    18yzhmcgHtRVoEX3doCrqhiS6fFU1dHFUE    0.00062973 BTC
                                                                 13iQsrwBYdrLpnitG5EV79o3PeHjH8XUBc    1.59000000 BTC
```

Example of wallet addresses and transaction hashes.

Proof of ownership

In some cases, the customer can sign a message from their wallet to prove direct control. Alternatively, screenshots of wallet balances or exchange statements can serve as supporting evidence (though screenshots alone could certainly be falsified).

Exchange or platform statements

Trade statements and funding history

Request documented statements from major exchanges where the customer trades. Look for consistency between deposits, withdrawals, fiat conversions over time, and any potential transfers to other wallet addresses.

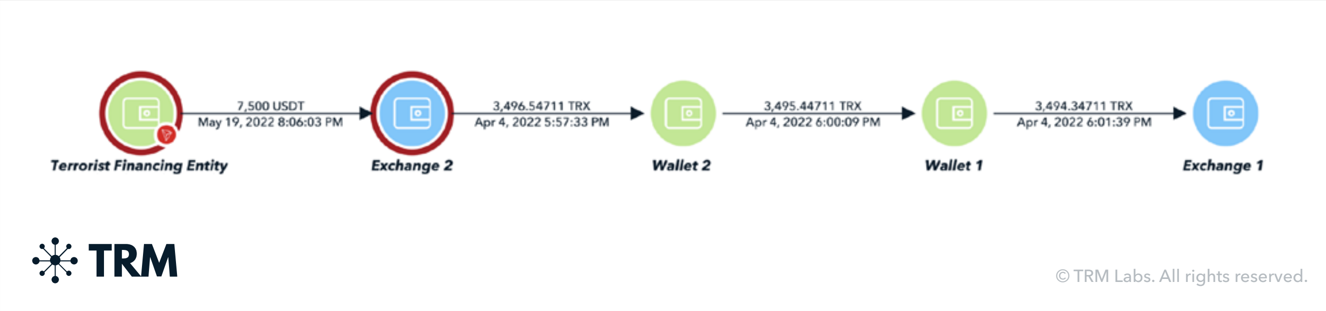
If the customer has an extensive history of many years of trading and transacting in crypto, institutions may need to ascertain where a sampling approach may be sufficient, or perhaps ask more targeted questions over specific time periods. Here, institutions should be guided by a risk-based approach and consider other risk factors related to the potential customer.

On-chain analysis

When you begin to conduct an on-chain analysis, your goal is to verify that the prospect's story about their crypto wealth matches what you see on the blockchain, and to ensure you don't see any red flags. Here are some practical tips to keep in mind:

1. Be wary of tracing through services

As you trace funds back through different addresses in the SoF analysis, recall that one of the tenants of blockchain tracing is that, generally, one **cannot trace through a service** such as an exchange, OTC desk, payment processor, etc. This stems from the fact that crypto services often use omnibus or consolidated wallet infrastructures to manage customer deposits and withdrawal efficiently. Tracing through a service will likely cause an investigator to make incorrect assumptions about the validity of a source of funds path.



Exchange 1 is conducting a source of funds review on Wallet 1, who deposited funds to the exchange. If you attempt to trace back through Wallet 2 until you hit the Terrorist Financing Entity wallet, you will have traced through an exchange.

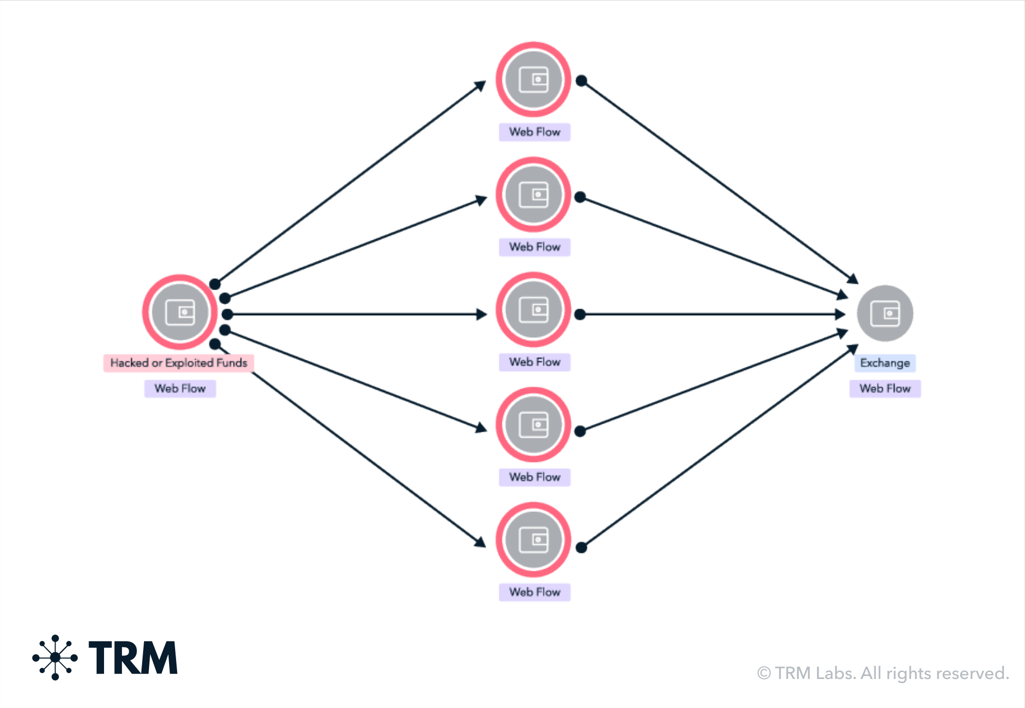
2. Explore exposure to a range of risk categories

In addition to reviewing whether the relevant wallet addresses have exposure to illicit finance risk categories (e.g. sanctions, terrorist financing, child sexual abuse material), there may be **exposure to other categories that, on their face, may not appear to be illicit – but may be inconsistent with what you would expect from the customer** based on their narrative and background. This may include things like individuals using OTC services, payment processors, gambling services, or other money transmitters that facilitate laundering services.

3. Look at all data points to assess the holistic set of risks

Keep in mind that while blockchain intelligence tools excel at mapping bad actors and services to wallet addresses, there are other data points to consider as you analyze the flow of funds – including what services are used, the number of addresses used by a prospect, the timing of transfers, the type of assets they're using, patterns indicative of sanctions evasion, etc.

To assist users with monitoring for unusual patterns of activity, TRM pioneered the automatic identification of suspicious behaviors, called Signatures®, to automatically detect and trace behavioral anomalies that are often used as obfuscation techniques. The automatic detection and plotting of these patterns reduces the complexity and time needed for investigations. These behaviors include not only peel-chains (i.e. small transactions are peeled off from the main flow of funds path and sent to other addresses or services) and cross-chain swaps (i.e. a technique used to swap one crypto asset for another without using an exchange), but other types of behaviors that are not normal and expected types of transactional activity.



This obfuscation pattern shows an address that disperses funds to many addresses, before reconsolidating the assets back to a single wallet, in order to obfuscate the risk that the original wallet may be exposed to.

Red flag indicators

Here are some additional red flags to look out for in the course of your analysis:

- Use of services in higher risk jurisdictions or offshore tax havens
- Use of privacy coins, mixers, or other services that obfuscate the flow the funds
- Inconsistent or vague explanations (e.g. "early investor" with no documentation)
- Use of intermediary or single-use addresses with no other activity
- Frequently changing wallet addresses
- Large inflows from other unhosted wallets without a clear explanation
- Large deposit and sales of token projects that experienced dramatic price decreases following a sale
- Chain hopping without clear indication of why the swap of assets took place
- Swapping of tokens or NFTs back and forth between addresses (i.e. wash trading)
- Splintering funds across multiple wallet addresses prior to a deposit at an exchange
- Structuring transfers to circumvent certain reporting requirements (e.g. VCTR, daily limits for crypto ATMs, etc.)

While it may seem daunting at first, by combining a prospect's narrative with diligent evidence gathering and careful on-chain analysis, you can build a robust source of wealth assessment process that supports regulatory requirements and protects your institution from bad actors looking to exploit it. Blockchain intelligence tools like TRM can accelerate the ability for compliance teams to conduct this kind of analysis by providing key red flag indicators and evidenced-based insights to the forefront of your team's analysis.

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