FATF

FATF REPORT

Virtual Assets

Red Flag Indicators

of Money Laundering and Terrorist Financing

September 2020

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2020), *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets,* FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

Table of Contents

Acronyms

AEC	Anonymity enhanced cryptocurrency
CDD	Customer due diligence
DNFBPs	Designated non-financial businesses and professions
DNS	Domain name registrars
FATF	Financial Action Task Force
FIs	Financial Institutions
FIUs	Financial Intelligence Units
ICO	Initial Coin Offering
KYC	Know-your-customer
LEAs	Law enforcement authorities
ML	Money Laundering
STRs	Suspicious Transaction Reports
TF	Terrorist Financing
VA/VAs	Virtual Assets
VASPs	Virtual Asset Service Providers

Introduction

1. Virtual assets (VA) and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. The ability to transact across borders rapidly not only allows criminals to acquire, move, and store assets digitally often outside the regulated financial system, but also to obfuscate the origin or destination of the funds and make it harder for reporting entities to identify suspicious activity in a timely manner. These factors add hurdles to the detection and investigation of criminal activity by national authorities.

2. 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, among other things, 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. In June 2019, the FATF adopted an Interpretative Note to Recommendation 15 to further clarify the application of FATF requirements to VA activities or operations and VASPs, including with respect to suspicious transaction reporting.

3. The FATF has prepared this brief report on ML/TF red flag indicators associated with VAs to assist reporting entities, including financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), and VASPs; however, they are categorised, in identifying and reporting potential ML and TF activity involving VAs. This report should also facilitate reporting entities' application of a risk-based approach to their Customer Due Diligence (CDD) 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.

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

5. Financial, DNFBP, and VASP regulators, on the other hand, may find these indicators useful when preparing STRs and monitoring for entities' compliance with AML/CFT controls. Where a reporting entity has information indicating the existence of one or more indicators without logical business explanation, but fails to file an STR despite a customer's inconsistent explanation or fails to seek clarification on the transaction, competent authorities may consider following up with the reporting entity taking into account the latter's business profile.

Methodology and sources used in drawing up the list of red flag indicators

6. The red flag indicators included in this report are based on more than one hundred case studies contributed by jurisdictions from 2017-2020, the findings of the *Confidential FATF Report on Financial Investigations Involving Virtual Assets* (June 2019) and the published *FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014), as well as information on the misuse of VAs available in the public domain.

Trends in use of VAs for ML/TF purposes

The majority of VA-related offences focused on predicate or ML offences. Notwithstanding, criminals did make use of VAs to evade financial sanctions and to raise funds to support terrorism.

The types of offences reported by jurisdictions include ML, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, computer crimes (e.g. cyberattacks resulting in thefts), child exploitation, human trafficking, sanctions evasion, and TF. Among these, the most common type of misuse is illicit trafficking in controlled substances, either with sales transacted directly in VAs or the use of VAs as an ML layering technique. The second most common category of misuse is related to frauds, scams, ransomware, and extortion. More recently, professional ML networks have started exploiting VAs as one of their means to transfer, collect, or layer proceeds.

Source: Case studies contributed by jurisdictions from 2017-2020

Issues to note when reading this Report

7. These indicators are specific to the nature of VAs and their associated financial activities, and are by no means exhaustive. Suspicious activities involving the use of VAs may also share similar traits with ML/TF activities involving the use of fiat currency, or other kinds of assets. Reporting entities should therefore consider the risks posed by their customers, products, and operations, as well as the presence of conventional risk indicators. Red flag indicators should always be considered in context.

8. Freestanding red flags such as those listed below can be developed or combined with information from operational agencies, which can in turn be further developed through a public-private partnership, in a cyclical, evolutionary process that takes into account the unique risk and context of a jurisdiction, customer type, or the reporting entity itself. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, but could prompt further monitoring and examination. Ultimately, a client may be able to provide an explanation to justify the red flag indicator, business or economic purposes of a transaction.

9. When evaluating potential suspicious activity, competent authorities, FIs, DNFBPs, and VASPs should be mindful that some red flag indicators might be more readily observable during general transactional monitoring, while others may be more readily observable during transaction-specific reviews. The observation of one or more of the indicators is dependent on the business lines, products, or services that an institution or VASP offers and how it interacts with its customers. 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 ML or TF is occurring.[1] These indicators should not be the sole determinant of whether or not an STR should be filed. Reporting entities should consider filing of an STR if they know, suspect, or have reasonable grounds that ML/TF has been committed.

Red Flag Indicators

10. The following sections contain a collection of red flag indicators of suspicious VA activities or possible attempts to evade law enforcement detection, as identified through more than one hundred case studies collected since 2017 from across the FATF Global Network, literature reviews, and open source research. As previously mentioned, 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.

Red Flag Indicators Related to Transactions

11. While VAs are still not widely used by the public, their use has caught on among criminals. The use of VAs for ML purposes first emerged over a decade ago, but VAs are becoming increasingly mainstream for criminal activity more broadly. This set of indicators demonstrates how red flags traditionally associated with transactions involving more conventional means of payment remain relevant to detecting potential illicit activity related to VAs.

Size and frequency of transactions

- Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions –
  - in short succession, such as within a 24-hour period;
  - in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or

[1] While a number of red flag indicators could apply to both instances of ML and TF, e.g. fundraising activities, financing of foreign terrorist fighters (FTFs), and purchase of weapons (e.g. on the darknet) using VAs, readers are encouraged to read in connection with the Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators (June 2016) (restricted access to FATF Members).

  - to a newly created or to a previously inactive account.
- Transferring VAs immediately to multiple VASPs, especially to VASPs 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.
- Depositing VAs at an exchange and then often immediately –
  - withdrawing the VAs without additional exchange activity to other VAs, which is an unnecessary step and incurs transaction fees;
  - converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
  - withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.
- Accepting funds suspected as stolen or fraudulent -
  - depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

Case Study 1. Multiple immediate transfers of large amount of VAs to overseas VASPs

A local VASP submitted STRs following suspicions concerning the purchase of large amounts of VAs by various individuals and their subsequent immediate transfers to VASPs in a foreign jurisdiction. In various instances, the individuals shared the same residential address; and most of the VA addresses were accessed from the same IP address – indicating the potential use of money mules by professional money launderers to launder the illicit proceeds.

In addition, multiple layering of the fiat funds was arranged prior to the VA purchase by mules. To disguise the funds' origin, cash was first deposited into various accounts at different FIs across the jurisdiction. Those funds were then further transferred to various accounts held in the name of entities registered in the jurisdiction. Electronic payments were made into the accounts in smaller amounts. After that, funds were transferred to another group of accounts before reaching the mules' accounts held with local VASPs. VAs were immediately purchased and transferred to foreign VASPs. More than 150 individuals were involved in this case, responsible for transferring a total of about USD 108 352 900 (or BTC 11,960) to multiple VA accounts held by two overseas VASPs.

Source: South Africa

Case Study 2. Multiple VAs and multiple transfers to foreign VASPs

A local VA exchange reported that approximately KRW 400 million (EUR 301 170) was stolen from phishing victims and was ultimately exchanged for VAs as a layering technique. What triggered the reporting was the multiple high-value transactions transferred to a foreign VASP into one single wallet. The stolen funds in fiat currency were first exchanged to three different types of VAs and then deposited to the suspect's VA wallet held with a local VASP. The suspect then attempted to obfuscate the source of funds by transferring funds an additional 55 times through 48 separate accounts held in different local VASPs, and then to a different VA wallet located abroad.

Source: South Korea

Red Flag Indicators Related To Transaction Patterns

12. Similar to the above section, the red flags below illustrate how the misuse of VAs for ML/TF purposes could be identified through irregular, unusual, or uncommon patterns of transactions.

Transactions concerning new users

- Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile.
- Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading.[2]
- A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.

Case Study 3. Initial deposit inconsistent with customer profile

The presence of the following suspicious indicators prompted an FI (bank) to file an STR with authorities, leading to an ML investigation:

- transactions inconsistent with the profile of the account holder – in the first two days after a personal account had been created for a young individual, the account received deposits of a commercial nature from different legal persons in large amounts;
- transaction patterns – the deposited funds were immediately transferred to accounts of several VASPs (in one day) for VA purchase (Bitcoin);

[2] Over-the-counter trading refers to securities that are traded for companies that are not listed on a formal exchange, and via a broker-dealer network.

- customer profile – one of the ordering parties was known to the bank as a subject in a fraud case. The bank also provided IP addresses used for internet banking services to the authorities.

Based on an investigation, the personal account holder appeared to be a money mule recruited by criminals on a social media platform to help receive claimed payments for goods sold online. However, such funds appeared to have been deposited by other victim companies and were not payments for goods. The deposited funds were immediately transferred out from the personal bank account via several divided payments to another account held by a joint-stock company in Czech Republic, and were exchanged to VA (Bitcoin) held in several local VASPs. These VASPs were then immediately withdrawn from the account. In addition to filing an STR, the bank also suspended the suspicious transfers, which made subsequent seizure of funds possible.

The local VASP also noticed irregularities in the funds received and provided useful information to aid the investigation. The information included: circumstances where the VAs were purchased; transaction and other CDD information such as wallet address, copy of misused identification document for the purchase, and name of the alleged buyer. These allowed authorities to request additional information from the banks (e.g. bank statements).

Source: Czech Republic

Transactions concerning all users

- Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation.
- Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account –
  - by more than one person;
  - from the same IP address by one or more persons; or
  - concerning large amounts.
- 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.

Case Study 4. Transfers conducted in a recurrent time

A local FI (securities firm) filed an STR regarding unauthorised payments between the VA accounts of their broker and a foreign national. The securities firm reported the activity after it determined that the foreign national intended to make transfers totalling USD 4.8 million (two separate transactions that occurred six minutes apart on the same day), and filed an application to the broker for a trading account the next business day. The wallet was not hosted in the Cayman Islands. The STR reporting led to a successful information exchange with foreign FIUs and the successful return of most of the funds to the victim, as the online platform in a foreign jurisdiction had been able to freeze the suspect's account before the offence had been completed.

Source: Cayman Islands

Red Flag Indicators Related to Anonymity

13. This set of indicators draws from the inherent characteristics and vulnerabilities associated with the underlying technology of VAs. The various technological features below increase anonymity and add hurdles to the detection of criminal activity by LEAs. These factors make VAs attractive to criminals looking to disguise or store their funds. Nevertheless, the mere presence of these features in an activity does not automatically suggest an illicit transaction. For example, the use of a hardware or paper wallet may be legitimate as a way to secure VAs against thefts. Again, the presence of these indicators should be considered in the context of other characteristics about the customer and relationship, or a logical business explanation.

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.
- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin.
- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.
- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.

- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.
- Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.
- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.
- A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.
- Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent.
- Using VA ATMs/kiosks –
    - despite the higher transaction fees and including those commonly used by mules or scam victims; or
    - in high-risk locations where increased criminal activities occur.

  A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).

Case Study 5. Use of IP address associated with Darknet Marketplace – Alpha Bay

AlphaBay, the largest criminal darknet market dismantled by authorities in 2017, was used by hundreds of thousands of people to buy and sell illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals over a two-year span. The site operated as a hidden service on the TOR network to conceal the locations of its underlying servers as well as the identities of its administrators, moderators, and users. AlphaBay vendors used a number of different types of VAs, and had approximately 200 000 users, 40 000 vendors, 250 000 listings and facilitated more than USD 1 billion in VA transactions between 2015 and 2017.

In July 2017, the U.S. Government, with assistance from foreign counterparts, took down the servers hosting the AlphaBay marketplace, arrested the administrator, and pursuant to a seizure warrant issued in the Eastern District of California, seized the physical and virtual assets from the marketplace itself, and those that represented the unlawful proceeds from the AlphaBay criminal enterprise. Federal agents obtained the warrants after tracing VAs transactions originating from AlphaBay to other VA accounts and identifying bank accounts and other tangible assets controlled by the alleged administrator.

Source: United States

Case Study 6. Use of mixing and tumbling – Helix

A darknet-based VASP, Helix, provided a mixing or tumbling service that helped customers conceal the source or owners of VAs for a fee over a three-year period. Helix allegedly transferred over 350,000 Bitcoin, with a value at the time of transmission of over USD 300 million. The operator specifically advertised the service as a way to conceal transactions on the darknet from law enforcement. In February 2020, criminal charges including ML conspiracy and operating an unlicensed money transmitting business were brought against an individual who operated Helix.

Helix partnered with the darknet marketplace AlphaBay until AlphaBay's seizure by law enforcement in 2017.

Source: United States

Case Study 7. Use of decentralised wallet

This case demonstrates how criminals make use of decentralised wallet to obfuscate the source of illicit funds generated from illicit drug trafficking activities. In this case, criminals conducted a large quantity of drug sales on the Internet and sought payment not only in fiat currency but also in the form of VAs (Bitcoin, EX-codes, EXMO-cheques).

Illicit funds received in fiat currency were converted to VA with the aid of an anonymous account at an online Blockchain trading platform. Such funds, in the form of VAs, were then converted back into fiat currency via an exchanger, before being transferred back to the criminals' personal bank card accounts. As for those illicit funds received in the form of VAs, they were first transferred to decentralised Bitcoin wallets held by the criminals concerned, before being further transferred to other Bitcoin wallets at different exchanges. This increases the difficulty of tracing and tracking the funds. Similarly, the laundered funds (in VAs) were then converted back to fiat before being credited into the criminal's bank card accounts. The criminal was convicted and sentenced to seven years' imprisonment and a criminal fine after trial.

Source: Russian Federation

Red Flag Indicators about Senders or Recipients

14. This set of indicators is relevant to the profile and unusual behaviour of either the sender or the recipient of the illicit transactions.

Irregularities observed during account creation

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.
- Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
- Trying to open an account frequently within the same VASP from the same IP address.
- Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.

Irregularities observed during CDD process

- Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.
- Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

Case Study 8. Customer refusing to provide information on source of funds

An FI (bank) filed an STR concerning an account of a local company that held funds generated by the sale of coupons that can be traded with a product (bioplastics in this case). The funds were deposited by both natural and legal persons, with some originally in VAs. Despite further inquiries by the bank, representatives of the account holder did not provide information on the origins of the funds. Subsequent analysis by the authorities indicated that the funds sent by the company showed links with subjects connected to organised crime and with funds received from a fraudulent project.

Source: Italy

Profile

- A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account.
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer's VA address appears on public forums associated with illegal activity.
- A customer is known via publicly available information to law enforcement due to previous criminal association.

Case Study 9. Customer profile does not match with regular high-value VA trading

A VASP (exchanger) and an FI (payment institute) filed STRs with the FIU concerning a high value of VA trading that began when the account at the exchanger was opened. Specifically, the account holder had been carrying out various VA buying and selling transactions for over EUR 180 000 – which did not match the profile of the account holder (including occupation and salary).

Analysis found that the VAs were subsequently used for (i) transactions on a darknet market; (ii) online betting; (iii) transactions with VASPs that did not have adequate AML/CFT controls or that were under previous ML investigations involving millions of dollars; (iv) operations on platforms that offered peer-to-peer transactions of VAs; and (v) "mixing". The account holder had also made use of a variety of different means (e.g. money transfer, online banking, and prepaid cards) to move a consistent amount of funds out of his account in the same time frame. The funds received by the account holder appeared to come from a network of individuals who bought VAs (Bitcoin) in cash and were located in different jurisdictions in Asia and Europe (including Italy),

both via money transfer and the banking system. He also received funds on his prepaid cards from subjects in Africa and the Middle East, who in turn collected funds from fellow citizens residing in Italy and abroad. These funds were then used for cross-border transfers and online gambling, and were withdrawn in cash from ATMs in Italy.

Source: Italy

Profile of potential money mule or scam victims

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.
- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.
- Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

Case Study 10. Scam victims turned mules

In these investment scams, foreign nationals contacted pensioners and generally older persons by direct phone calls, emails, or through social media, and offered them investment opportunities in Bitcoin or other VAs with the promise to generate huge profits due to rising popularity in VAs and their increase in price. The initial investment in small amounts (in many cases no more than EUR 250) was made from the victims' bank account, credit card or via other means to various payment services and then ending up in the hands of the criminals. Alternatively, victims were instructed to exchange fiat currency to Bitcoin using a VA ATM and send the funds to an address specified by the criminals.

Victims were technologically not very adept and did not generally understand the VA technology or what they were really investing in. Criminals also asked victims to install a remote desktop application on their device so that the criminals could help transfer the funds correctly to specific accounts. This compromised the victims' devices so that the criminals could conduct unauthorised money transfers without the victim being aware of it until he/she noticed money missing from the account. In some cases, criminals also fabricated articles claiming that famous celebrities or wealthy businesspeople or newscasters were promoting VA investments, thereby giving victims a sense of trust and legitimacy to the "investments".

Source: Finland

Other unusual behaviour

- A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.
- A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day.
- Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.
- A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure.

Red Flag Indicators in the Source of Funds or Wealth

15. As demonstrated by cases submitted by jurisdictions, the misuse of VAs often relates to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, fraud, theft and extortion (including cyber-enabled crimes). Below are common red flags related to the source of funds or wealth linked to such criminal activities:

- Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.
- VA transactions originating from or destined to online gambling services.
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.
- Deposits into an account or a VA 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.
- A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.
- Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.
- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

Case Study 11. Use of shell companies – Deep Dot Web

In May 2019, U.S. LEAs seized a website, DeepDotWeb (DDW), pursuant to a court order. The alleged owners and operators of DDW were charged in an ML conspiracy related to millions of dollars in kickbacks they received for referring individuals to darknet marketplaces from the DDW website. Through referral links, the alleged owners and operators of DDW received kickback payments, representing commissions on the proceeds from the purchase of illegal goods, such as fentanyl and heroin, made by individuals referred to a darknet marketplace from the DDW site.

These kickback payments were made in VA and paid into a DDW-controlled Bitcoin wallet. To conceal and disguise the nature and source of the illegal proceeds, which totalled over USD 15 million, the owners and operators transferred their illegal kickback payments from their DDW Bitcoin wallet to other Bitcoin wallets, as well as to bank accounts that they controlled in the names of shell companies. The defendants used these shell companies to move their ill-gotten gains and conduct other activity related to DDW. During a five-year period, the website received approximately 8 155 Bitcoin in kickback payments from darknet marketplaces, worth approximately USD 8 million, adjusted for the trading value of Bitcoin at the time of each transaction. The Bitcoin was transferred to DDW's Bitcoin wallet, controlled by the defendants, in a series of more than 40 000 deposits, and was subsequently withdrawn to various destinations in over 2 700 transactions. The value of the Bitcoin at the time of the withdrawals from the DDW Bitcoin wallet equalled to approximately USD 15 million.

Source: United States

Case Study 12. Use of multiple VA exchanges, false identification documents for CDD and prepaid cards

The defendants in this matter allegedly operated an ML scheme in connection with cybercriminals who hacked a VA exchange and stole USD 250 million worth of VAs. The two defendants allegedly laundered about USD 91 million worth of the stolen VAs, as well as USD 9.5 million from another cyber theft.

The stolen VAs were then routed through hundreds of automated VA transactions and multiple VA exchanges. The launderers used doctored photographs and falsified identification documents in some cases to circumvent KYC procedures at the VA exchanges. Some USD 35 million of the illicit funds ultimately were transferred into foreign bank accounts and were also used to purchase prepaid cards, which could be exchanged for VAs. The defendants operated through independent as well as linked accounts and provided VA transmission services, such as

converting VAs into fiat currency, to customers for a fee. The defendants also conducted business in the US but at no time registered with the Financial Crimes Enforcement Network (FinCEN).

Source: United States

Red Flag Indicators Related to Geographical Risks

16. This set of indicators emphasises how criminals, when moving their illicit funds, have taken advantage of the varying stages of implementation by jurisdictions on the revised FATF Standards on VAs and VASPs.[3] Based on cases reported by jurisdictions, criminals have exploited the gaps in AML/CFT regimes on VAs and VASPs by moving their illicit funds to VASPs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations on VAs and VASPs. These jurisdictions may not have a registration/licensing regime, or have not extended STR requirements to cover VAs and VASPs, or may not have otherwise introduced the full spectrum of preventive measures as required by the FATF Standards. While this report does not seek to identify a list of "high risk" jurisdictions, reporting entities are invited to take into account the following indictors when considering geographical risks. These risks are associated with source, destination, and transit jurisdictions of a transaction. They are also relevant to risks associated with the originator of a transaction and the beneficiary of funds that may be linked to a high-risk jurisdiction. In addition, they may be applicable to the customer's nationality, residence, or place of business.

- 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 VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures.
- Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls.
- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

[3] In July 2020, the FATF published a 12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. Section 2 of the Report covers the progress of implementation of the revised Standards since June 2019.

Case Study 13. Bitcoin dealer operating unlicensed money transmitting businesses (cross-border elements)

In April 2019, the defendant received a sentence of two years in prison for operating an unlicensed money transmitting business after selling hundreds of thousands of dollars of VA (Bitcoin) to more than a thousand customers in the US. The defendant was also ordered to forfeit USD 823 357 in profits.

The defendant advertised his services on websites for VA users, meeting some customers in person to accept cash in exchange for VAs. Other customers paid him via nationwide ATMs or money transmitting services. The defendant received a five percent premium on the prevailing exchange rate for his services. He first acquired Bitcoin through a US exchange, but once his activities triggered suspicion and his account was closed, the defendant then switched to an exchange in Asia. Using that exchange, the defendant bought USD 3.29 million in Bitcoin, in hundreds of separate transactions, between March 2015 and April 2017. The defendant also admitted that he exchanged his US cash, which he kept in another jurisdiction bordering the US, with a precious metals dealer, and that between late 2016 and early 2018, he and others imported into the US a total of over USD 1 million, in amounts slightly below the USD 10 000 reporting requirement.

Source: United States

VASP moving its operation to a jurisdiction that has inadequate AML/CFT regulations

Ahead of the implementation of a policy to prohibit VASP operation in Jurisdiction A in Asia in 2017, a VASP (exchange) established in Jurisdiction A transferred its operation to Jurisdiction B in the same region. In 2018, Jurisdiction B stepped up its AML/CFT legal regime on VAs following significant hacks of some major VASPs (exchanges). In March 2018, the VASP announced its intentions to relocate its headquarters to Jurisdiction C in Europe (a jurisdiction which had not yet introduced a comprehensive AML/CFT regime in relation to VAs and VASPs at the time). Later in November 2018, Jurisdiction C introduced certain regulations on VASPs, and in February 2020, it confirmed that no authorisation was given to the corresponding VASP to operate. More recent reports in 2020 indicated that the VASP had already relocated its registration and domicile status to Jurisdiction D in Africa.

Source: Public domain

Conclusion

17. This Report is drawn from extensive input by FATF Members across the global network, and seeks to provide a practical tool for both the public and private sectors in identifying, detecting, and ultimately preventing criminal, ML, and TF activities involving VAs.

18. The indicators included in this Report are specific to the inherent characteristics and vulnerabilities associated with VAs. They are neither exhaustive nor applicable in every situation. The indicators are often just one of many elements contributing to a bigger overall picture of potential ML or TF risk and it is important that the indicators (or any single indicator) not be viewed in isolation. They should be contextualised with information obtained from relevant authorities.

19. A risk-based approach implemented with a regular and dynamic two-way dialogue between the public and private sectors would no doubt enhance the effectiveness of this Report. Competent authorities are therefore encouraged to disseminate this Report to reporting entities, and to conduct engagement and awareness-raising sessions with them to promote their understanding of this Report.

20. While the indicators identified are constantly evolving, they are best used when applying other contextual information from domestic law enforcement and public sources. Competent authorities may also provide private sectors with the indicators and information most relevant for that jurisdiction. For example, using the information in this Report to prepare their own advisories to relevant reporting entities. However, this Report should not be intended for use as a regulatory tool for compliance and examination purposes, or as a checklist when supervising private sector institutions as not all indicators are applicable to all jurisdictions or all institutions.

References

FATF (June 2014), FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks

FATF (June 2019), FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

FATF (June 2020), 12-month Review of Revised FATF Standards – Virtual Assets and VASPs

Reports restricted to FATF Members

FATF (June 2016), Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators

FATF (June 2019), Confidential FATF Report on Financial Investigations Involving Virtual Assets

www.fatf-gafi.org

September 2020

Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing

Virtual assets and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities

The FATF has prepared this brief report on red flag indicators associated with virtual assets to assist reporting entities, including financial institutions, designated non-financial businesses and professions, and virtual asset service providers, in identifying and reporting potential money laundering and terrorist financing activity involving virtual assets.