VIRTUAL ASSETS –

RED FLAGS AND INDICATORS

GUIDANCE FOR FINANCIAL INSTITUTIONS

NOVEMBER 2020

I. PURPOSE, SCOPE, AND APPLICABILITY

- This guidance paper issued by the Central Bank of Bahrain ("CBB") should be read in conjunction with local and international standards. The guidance included in this paper is applicable to all licensees regulated and supervised by the CBB.

- This paper aims to provide guidance to the private sector in terms of monitoring and reporting suspicious activities concerning the misuse of Virtual Assets ("VA") or Virtual Assets Service Providers ("VASPs") for ML/TF purposes, in addition to potential red flags and indicators of ML/TF.

- The term "Virtual Assets ("VA")" and "Virtual Asset Service Providers ("VASPs")" used in this guidance paper has the same meaning as "Crypto-assets" and "Crypto-asset licensees" respectively. All licensees regulated and supervised by the CBB are required to take note of the applicability of this guidance paper irrespective of the terms used.

- This guidance paper was developed by consolidating relevant information applicable to financial institutions included in guidance papers issued by the Financial Action Task Force ("FATF"), including 'Virtual Assets – Red Flag Indicators' issued in August 2020, and 'Virtual Assets: What, When, How?'.

- This paper summarises the trends, red flags, and indicators of how VAs and VASPs can be misused by money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. However, all financial institutions are strongly urged to comprehensively read all FATF issued guidance papers.

II. INTRODUCTION

The term **virtual asset** ("VA") refers to the digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Moreover, a **Virtual Asset Service Provider** ("VASP") means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer[1] of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Virtual assets have many potential benefits. They could make payments easier, faster, and cheaper; and provide alternative methods for those without access to regular financial products. But without proper regulation or monitoring, they risk becoming a virtual safe haven for the financial transactions of criminals and terrorists.

[1] In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

III. TRENDS

- 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 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.

- The types of offences associated with VAs include the following:

  - Money laundering ("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
  - Terrorist financing ("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 the use of VAs as one of their means to transfer, collect, or layer proceeds.

- The aforementioned types of offences are specific to the nature of VAs and their associated financial activities, and are by no means exhaustive.

IV. RED FLAG INDICATORS

The following points contain a collection of red flag indicators of suspicious VA activities or possible attempts to evade law enforcement detection. The presence of a single indicator may not necessarily raise a suspicion, but could warrant further monitoring and examination.

I. **Red Flag Indicators Related to Transactions:** The use of VAs for ML purposes first emerged over a decade ago, but VAs are becoming increasingly mainstream for criminal activity more broadly. The following set of indicators (in relation to size and frequency of transactions) demonstrates how red flags, which are traditionally associated with transactions involving more conventional means of payment, remain relevant to detecting potential illicit activity related to VAs:

- 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, either in a short succession, or in a staggered and regular pattern;
- 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, or
  - converting the VAs to multiple types of VAs without logical business explanation, or
  - withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.; and
- Accepting and depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

II. **Red Flag Indicators Related to Transaction Patterns:** 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:*** Red flags involving initial deposits of new users include, but are not limited to, the following:
  - 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 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; and

- 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.

– ***Transactions concerning all users:*** Red flags involving new and existing users include, but are not limited to, the following:

- 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 either 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 the transactions with no logical business explanation); and
- 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.

III. **Red Flag Indicators Related to Anonymity:** 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:

– Transactions by a customer involving more than one type of VA, despite additional transaction fees;
– Moving a VA that operates on a public, transparent block chain, such as Bitcoin, to a centralised exchange and then immediately trading it for an anonymity enhanced cryptocurrency ("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 another customer's behalf, and charge higher fees to their customers than transmission services offered by other exchanges;
– 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 dark-net marketplaces;
- Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including dark-net 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 dark-net or other similar software that allows anonymous communication, including encrypted emails and VPNs;
- Transactions between partners using various anonymised or 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 are linked to possible fraud or other tools aimed at implementing fraudulent schemes;
- Receiving funds from or sending funds to VASPs whose CDD or know-your-customer ("KYC") processes are demonstrably weak or non-existent; and
- Using VA ATMs/kiosks despite the higher transaction fees and those commonly used by mules or scam victims, or in high risk locations where increased criminal activities occur.

IV. **Red Flag Indicators about Senders of Receipts:** This set of indicators is relevant to the profile and unusual behavior of either the sender or the recipient of the illicit transactions.

- ***Irregularities observed during account creation:*** Red flags involving unusual patterns during account creation include, but are not limited to, the following:

    - 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; and
    - 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:*** Red flags involving unusual patterns during the CDD process include, but are not limited to, the following:

  - 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; and
  - Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

- ***Profile:*** Red flags involving the customer's profile include, but are not limited to, the following:

  - 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; and
  - A customer is known, via publicly available information, to law enforcement due to previous criminal association.

- ***Profile of potential money mule or scam victims:*** Red flags involving potential money mule or scam victims include, but are not limited to, the following:

  - 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 are often used by drug dealers to assist them in their trafficking business; and
  - 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.

- ***Other unusual behavior:*** Red flags relating to other unusual behavior include, but are not limited to, the following:

    - 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.

V. **Red Flag Indicators in the Source of Funds or Wealth:** 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, dark-net 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),
- The use of illicit funds for purchasing VAs via cash deposits into credit cards;
- Deposits into an account or 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.; and
- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

VI. **Red Flag Indicators Related to Geographical Risks:** The following indicators must be taken into consideration when evaluating the 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; and
- Customer sets up offices in or move 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.

V. EVALUATING SUSPICIOUS ACTIVITIES

- 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. Therefore, the risks posed by their customers, products, and operations, as well as the presence of conventional risk indicators must be considered. Red flag indicators should always be considered in context.

- 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.

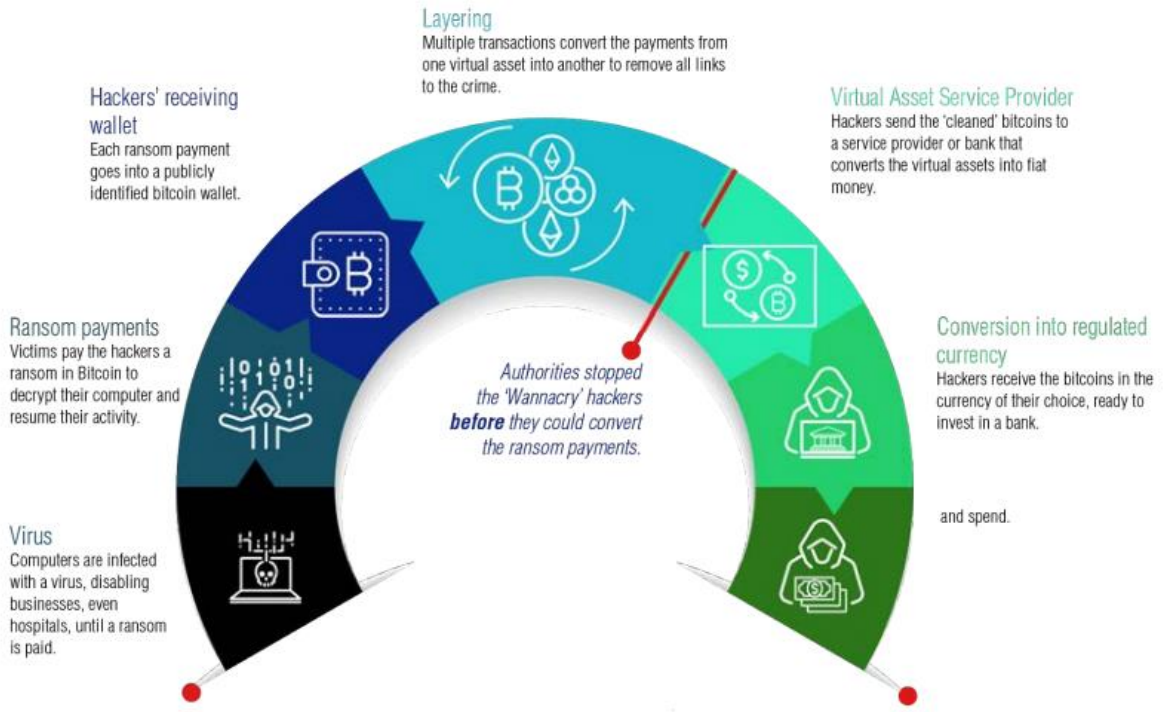
- When evaluating potential suspicious activity, it is important to note that red flag indicators might be more readily observable during general transactional monitoring, while others may be more readily observable during transaction-specific reviews. The observation of one or more of the indicators 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. These indicators should not be the sole determinant of whether or not a Suspicious Transaction Report ("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.

- 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.

VI. HOW CRIMINALS MAY MISUSE VIRTUAL ASSETS

- Below is an example on how criminals and/or terrorists may misuse virtual assets. The example is based on the 2017 Wannacry ransomware attack, where thousands of computer systems were held hostage until the victims paid hackers a ransom in bitcoin. The cost of the attack went far beyond the ransom payments, and resulted in an estimated USD 8 billion in damages to hospitals, banks and businesses across the world. Other ransomware attacks have taken place since and seem to be on the rise.[2]



[2] FATF, 'Virtual Assets: What, When, How?', n.d.

VII. CONCLUSION

- The indicators included in this guidance paper 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) are not viewed in isolation.

- In order to minimise the risk of possible misuse by money launderers and terrorist financiers, VASPs are strictly reminded of their obligation to implement the same preventive measures as financial institutions, including, but not limited to, customer due diligence measures, record keeping and reporting of suspicious transactions, as well as obtaining, holding and securely transmitting originator and beneficiary information when making transfers. More specifically, VASPs must securely and confidentially transmit customer information when sending a payment to another VASP.

- FIs and VASPs are strictly reminded that it remains imperative to implement and maintain effective systems and controls to ensure that the Kingdom's financial system is not abused for money laundering or terrorist financing purposes.