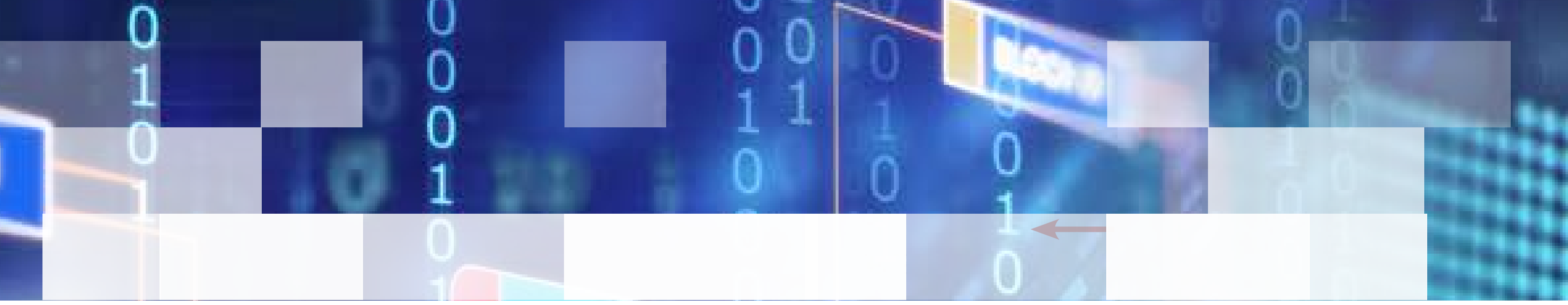
Virtual Assets Red Flag Indicators

of Money Laundering and Terrorist Financing

Public Sector

September 2020



Criminals and terrorist continuously seek new ways to launder the proceeds of crime and move assets with links to terrorism. Virtual assets, which can be swiftly transferred around the world, have unfortunately attracted criminals. Cases collected by FATF members across the Global Network during the last three years show that criminals have used virtual assets to evade financial sanctions and to raise funds to support terrorism. On the basis of these cases, the FATF has established red flag indicators of money laundering and terrorist financing.

The majority of virtual asset-related offences focused on predicate or money laundering offences. **The most common type of misuse of virtual assets was for illicit trafficking in controlled substances**. These involve sales transactions directly in virtual assets or where virtual assets are used as a money laundering layering techniques.

The second most common category of misuse is related to **frauds, scams, ransomware, and extortion**. More recently, professional money laundering networks have started exploiting virtual assets as one of their means to transfer, collect, or layer proceeds.

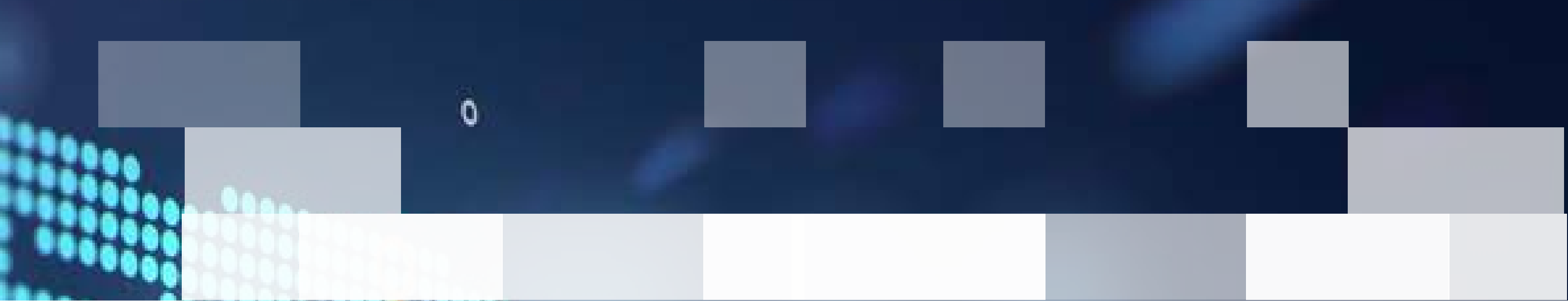
Other serious criminal offences involving the use of virtual assets include **tax evasion**, **computer crimes** (e.g. cyberattacks resulting in thefts) **child exploitation** and **human trafficking**.

What do countries need to do?

To prevent the misuse of virtual assets for the financing of crime and terrorism, the FATF strengthened its global anti-money laundering and counter-terrorist financing standards.

- **Understand** the money laundering and terrorist financing risks the sector faces
- **Licence** or **register** virtual asset service providers
- **Supervise** the sector, in the same way it supervises other financial institutions

If a country decides to prohibit virtual assets, it should take action for non-compliance with the prohibition. The red flag indicators of money laundering and terrorist financing may assist them in identifying illicit virtual asset activity.



How will the Red Flag Indicators help detect and prevent money laundering and terrorist financing using virtual Assets?

Operational agencies including Financial Intelligence Units, law enforcement authorities, and prosecutors may find this report a useful reference for analysing suspicious transaction reports or improving detection, investigation, and confiscation of VAs involved in misuse.

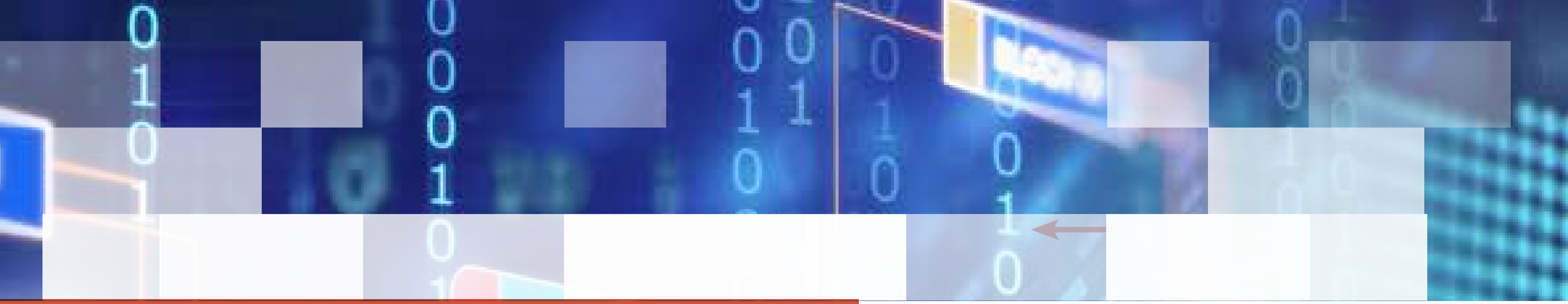
Regulators, may find these indicators useful when monitoring for entities' compliance with AML/CFT controls. For example, if a virtual asset service provider has information indicating the existence of one or more indicators without logical business explanation, but fails to report it as a suspicious transaction, competent authorities may consider following up with the virtual asset service provider.

Information from operational agencies and/or public-private partnerships, can help further develop these red-flag indicators. A risk-based approach implemented with a regular and dynamic two-way dialogue between the public and private sectors can help promote understanding of how criminals misuse virtual assets.

What does private sector need to do?

Virtual asset service providers, financial institutions and designated non-financial businesses and professions need to:

- Implement the same preventive measures as financial institutions, including customer due diligence, record keeping and reporting of suspicious transactions
- Obtain, hold and security transmit originator and beneficiary information when making transfers



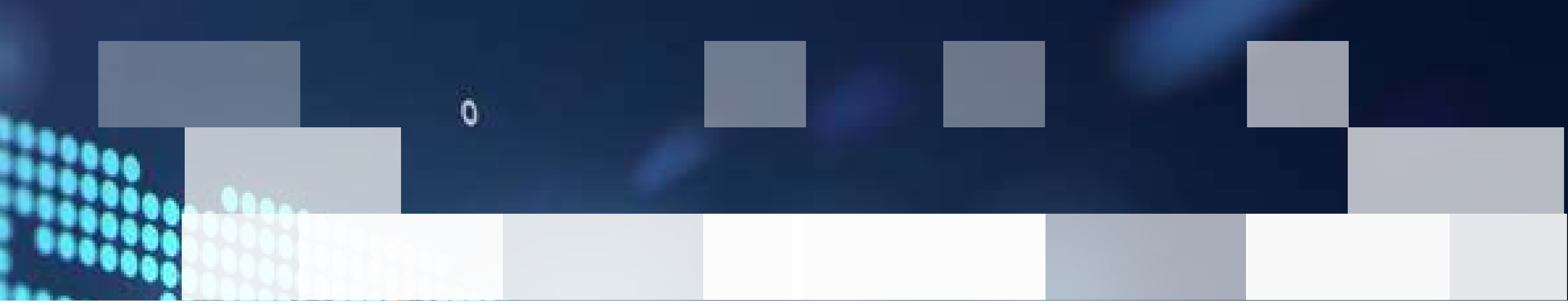
What are the main red flag indicators of money laundering and terrorist financing?

Geographical risks - criminals can exploit countries with weak or absent national anti-money laundering and counter-terrorist financing measures regarding virtual assets. Globally, many countries have implemented robust measures to comply with FATF's requirements. However, when it comes to addressing the money laundering and terrorist financing risks that virtual assets pose, some countries have not, or not yet, fully implemented the FATF's latest safeguards. Criminals exploit these gaps in implementation and move their illicit funds to countries where regulations are less strict. Indicators of this type of activity include:

- Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
- Customer uses a virtual asset exchange or foreign-located money value transfer service in a high-risk jurisdiction known to have inadequately regulated for virtual asset entities, including inadequate CDD or KYC measures.

Technological features that increase anonymity make virtual assets more attractive to criminals. Virtual assets have introduced a whole new vocabulary that identify processes and features that only exist in a virtual context, such as peer-to-peer exchanges, mixing or tumbling services or anonymity enhanced cryptocurrencies. These features complicate law enforcement investigations and could suggest illicit activity:

- Transactions involving more than one type of virtual assets, particularly those that provide higher anonymity, such as anonymity enhanced cryptocurrency or privacy coins and despite additional transaction fees.
- Virtual assets moved from a public, transparent blockchain to a centralised exchange and then immediately traded for anonymity enhanced cryptocurrency or privacy coin.
- Customers that operate as an unregistered or unlicensed virtual asset service provider on peer-to-peer exchange website.
- Abnormal transaction activity of virtual assets from peer-to-peer platform associated wallets with no logical business explanation.
- Virtual assets traded to or from wallets that indicated the use of mixing or tumbling services or peer-to-peer platforms.



Size and frequency of transactions, including:

- Structuring transactions in small amounts and under the record-keeping or reporting thresholds.
- Making multiple high-value transactions.
- Transferring virtual assets immediately to multiple virtual asset service providers, including those registered or operated in other countries.

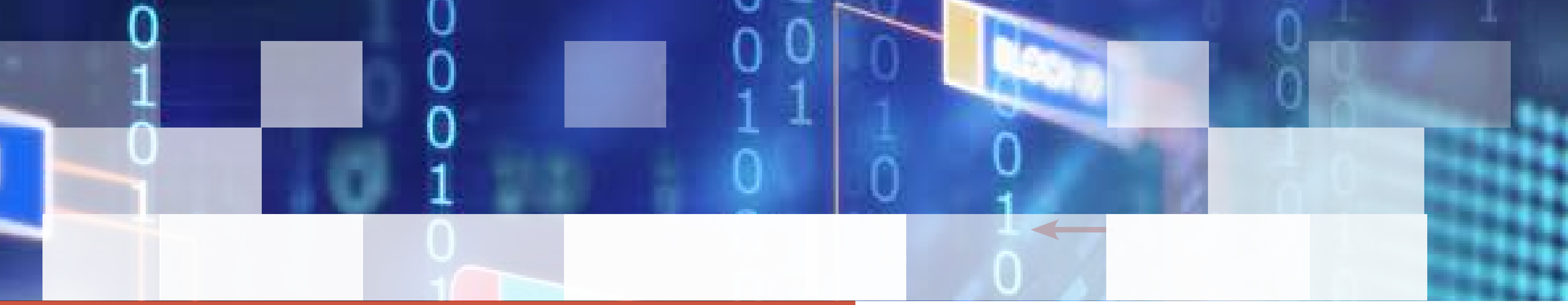
Transaction patterns that are irregular, unusual or uncommon can suggest criminal activity, for example when:

- New users make a large initial deposit to open a new relationship with a virtual asset service provider, inconsistent with the customer profile.
- Transactions involve multiple virtual assets, or multiple accounts, without a logical business explanation.
- Frequent transfers occur in a certain period of time, to the same virtual asset account by more than one person, from the same location or concerning large amounts.

The sender or recipient suggest criminal activity:

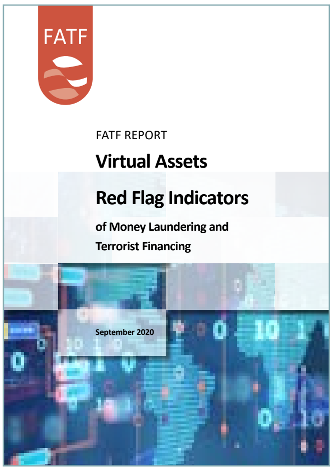
- Irregularities during account creation, such as creating different accounts under different names, or transactions initiated from IP addresses from sanctioned jurisdictions.
- Irregularities during the customer due diligence process, for example incomplete or insufficient customer information, forged identification document during onboarding.
- Irregularities in customer profile, such as shared credentials or presence on forums associated with illegal activity.
- Potential mule or scam victims, who are often unfamiliar with virtual assets technology.

The source of funds or wealth, relates to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, darknet marketplace, online gambling or fraudulent initial coin offerings.



Download the report

and more information about the FATF's focus on virtual assets



FATF

FATF REPORT

Virtual Assets

Red Flag Indicators

of Money Laundering and Terrorist Financing

September 2020

The FATF report on **Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing** provides further explanation and examples of red flag indicators.

These indicators are neither exhaustive nor applicable in every situation. They are often just one of the elements contributing to a bigger overall picture of a potential money laundering or terrorist financing risk. It is important that the indicators (or any single indicator) should not be viewed in isolation.

Competent authorities should provide additional advisories to reporting entities, conduct engagement and awareness-raising sessions with reporting entities to promote their understanding of the evolving risk environment.

***Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing* (September 2020)**
www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

FATF

GUIDANCE FOR A RISK-BASED APPROACH

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

JUNE 2019

In addition to the red flag indicators, the FATF has also established guidance with significant input from the private sector. The guidance explains how to understand the risks, how to license and register the sector, and what the sectors needs to do to know who their customers are, store this information securely and detect and report suspicious transactions.

***Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (June 2019)**
www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

More information:

www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html