FATF Report on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

Introduction

On 14 September 2020, the Financial Action Task Force (FATF) published a report on virtual assets (VAs) red flag indicators of money laundering and terrorist financing (ML/TF) based on over 100 case studies from recent years. Since there are different methods and red flags for ML/TF involving VAs compared to traditional assets, the indicators and details in this report provide valuable insights to support efforts to tackle ML/TF concerning VAs.

This FATF report aims to facilitate the identification of ML/TF activity and risks for various industry participants, including operational and regulatory agencies as well as financial institutions. This report may assist reporting entities such as Virtual Asset Service Providers (VASPs) and banks in identifying and reporting ML/TF risks involving VAs and should help adopt a risk-based approach to the implementation of anti-money laundering and counter-terrorist financing (AML/CTF) controls.

Red Flag Indicators Related to Transactions

The FATF highlights that in many situations, the size, frequency, and timing of transactions may be red flag indicators. This includes when numerous transactions are conducted which are small or just below the thresholds for transaction reporting and recording, as this activity may be a deliberate attempt by criminals to evade detection. Firms facilitating VA transactions must recognise that multiple low-value transactions which are related may collectively meet thresholds and apply the relevant customer due diligence (CDD) measures if this is the case.

Equally, high-value transactions may be considered suspicious in some cases, especially when the transactions are inconsistent with the customer's profile or are sent to new or previously inactive addresses. Close and continuous monitoring of the customer is key in recognising red flag indicators such as these, especially as the customer's expected activity and risk profile may change over time. Blockchain analytics and VASP identification services greatly facilitate the identification of many of these indicators, as well as the subsequent application of further CDD measures.

Red Flag Indicators Related to Transaction Patterns

Potential ML/TF activity may be identified through the recognition of transaction patterns which are abnormal or inconsistent with the customer's expected activity. In relation to new customers, in particular, unusually large deposits and hasty trades or withdrawals of funds may give rise to suspicions.

Due to deposit and withdrawal limits enforced by most VASPs, Over-The-Counter (OTC) trading without limits may be popular among large-scale money launderers, especially where OTC brokers have lax CDD requirements. Indeed, a 2020 report by Chainalysis on the state of crime in the VA

industry found that OTC brokers often have lower CDD requirements than VA exchanges and that some brokers even specialise in the laundering of criminal funds.[1]

Red Flag Indicators Related to Anonymity

Various methods of enhancing anonymity when using VAs are identified by the FATF as red flag indicators in some circumstances, since they may impede the tracing of funds and detection of illicit activity. Although there are legitimate uses for these means of enhancing anonymity, they may be particularly suspicious in cases where transactions are:

- unusually high in value or volume
- unnecessarily complex despite transaction fees
- linked to suspicious sources or potential fraud

Table 1: Anonymisation methods which may be red flag indicators

Privacy-enhanced Technology	Privacy-enhanced Exchange
Privacy coins	Peer-to-peer or decentralised exchanges
Mixers	Exchanges with poor or non-existent CDD requirements
Decentralised, unhosted or private wallets	Virtual Asset ATMs
Internet anonymisation software such as VPNs	

Red Flag Indicators about Senders or Recipients

The FATF points out several examples of unusual customer activity or behaviour which may be indicative of ML/TF, especially of behaviour which leads to doubts regarding the accuracy of information provided by the customer. These red flag indicators include, for example, when a single customer uses several different accounts, names, or IP addresses. Further, there would be a clear red flag if any of the customer's information is found to be linked to suspicious or illicit activity such as darknet markets and forums, or to sanctioned entities or jurisdictions. Background checks of customers against regularly updated negative lists are key in ensuring these links, and potential illicit activities are identified.

Red Flag Indicators in the Source of Funds or Wealth

Red flag indicators relating to the source of funds or wealth include when:

- transactions are linked to known illicit activity
- customers make unusually large deposits and withdrawals with conversion between VAs and fiat currency

[1] Chainalysis, 'The 2020 State of Crypto Crime' (2020) https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf.

- funds or wealth derive mainly from VA investments or VASPs with poor AML/CTF controls

These behaviours may be indicative of various illicit activities involving the misuse of VAs which were identified in cases submitted to the FATF.

Red Flag Indicators Related to Geographical Risks

Since the FATF Standards and Recommendations for VAs and VASPs have not seen harmonised implementation across the globe, criminals may seek regulatory arbitrage opportunities and conduct VA activities in jurisdictions with weak AML/CTF controls. As such, the FATF outlines several indicators that criminals may be exploiting these opportunities, including where transactions involve a VA exchange in a jurisdiction with weak or non-existent AML/CTF regulations. However, as with many red flag indicators discussed above, these do not necessarily indicate illicit activity. Indeed, some entities within these jurisdictions may nonetheless have strong AML/CTF controls.

Conclusion

Based on a substantial set of case studies and inputs from FATF Members, the red flag indicators in this report provide valuable insights to support the identification and prevention of ML and TF in the VA industry. However, the FATF emphasise that these indicators are purely indicative and not demonstrative of illicit activity and should be considered in context among a range of other factors as part of a risk-based approach. Since the methods and indicators of money laundering are constantly evolving, attention to the current context and technologies will be essential in keeping AML/CTF controls up to speed with the techniques used to evade them.