Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

Financial and Non-Financial Sectors

September 2020

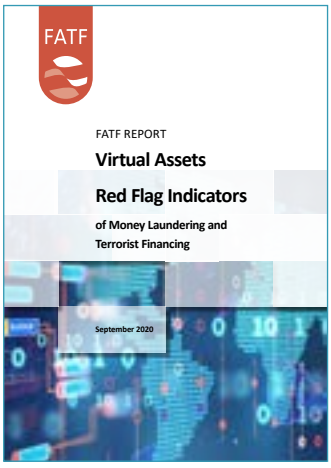
Innovative technology has dramatically shifted the financial landscape. Virtual assets, using innovative technology to swiftly transfer value around the world, present many benefits, such as speed and efficiency. They have unfortunately also attracted criminals who have used virtual assets to launder the proceeds of a range of offences such as drug trade, illegal arms trade, fraud, tax evasion, cyber attacks, child exploitation, human trafficking, and sanctions evasion.

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. Financial institutions, money service businesses, and other non-financial services and professions (DNFPBs) that need to deal with virtual asset transactions, need to understand these requirements. In particular, how to apply the risk-based approach to their customer due diligence requirements, which require knowing who their clients and the beneficial owners are, understanding the nature and purpose of the business relationship, and understanding the source of funds and wealth.

Which indicators suggest suspicious transactions?

The FATF has identified red flag indicators that may help financial services and DNFPBs identify suspicious activity.

A single indicator is not necessarily proof of criminal activity. A transaction with multiple indicators and with little or no logical business explanation could indicate potential criminal activity. This then requires further monitoring, examination, and reporting where appropriate.



www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

The technological features of virtual assets increase anonymity. These features make virtual assets more attractive to criminals. The blockchain technology behind virtual assets sets these transactions apart from traditional financial transactions. The challenge for the financial and designated non-financial businesses and professions sectors is now to develop the skills to understand and manage virtual asset transactions and to detect and prevent criminals and terrorists from misusing their services for criminal activities. 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.

The technological features of virtual assets also add hurdles to the usual customer due diligence and know-your-customer measures. **Often, it is easy easier to observe suspicious activities during general transaction monitoring or transaction-specific reviews:**

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 funds 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

- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency.
- Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).
- Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.

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, or available wealth not consistent with an individual's historical financial profile.

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.

- Transacting with bank cards that are connected to known fraud, ransomware schemes or darknet marketplaces.
- The use of one or multiple credit and/or debit cards that are linked to a virtual asset wallet to withdraw large amounts of fiat currency (crypto to plastic), or funds for purchasing virtual assets are sourced from cash deposits into credit cards.
- Deposits into an account or virtual assets address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available, or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.
- Bulk of a customer's source of wealth is derived from investments in virtual assets, ICOs, or fraudulent ICOs, etc.
- A customer's source of wealth is disproportionately drawn from virtual assets originating from other virtual asset service providers that lack anti-money laundering or counter-terrorist financing controls.

Geographical risks - criminals can exploit countries with weak or absent national measures to detect, prevent and punish money laundering and terrorist financing regarding virtual assets. Globally, many countries have implemented robust anti-money laundering and counter-terrorist financing measures to comply with FATF's requirements.

However, when it comes to addressing the money laundering and terrorist financing risks posed by virtual assets, some countries have not, or not yet, fully implemented the FATF's latest safeguards. Criminals can 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 utilises a virtual asset exchange or foreign-located money value transfer service in a high-risk jurisdiction lacking, or known to have inadequately regulated virtual asset entities, including inadequate customer due diligence and know-your-customer measures.

The FATF report on virtual asset red flag indicators provides further explanation and examples of red flag indicators, including those about anonymity.

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 **not to view the indicators (or any single indicator) in isolation**. If there is suspicious activity, this must be reported to the relevant authorities.

More information
about the FATF's focus on virtual assets

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

www.fatf-gafi.org | September 2020