TRM

GUIDE

How Regulators Can Detect and Investigate Unregistered VASPs Using Blockchain Intelligence

trmlabs.com

As digital asset anti-money laundering (AML) regimes proliferate, regulators are focusing more than ever on the risks posed by unregistered virtual asset service providers (VASPs). This practical guide outlines methods to detect and investigate these services using blockchain intelligence tools, ultimately supporting an enforcement action against the unregistered VASP and its responsible individuals.

Regulators are generally concerned with identifying VASPs that are operating without the required license or registration in their jurisdiction, in direct contravention of local requirements. Often, these VASPs, especially those who wilfully contravene requirements, are operating without any form of licensing or registration, meaning that they are subject to little or no oversight and AML/CFT requirements, heightening their illicit finance risks.

"Unlicensed or unregistered VASPs…are vulnerable to abuse by illicit actors, and their lack of effective AML/CFT obligations complicates law enforcement efforts to address abuse..."

> *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, Financial Action Task Force, June 2023*

Defining Unregistered VASPs

Unregistered VASPs generally fall into four categories:

- **Unintentional.** Ignorance, misunderstanding, or misinterpretation of the regulations by a business regarding regulated activities they are undertaking.
- **Intentional.** Wilful rejection of registration requirements as a unique selling point, for example offering "No KYC" services.
- **Unsuccessful Application.** VASPs that applied and moved through a licensing process with a regulator, but were not successful.
- **License Revoked.** VASPs that previously operated with a license but later had it revoked.

Unregistered VASPs may operate in the open in a seemingly compliant manner, or in hiding, potentially as so-called parasite exchanges, which use the architecture and liquidity of larger, compliant services without being transparent with the compliant service about the reasons for holding accounts.

Detecting Unregistered VASPs Using Blockchain Intelligence

Here are three key ways regulators can use blockchain intelligence tools to identify unregistered VASPs that are operating in their jurisdiction:

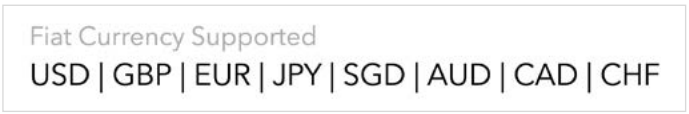
1. Review Location Data

Blockchain intelligence tools provide regulators with access to a vast database of on-chain entities, including VASPs. Many of these entity profiles are enriched with open source information, including location data, which allows regulators to identify VASPs that may be operating in their jurisdictions without the required registration.

TRM sources location data according to definitions provided in FATF guidance.

2. Review Fiat Currency Data

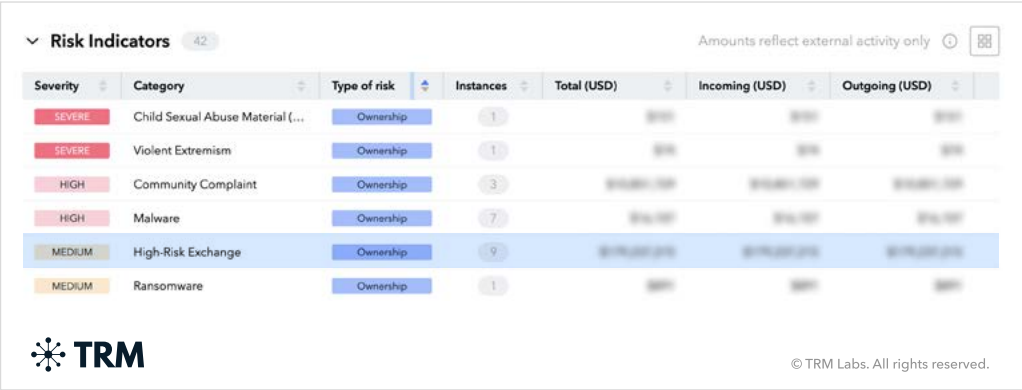
Another helpful data point to consult is the fiat currencies supported by VASPs, which provides a useful indicator of the jurisdictions a VASP serves. In some jurisdictions, this information may allow authorities to open an investigation on that VASP.



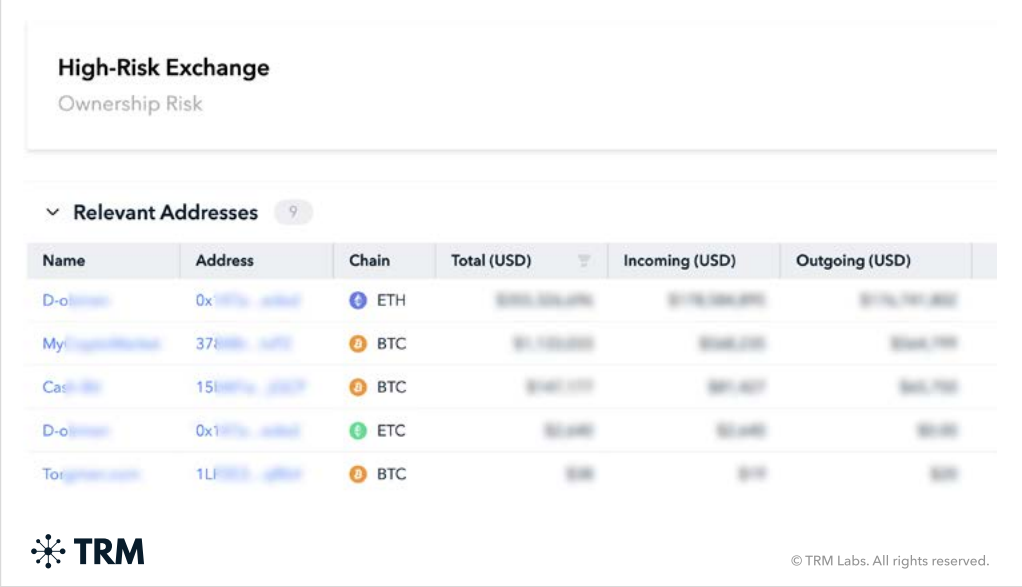
3. Identify Nested Services

Nesting refers to the practice of relying on the liquidity and architecture of another larger exchange to provide digital assets trading services to end users. In some cases, this activity reflects an intentional, legitimate commercial arrangement between two services However, there is also a subset of nested services that operate as so-called parasite exchanges.

Parasite exchanges often operate without the knowledge or consent of the host exchange and can be up to 100 times more exposed to illicit funds, according to TRM research.



In this example, when we view the list of Risk Indicators for a large, regulated, multi-jurisdictional exchange, we see that one of the risks present is High-Risk Exchange, and that the risk type is Ownership. Ownership risk indicates that the entity has addresses belonging to it that are tagged with that particular type of risk. It is distinct from Counterparty Risk or Indirect Risk, which indicate that it has transacted with an address one or more hops away that are tagged with risk. The High-Risk Exchange category as presented as Ownership risk is a key indicator that a high-risk exchange may be nested within the parent exchange.



Users can click the High-Risk Exchange risk indicator to learn more about addresses in question. Regulators can conduct further analysis on the nested service(s) to determine if the service is operating in their jurisdiction.

Case Prioritization

As potential cases are identified, regulators can review a VASP's AML/KYC controls to support case prioritization. A VASP that does not collect sufficient KYC or is facilitating a material volume of high risk activity may be a case to prioritize over one that collects substantial amounts of personal, verified information on customers. Regulators may also have access to additional information or intelligence sources that can be used to augment blockchain intelligence in identifying unregistered VASPs within their jurisdiction.

Once an investigative target is identified, a regulator can leverage on-chain data to better understand and further investigate a certain VASP.

Investigating Unregistered VASPs

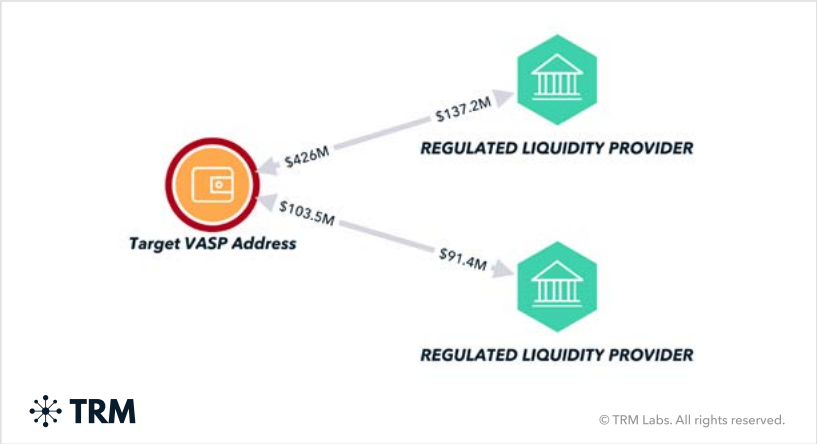
Having identified an unregistered VASP, here are three methods for conducting further investigations using blockchain intelligence tools.

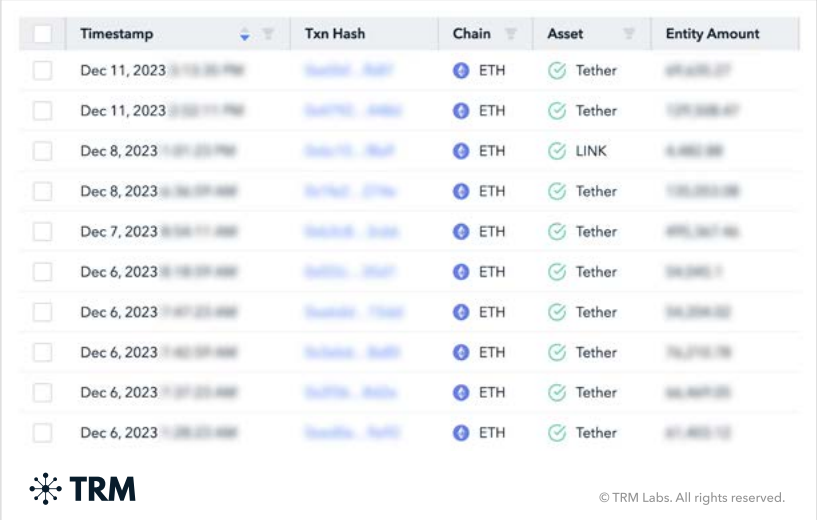
1. Identify Liquidity Providers

Many VASP business models such as exchanges, cash-to-crypto and P2P services source cryptocurrency liquidity from third parties. This allows them to offer services such as converting cryptocurrency to fiat, and vice versa.

Regulators can use blockchain intelligence to investigate where their target VASP sources its liquidity. Blockchain intelligence offers a detailed visual picture of the on-chain relationships between the VASP and third-party entities, including transaction values, frequency, and the assets being transacted.

Case Study:
A regulator identifies a cryptocurrency address suspected of belonging to an unregistered VASP in their jurisdiction. Using blockchain intelligence, the investigator identifies two licensed VASPs transacting with the address. Further analysis of transaction flows indicate potential liquidity provider relationships. This enables the regulator to request KYC information from the two VASPs, which are required to collect such due diligence as a condition of their licenses.

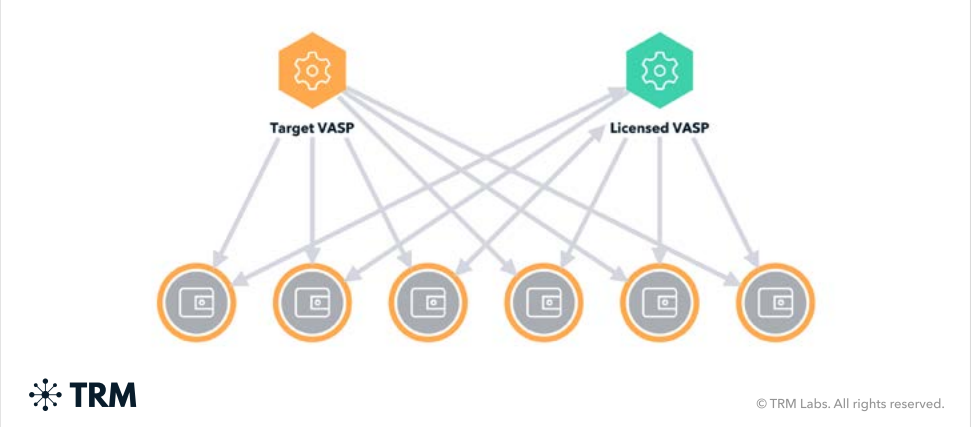




2. Third-party counterparty analysis

Customers using an unregistered VASP may use other licensed services within the same jurisdiction. Cross-referencing addresses that transact with an unregistered VASP to see if the same addresses are transacting with licensed VASPs can provide an indication of whether an unregistered VASP is servicing customers in one's jurisdiction.

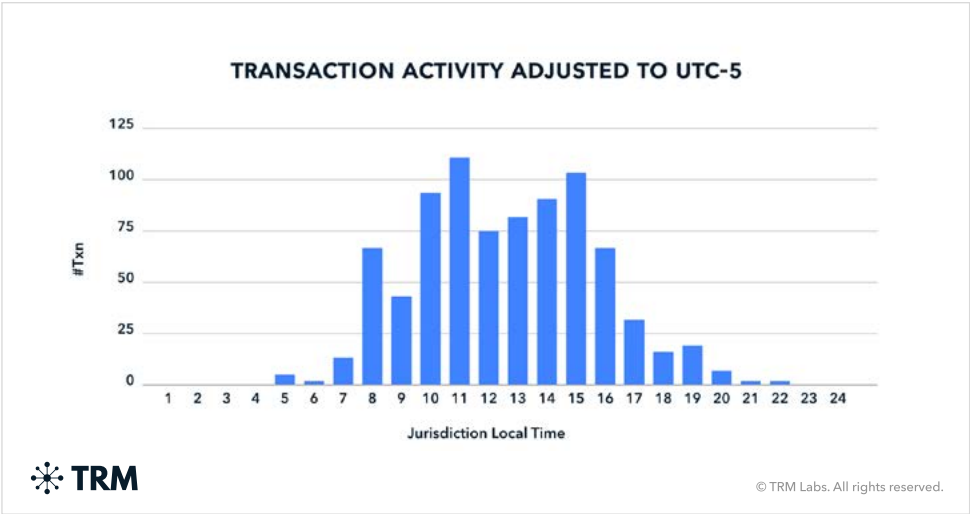
Case Study:
A regulator assessing a potential unregistered VASP (Target VASP, below) identifies multiple addresses that also transact with a licensed VASP operating solely within the same jurisdiction. This may help reveal where the target VASP conducts its activities.

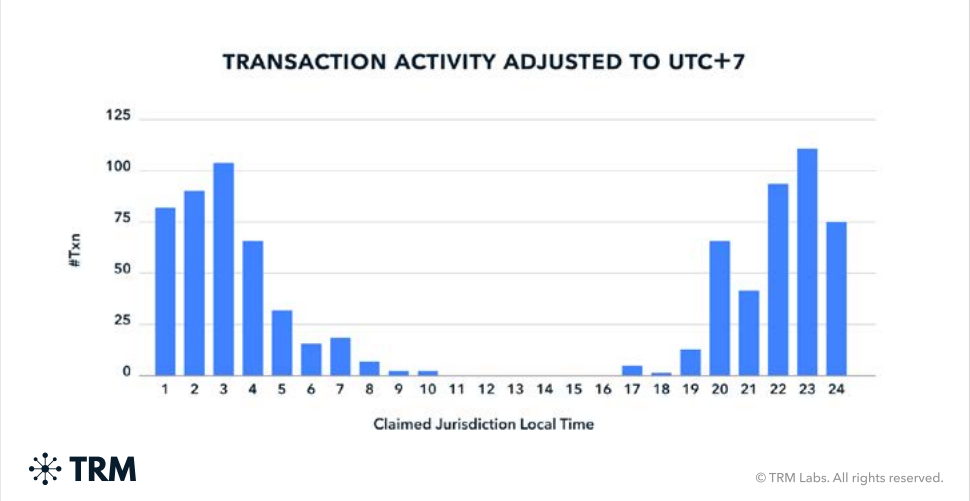


3. Time-based transaction analysis

Time-based analysis of transactions can also help to determine whether a VASP actually operates where it claims to, particularly when it comes to over-the-counter brokers, P2P traders or cash-to-crypto services.

Case Study:
A regulator operating in a jurisdiction the Coordinated Universal Time (UTC-5) timezone is engaging with a VASP, who they understand to be undertaking unregistered activity in their jurisdiction. This VASP informs the regulator that they are, in fact, operating in a different jurisdiction altogether, within the UTC+7 timezone. The regulator conducts a review of the VASP's addresses and identifies that most transaction activity took place during regular business hours in the UTC-5 timezone. As that would be night-time in the VASP's reported jurisdiction.





Whilst there may be legitimate reasons for the activity taking place during irregular hours, regulators can take this analysis to develop their investigation.

Depending on the case specifics, blockchain intelligence can be used in numerous other ways to investigate unregistered VASPs. Contact the TRM team to learn how we can support your unregistered VASP investigations.

About the author:

Ben is a Blockchain Intelligence Analyst at TRM. In this role, he ensures that TRM customers have access to the most timely, accurate and actionable VASP intelligence on the market. Prior to TRM, Ben was a Cryptoasset Technical Specialist at the UK's Financial Conduct Authority (FCA).

An early member of the department supervising VASPs, Ben was the technical lead on detection, investigation and disruption of unregistered crypto businesses operating in the UK, and was the intelligence lead for the FCA's well-publicized disruption of illegal Bitcoin ATMs in 2023.

Prior to joining the supervision team, Ben was an intelligence analyst. He developed the FCA's blockchain intelligence capability, including augmenting blockchain intelligence with other information sources to disrupt criminal actors from obtaining approval in the UK.