



# VIRTUAL ASSETS RED FLAG INDICATORS of Money Laundering and Terrorist Financing

The Financial Action Task Force (FATF) defines **Virtual Assets (VAs)** as digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes. VAs include digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value. The FATF emphasizes that VAs are distinct from fiat currency or legal tender.

VAs have the potential to spur financial innovation and efficiency as they allow transactions to occur across borders in a short timeframe. Notwithstanding, their distinct features also create new opportunities for Money Laundering, Terrorist Financing and the financing of criminal activities. VAs can be used by criminals to acquire, move and store assets digitally outside the regulated financial system, and to disguise the origin and destination of funds. These factors add hurdles to the detection, reporting and investigation of criminal and suspicious activity by the various authorities. The majority of VA related offences reported by jurisdictions include:

- Money Laundering
- Evasion of Financial Sanctions
- Terrorism Financing
- Scams
- Sale of Illegal Items and Controlled Substances
- Fraud
- Tax Evasion
- Ransomware
- Computer Crimes e.g. Cyberattacks
- Child Exploitation
- Human Trafficking
- Extortion

The FATF has outlined six (6) categories of **Red Flag Indicators** to assist reporting entities in identifying and reporting potential Money Laundering/ Terrorist Financing (ML/TF) and additional financial criminal activities. These red flag indicators are based on over one hundred case studies completed during 2017—2020 as well as information received relative to the misuse of VAs available in the public domain.

### Red Flag Indicators Related to Transactions

- Structuring of VA transactions in small amounts or in amounts under record-keeping or reporting thresholds;
- Making multiple high-value transactions:
  - in short succession periods;
  - in staggered and regular patterns with no further transactions recorded during a long period after; or
  - to a newly created or to a previously inactive account;
- Transferring VAs immediately to multiple Virtual Asset Service Providers (VASPs), especially those registered or operated in another jurisdiction where:
  - there is no relation to where the customer lives or conducts business; or
  - there is non-existent or weak AML/CFT regulation.

### Red Flag Indicators Related to Transactions (Cont'd)

- Depositing funds from VAs addresses that have been linked to stolen funds.
- Depositing VAs at an exchange and then immediately:
  - withdrawing the VAs without any activity;
  - converting the VAs to multiple types of VAs; or
  - withdrawing VAs from a VASP to a private wallet immediately.

### Red Flag Indicators Related to Geographical Risks

- Funds originate or are sent to an exchange that is not registered in the jurisdiction where the customer or exchange is located;
- Customer utilizes a VA exchange in a high-risk jurisdiction lacking AML/CFT regulations for VA and with inadequate Customer Due Diligence (CDD) measures;
- Customer sends funds to VASPs operating in countries that have no VA jurisdiction or Anti Money Laundering/ Countering the Financing of Terrorism (AML/CFT) controls;
- Customer sets up offices in jurisdictions that have no VA regulation.

In October 2018, the Financial Action Task Force (FATF) updated its Standards to clarify the application of the FATF Standards to VA activities and Virtual Asset Service Providers (VASPs) in order to assist jurisdictions in mitigating the money laundering (ML) and terrorist financing (TF) risks associated with VA activities and in protecting the integrity of the global financial system.



### Red Flag Indicators Related to Transaction Patterns

- Large deposit(s) inconsistent with the customer's profile;
- Large deposit(s) to fund opening deposit with VASP and starting to trade large amounts on the same day or the day after, or withdrawing the whole amount the day after;
- New user trading the entire balance of the VAs, or withdrawing the VAs and attempting to withdraw the entire balance involving multiple VAs;
- Frequent transfers in a certain period of time (eg. a day or a week) to the same VA account by numerous persons, from the same IP address;
- Incoming transactions from many unrelated wallets in relatively small amounts with subsequent transfer to another wallet or full exchange for legal tender; and
- Conversion of the VA to a fiat currency at a potential loss or without logical explanation.



### Red Flag Indicators Related to Anonymity


- Transactions involving multiple types of VA;
- Moving a VA that operates on a public, transparent blockchain to a centralized exchange then immediately trading it for an anonymity-enhanced cryptocurrency (AEC) or privacy coin;
- Customers that operate as an unregistered VASP on peer-to-peer (P2P) exchange websites;
- Abnormal activity of VAs cashed out on P2P platforms;
- VA transactions using VASPs which operate mixing or tumbling services or P2P platforms;
- Using VA ATMs/kiosks in high-risk locations; and
- Deposits/withdrawals from a VA address/wallet with direct and indirect exposure links to known suspicious sources.



### Red Flag Indicators about Senders or Recipients

- Irregularities observed during account creation such as suspicious IP addresses and multiple attempts to open accounts;
- Irregularities observed during the CDD process such as incomplete forms, inaccurate information, forged documents, edited photographs or IDs;
- Discrepancies between IP addresses associated with the customer's profile and transactions;
- Customer's VA address appears on public forums associated with illegal activity;
- Customer is known via publicly available information to law enforcement due to previous criminal associations;
- Frequent changes to ID, email address or IP address; and
- Sender unfamiliar with VA technology.

### Red Flag Indicators in the Source of Funds or Wealth

- Bulk of a customer's source of wealth is derived from investments in VAs, Initial Coin Offerings (ICOs), or fraudulent ICOs, etc;
  - Deposits significantly higher than usual with an unknown source of funds, followed by conversion to fiat currency;
  - Customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls;
  - Lack of transparency on the origin of funds;
  - Funds sourced directly from third-party mixing services or wallet tumblers;
  - Use of multiple credit/debit cards linked to a VA wallet to withdraw large amounts of fiat currency; and
  - Transacting with VA addresses or bank cards connected to fraud, sanctioned addresses, online gambling services, etc.
- 

Some red flag indicators might be more evident during general transactional monitoring, while others may be more readily noticeable during transaction-specific reviews. When one or more red flag indicators are present, and with little or no indication of a legitimate economic or business purpose, the reporting entity may be more likely to develop a suspicion that criminal activity is occurring. The existence of a single indicator does not necessarily indicate criminal activity. Often, it is the presence of multiple indicators in a transaction with no logical business explanation that raises suspicion of potential criminal activity. The presence of indicators should encourage further monitoring, examination, and reporting where appropriate. While the indicators identified are not exhaustive and are constantly evolving, they are best used when applying other contextual information from domestic law enforcement and public sources.

#### Reference:

September 2020 FATF Report—Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing.