Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

Virtual Asset Service Providers

September 2020

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, sanctions evasion, child exploitation and human trafficking.

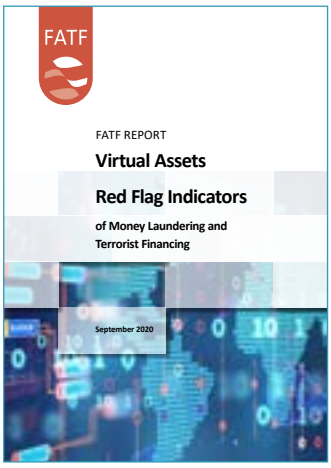
The FATF strengthened its global anti-money laundering and counter-terrorist financing standards to prevent the misuse of virtual assets for the financing of crime and terrorism. This will ensure transparency of virtual asset transactions and keep funds with links to crime and terrorism out of the cryptosphere. At the same time, this will increase trust in blockchain technology as the backbone behind a robust and viable means to transfer value.

How can virtual asset service providers

detect suspicious transactions?

The FATF has identified red flag indicators that to help virtual asset service providers identify suspicious activity.

A transaction with multiple indicators and with little or no logical business explanation, could indicate potential criminal activity. This would require 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 and add hurdles to the usual customer due diligence. Often, it is easier to detect suspicious activities during general transaction monitoring or transaction-specific reviews. For example :

Transaction size and frequency, 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.

Technological features that increase anonymity make virtual assets more attractive to criminals. Transactions involving technologies that are unique to virtual assets, such as peer-to-peer exchange websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies, complicate law enforcement investigations and could suggest illicit activity. Nevertheless, this is not always the case, and virtual asset service providers must consider these transactions in the context of the customer, the business relationship, or a legitimate business explanation. Indicators of this type of activity include:

- 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 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.

Geographical risks - criminals can exploit countries with weak or absent national anti-money laundering and counter-terrorist financing measures regarding virtual assets. Some countries have not, or not yet, fully implemented the FATF's requirements regarding the regulation of virtual assets. Criminals exploit these gaps and move their illicit funds to virtual asset service providers registered or operated in countries where regulations are less strict. This can concern the source, destination, or transit jurisdiction of a transaction. These risks also exist if the originator of a transaction or the beneficiary of funds is linked to a high-risk jurisdiction. Indicators of this type of activity include:

- Customer funds originate from, or are sent to, an exchange that is not registered in the country 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 country lacking, or known to have inadequate, AML/CFT regulations for virtual asset entities, including inadequate Customer Due Diligence or Know-Your-Customer measures.

The FATF report on virtual assets red flag Indicators provides further explanation and examples of indicators about senders, recipients, source of funds or wealth that may suggest criminal activity.

Each of these indicators alone, does not necessarily indicate criminal activity, but must be considered in context and lead to further monitoring and examination.

If there is suspicious activity, this must be reported to the relevant authorities.

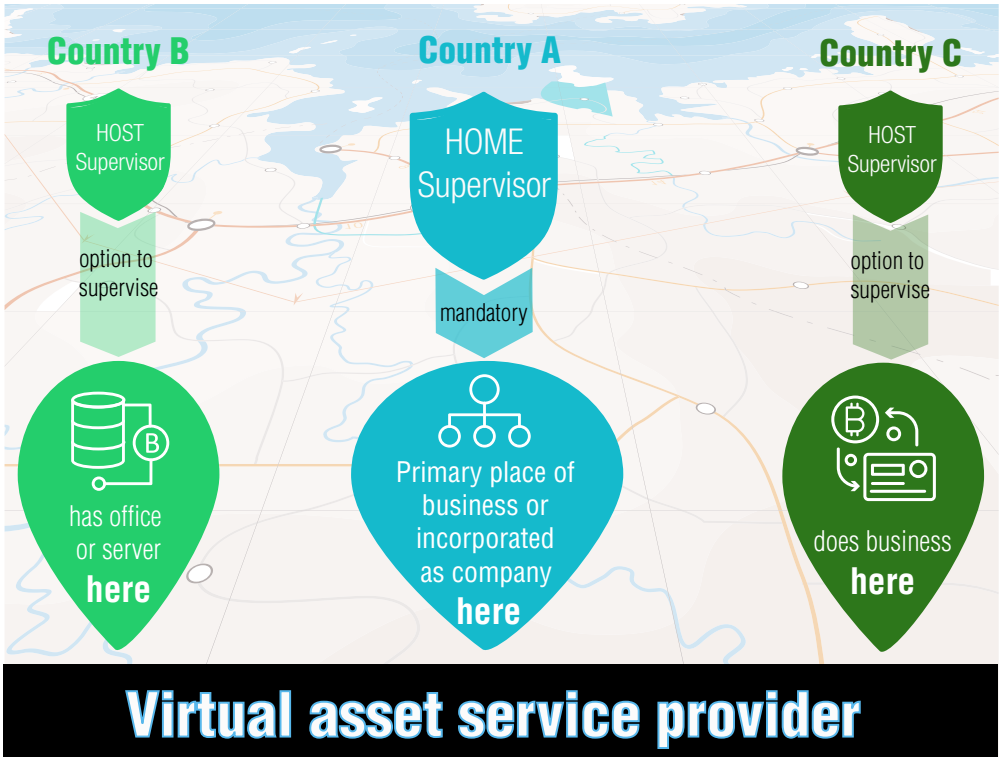
What should virtual asset service providers do

when they detect suspicious transactions?

The FATF Standards require virtual asset service providers to:

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

FATF also requires relevant competent authorities to establish guidelines and provide feedback that will assist virtual asset service providers (as well as other obliged entities, including traditional financial institutions) in applying national measures to combat money laundering and terrorist financing and, in particular, in detecting and reporting suspicious transactions—whether virtual/fiat or virtual/virtual. Regardless of the location of the virtual asset service provider's server, or where it does business, its home supervisor is in the country where it is incorporated as a company.



More information
about the FATF's focus on virtual assets

Guidance for a Risk-Based Approach to 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 virtual asset service provider 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.

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