VANUATU FINANCIAL SERVICES COMMISSION

VIRTUAL ASSET SERVICE PROVIDERS & INITIAL TOKEN OFFERING RISK ASSESSEMENT

NOVEMBER 20, 2025

VANUATU FINANCIAL SERVICES COMMISSION
PMB 9023, PORT VILA

Foreword

The Vanuatu Financial Services Commission (VFSC) is pleased to present this risk-assessment report for Virtual Assets Service Providers (VASPs) operating in Vanuatu. As the modern regulatory landscape for digital assets evolves, it is essential that VFSC and Vanuatu as a whole maintains a clear understanding of the money-laundering (ML), terrorist-financing (TF), and other financial-crime risks that VASPs may introduce, or are exposed to. This Risk Assessment Report provides a comprehensive analysis of those risks, evaluates the adequacy of existing controls, and offers practical recommendations to strengthen the resilience of Vanuatu's financial system.

This document is a pivotal step in Vanuatu's commitment to aligning with international standards, particularly those set forth by the Financial Action Task Force (FATF). It provides a detailed analysis of the threats and vulnerabilities linked to VAs and Initial Token Offerings (ITOs), offering guidance to regulated entities on implementing robust Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) measures.

By identifying red flag indicators, assessing sectoral risks, and outlining compliance obligations, this Risk Assessment serves as both a strategic tool and a regulatory compass. It empowers VASPs and Issuers of Initial Token Offerings (IITOs) to navigate the complexities of digital finance with prudence, transparency, and accountability. Moreover, it reinforces Vanuatu's resolve to remain a trusted and competitive hub for financial services in the Pacific region.

The VFSC extends its gratitude to our international partners, and the dedicated VFSC team that prepared this Risk Assessment. We hope this document will serve as a valuable resource for policymakers, industry participants, and other stakeholders as we work together to foster innovation while safeguarding the integrity of Vanuatu's financial industry. Together, we can build a resilient and secure virtual asset ecosystem that supports economic growth, protects consumers, and upholds the highest standards of financial integrity for Vanuatu.

Mr. Branan Karae
Commissioner
Vanuatu Financial Services Commission

VANUATU

Risk Assessment for Virtual Asset Service Providers & Issuers of Initial Token Offerings in Vanuatu

Table of Contents

Acronyms

AML/CFT	Anti-Money Laundering and Combatting the Financing of Terrorism
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FIAMLA	Financial Intelligence and Anti-Money Laundering Act
FIAMLR	Financial Intelligence and Anti-Money Laundering Regulations
FATF	Financial Action Task Force
FDLA	Financial Dealers Licensing Act
VFSC	Vanuatu Financial Services Commission
ITO	Initial Token Offering
IITOs	Issuers of Initial Token Offerings
IP	Internet Protocol
KYC	Know Your Customer
ML/TF	Money Laundering and Terrorism Financing
NRA	National Risk Assessment
FIU	Financial Intelligence Unit
PEPs	Politically Exposed Persons
PII	Personally Identifiable Information
RBA	Risk-Based Approach
STR	Suspicious Transaction Reporting
TFS	Targeted Financial Sanctions
UN	United Nations
UNSC	United Nations Security Council
VA	Virtual Asset
VAs	Virtual Asset Act

VASPs	Virtual Asset Service Providers
VFSC	Vanuatu Financial Services Commission

1 INTRODUCTION

The Vanuatu Financial Services Commission, (the "VFSC") is established under the Vanuatu Financial Services Commission Act No. 39 of 1993 (the "VFSC Act") and is mandated to regulate the non-bank financial services and other business sectors. The VFSC is, by virtue of `Virtual Asset Service Providers Act No.3 of 2025, responsible for regulating and supervising of Virtual Assets Service Providers ("VASPs") and Initial Token Offerings ("ITOs").

The VFSC continues to be committed to the fight against money laundering and terrorist financing (ML/TF), as well as the financing of proliferation and other related threats to the integrity of the Vanuatu financial system. In this regard, VFSC has conducted its first overall Virtual Assets (VA) and Virtual Assets Service Providers (VASP) risk assessment as part of the Vanuatu National Risk Assessment (NRA), and in consideration of the FATF recommendations to protect Vanuatu's financial system from misuse.

In recent years, VAs have slowly gained legitimacy, and many investors have begun to diversify in opportunities for VA-related investment. The popularity and public adoption of VAs in Vanuatu and elsewhere has generated significant ML/TF threats and threats to the Vanuatu Financial system related to Vas have also grown. Hence, Vanuatu's obligation to conduct a risk assessment of VA and VASP has increased in urgency to prevent abuse of its financial system.

This VA and VASP ML/TF risk assessment is done by VFSC as part of the overall NRA of Vanuatu which is critical in developing Vanuatu's Virtual Asset and digital financial technology sector.

Vanuatu commits to becoming a frontier of integrity, prudence, and fortitude in preserving its reputation with a fully compliant international financial sector and protecting its citizens.

This risk assessment is intended to compliment the National Risk Assessment (NRA) on VA which will not only assess the country's exposures but set directions to have adequate mitigants in place to incite good legitimate VASP businesses to continue to flow in the country. The VA Risk Assessment reinforces and introduces new areas of assessment, such as the emerging risks related to the rapid development in the use of VAs and the new players providing services connected with it.

The result of the NRA will guide the country to adopt a cutting-edge framework to regulate VAs and VASP activities and to help the financial services industry attract new clients and, in turn, contribute further to Government revenue while incentivising innovative entities to invest and operate from Vanuatu at a time where investment is needed the most.

2. PURPOSE

2.1 The VA and VASP Risk Assessment is established to:

- provide an outlook on the significance of ML/TF risks associated with Virtual Asset ("VA") activities; and

- guide VASPs and IITOs with an understanding of their specific AML/CFT compliance obligations under the Virtual Asset Service Providers Act.

3. EFFECTIVE DATE

3.1 The VASP Risk Assessment shall be taken into account in the drafting of the National Risk Assessment

3.2 The VASP Risk Assessment may be subjected to regular amendments or updates with a view to reflect changes at the level of the domestic and international regulatory landscape, including the market dynamics of the VA sector, in or from Vanuatu.

4. BACKGROUND OF VIRTUAL ASSET SERVICE PROVIDERS ACT NO. 3 OF 2025

4.1 The VASP Act No.3 of 2025, that was passed in Parliament on 26 March 2025 and came into force on 12 May 2025, provides a comprehensive legislative framework for VASPs and ITOs in line with the international standards of Financial Action Task Force ("FATF") with respect to managing, mitigating and preventing any ML/TF risks relating to VASP businesses.

4.2 The Act designates the VFSC as the prudential and supervisory authority, responsible for regulating and supervising the business activities of VASPs and ITOs respectively and the VFIU as the AML/CTF Supervisor.

4.3 Any person carrying out the business activities of a VASP and ITO, in or from within Vanuatu, shall hold a licence, issued by the Commissioner of the VFSC.

4.4 VASPs and IITOs (hereinafter also collectively referred to as "regulated entities") are encouraged to:

- reflect the elements of this Risk Assessment into their internal policies, procedures and controls; and consequently, apply the risks controls inter-alia for the assessment of persons managing, controlling, directing, owning or performing key functions within their entities.

5. DEFINITIONS AND TERMINOLOGIES

5.1 The FATF, via its Recommendation 15 and relevant interpretative notes issued thereunder, requires countries to ensure that VASPs are regulated for AML/CFT purposes, licensed, or registered and subject to effective systems for monitoring and ensuring compliance with the measures therein.

5.2 VASPs and other financial Institutions that engage in VA-related activities, are required to identify, assess, and take effective actions to mitigate their ML/TF risks.

5.3 For any additional information, in that respect, please refer to the following link.

Virtual Asset FATF Guidance:

https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

5.4 A VA is a digital representation of value that can be digitally traded or transferred and may be used for payment or investment purposes. VA does not include digital representations of fiat currencies, securities, and other financial assets that fall under the purview of the Financial Dealers Licensing Act or any other laws that are already covered by the FATF Recommendations.

5.5 The VA should have an inherent value to be traded or transferred and used for payment or investment or, is a means of recording or representing ownership of assets.

5.6 Virtual Asset Service Provider:

A VASP means a person that, as a business, conducts one or more of the following activities or operations, for, or on behalf of, another person:

- Exchange between VAs and fiat currencies.
- Exchange between one or more forms of VAs;
- Transfer of VAs; (In the context of VAs, transfer means to conduct a transaction on behalf of another person that moves VAs from one VA's address or account to another)
- Safekeeping and/or administration of VAs or instruments enabling control over VAs; and
- Participation in, and provision of, financial services related to an issuer's offer and/or sale of a VAs.

5.7 Section 11 of the Virtual Asset Service Providers Act No. 3 of 2025 provides for the different classes of VASP licence that may be issued by the VFSC:

- Class D – To authorized the exchange between virtual assets and fiat currencies or exchange between one or more virtual assets;
- Class D.1 – To authorise the transfer of virtual assets;
- Class D.2 – To authorise the safe keeping of virtual assets or enabling control over virtual assets
- Class D.3- To authorise the participation in and provision of the financial business related to both or either issuer offer and sale of virtual assets;
- Class D.4 – To authorise a bank to operate the exchange between virtual assets and fiat currencies and their safekeeping of the virtual assets or enabling control over virtual assets.

6. INITIAL TOKEN OFFERING ("ITO")

6.1 ITO refers to an offer for sale to the public, by an Issuer of Initial Token Offering (IITO) of a virtual token in exchange for fiat currency or another VA.

6.2 ITO is a means of raising funds for projects through innovative and digital platforms.

6.3 ITO involves persons who participate in, or provide financial services related to issuers' offer and/or sale of VAs through activities.

6.4 Such persons may be affiliated or unaffiliated with the issuer undertaking the ITO in the context of the issuance, offer, sale, distribution, ongoing market circulation and trading of a VA.

7. NATIONAL RISK ASSESSMENT ("NRA")

7.1 Vanuatu has conducted its NRA with respect to the VA sector in 2024. This NRA exercise relied upon the McDonnel -Nadeau Consultants and the risk assessment tool based on the FATF methodology.

7.2 The NRA once concluded, will enable for the identification and evaluation of the associated ML/TF threats and vulnerabilities with VAs/VASPs through a sectoral approach.

7.3 At the time of the assessment, the overall ML/TF residual risk associated to VAs/VASPs was considered to be "High" after the consideration of mitigating measures.

7.4 The combined ML/TF vulnerability ratings indicated a general tendency of "moderate to High" vulnerabilities driven by factors such as the nature and complexity of the VASP businesses, country risks, customer types, products and services of the VA ecosystem and their operational features (for instance, anonymity, speed of settlement and whether the VASPs were registered).

7.5 The combined ML/TF threat ratings indicated a general tendency of "Medium to High" threats driven by factors, such as the nature and profile of VAs, their sources of funding, the ease with which VA channels are accessible to criminals and their economic impacts.

7.6 VASPs and ITOs must ensure to consider any relevant findings of the NRA when conducting their business risk assessments.

8. SIZE SECTOR

8.1 According to data from Chainalysis, the global cryptocurrency market capitalisation grew from $1.3 Trillion in January 2019 to as high as $3.8 Trillion in October 2023.

8.2 SE Asia is second biggest region for crypto trading.

8.3 There are no specific data on the volume of the VA business in Vanuatu at the time of this report.

9. RED FLAG INDICATORS (ML/TF)

9.1 This section depicts the salient ML/TF red flag indicators which are associated with VAs. This will enable regulated entities licensed under the VASP Act to better identify and prevent the ML/TF risks linked with their business activities and also, to set up adequate controls to mitigate those risks.

9.2 VAs have certain characteristics such as their global reach, capacity for rapid settlement, ability to enable Peer-to-Peer ("P2P") transactions, and potential for increased anonymity and obfuscation of transaction flows and counterparties that have created new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities.

9.3 The following paragraphs provide a summary of red flag indicators which indicate suspicious VA activities. The presence of such indicators should raise further monitoring, examination, and reporting, as appropriate, by regulated entities under the VASP Act.

9.4 VA products/services that facilitate pseudonymous or anonymity-enhanced transactions pose significantly higher ML/TF risks since they can obstruct the ability of regulated entities to access beneficial ownership information, implement effective Customer Due Diligence ("CDD") and apply other appropriate AML/CFT measures.

9.5 The VA ecosystem has witnessed the rise of anonymity-enhanced cryptocurrencies, mixers and tumblers, decentralised platforms and exchanges, privacy wallets, and other similar types of products.

10. ANONYMITY

The below non-exhaustive red flag indicators demonstrate how criminals can make use of technological features associated with VAs that increase anonymity.

10.1 Customers prepared to pay additional transaction fees for one or more types of VAs with technological features providing higher anonymity.

10.2 Customers entering the digital platforms of VASPs and IITOs using an Internet protocol (IP) address that allows anonymous communication such as the Onion router, I2P or IP associated with a darknet.

10.3 Receiving funds from or sending funds to VASPs and IITOs with weak or non-existent CDD or Know Your Customer ("KYC") requirements.

10.4 The use of decentralised/un-hosted, hardware or paper wallets to transport VAs across borders. Decentralised VA systems are particularly vulnerable to anonymity risks compared to a centralised system where some risks are mitigated.

10.5 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.

10.6 Abnormal volume of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.

10.7 VA vendors, which facilitate VA activities via terminals, present higher risk, if the machine or kiosk is located in a high-risk area and used for repeated small transactions.

11. TRANSACTIONS

The below non-exhaustive list of indicators demonstrates how red flags traditionally associated with transactions involving more conventional means of payment, remain relevant in detecting potential illicit VA-related activities.

11.1 Structuring of VA transactions (e.g., exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.

11.2 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 are particularly common in ransomware cases related to VAs or to a newly created or to a previously inactive account.

12. TRANSACTION PATTERNS

The non-exhaustive list of indicators below further illustrates how the misuse of VAs for ML/TF purposes could be identified through irregular, unusual, or uncommon patterns of transactions.

12.1 Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile.

12.2 Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit on 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.

12.3 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.

12.4 Making frequent transfers of large amounts 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; or from the same IP address by one or more persons.

12.5 Conducting VA-fiat currency exchange at a potential loss.

13. SENDERS OR RECIPIENTS

The non-exhaustive indicators listed below relates to the profile and unusual behaviour of either the sender or the recipient of the illicit transactions including irregularities observed during account creation and CDD process.

13.1 Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.

13.2 Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.

13.3 Sender/recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.

13.4 A customer provides identification or account credentials shared by another account.

13.5 Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.

14. SOURCES OF FUNDS OR WEALTH

Below are some additional and common red flags, which are related to the source of funds or wealth, resulting from criminal activities, in the context of VAs:

14.1 Transacting with VA addresses that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.

14.2 VA transactions originating from or destined to online gambling services.

14.3 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 that were recently deposits into credit cards.

14.4 Deposits into 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.

14.5 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 ITO 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.

14.6 A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.

14.7 Bulk of a customer's source of wealth is derived from investments in fraudulent VAs or ITOs.

14.8 A customer's source of wealth is disproportionately drawn from VAs or Virtual Tokens originating from other VASPs or IITOs that lack AML/CFT controls.

15. GEOGRAPHY

This set of non-exhaustive red flag indicators stress on how criminals, when moving their illicit funds, can take advantage of the varying stages of implementation across jurisdictions.

15.1 Criminals can potentially exploit the gaps in AML/CFT regimes which are applicable to the VA sector, by moving their illicit funds to VASPs or IITOs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations.

15.2 Moving VAs or funds through jurisdictions that may not have a licensing/registration regime or have not extended Suspicious Transaction Reporting ("STR") requirements to cover VA activities or may not have otherwise introduced the full spectrum of preventive measures.

15.3 Regulated entities which provide financial and other services that are related to VAs (including the issuance of ITOs) or have customers involved in VAs, should therefore consider the salient vulnerabilities, as described in this section of the Guidance Notes, and assess whether the ML/TF risks can be mitigated and managed appropriately.

15.4 However, these red flag indicators are constantly evolving and should not be viewed in isolation but should rather be considered in context.

15.5. These areas/examples are furthermore not exhaustive. Every VASP or IITO will accordingly have unique circumstances and contexts that will determine its exposure to ML/TF risks. It will ultimately be necessary to make its own informed decision.

16. SECTORS INHERENT RISK CHARACTERISTICS

This set of non-exhaustive red flag indicators stress on how criminals, when moving their illicit funds, can take advantage of the varying stages of implementation across different sectors of the economy:

16.1 Complexity of sector's structure and integration with other regulated sectors. Virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments.

16.2 The virtual assets ecosystem also evolves rapidly as occasioned by decentralised technology and business models which have resulted in the multiplicity of participants, products and services in the virtual assets space.

16.3 Decentralised Finance (DeFi) uses emerging financial technology based on secure distributed ledgers for P2P banking.

16.4 Mixing and tumbling service providers whose sole aim is to obscure the trail of cryptocurrency.

16.5 Non-custodial/unhosted/decentralised wallets that make it difficult to trace or scrutinise transactions.

16.6 A growing number of ATMs/kiosks where cryptocurrencies can be bought using bank cards or cash.

16.7 NFTs which are irrevocable digital certificates of ownership and authenticity for a given digital or physical asset

17. VASPs MAY HAVE INTERGARATION WITH THE FOLLOWING SECTOR:

17.1 Designated Non-Financial Institutions

These include:

- Dealers in Jewellery,
- Cars and Luxury Goods,
- Precious Stones and Metals,
- Real Estate, Estate Developers,
- Estate Surveyors and Valuers,
- Estate Agents,
- Chartered Accountants,
- Audit Firms,
- Tax Consultants,
- Clearing and Settlement Companies,
- Hotels,
- Casinos,
- Supermarkets,
- Dealers in Mechanized Farming Equipment and Machineries,
- Practitioners of Mechanized Farming,
- Non-Governmental Organizations)

Globally, it is possible to purchase physical services and products like cars, houses, electronics, jewellery and luxury items, etc. with cryptocurrency.

17.2 Money and value transfer services:

Traditional e-money and payment firms have the capacity to facilitate cryptocurrency exchange

17.3 Financial institutions

Inherently, virtual assets are well connected with financial institutions globally as assets are traded with or for fiat through banks

17.4 Banking sector:

Although VA activities offer an alternative to traditional banking activities, banks can be involved in VA activities directly as investors or indirectly through their products, services, or customers. Because of these exposures and the possibility of providing custody services for customers, including holding unique cryptographic keys associated with accessing private wallets, the banking sector is brought into the exercise. The banking sector may be interacting with VA activities as it could provide a non-resident business banking platform through the Companies and Trust Service Providers (CTSP), which could provide complex corporate structures that may be involved as a VA service provider overseas.

17.5 The non-banking financial sector:

The nature of services and products in the sector makes it attractive to VASPs that could be set up as International Companies (IC) and take advantage of the absence of a VASP licensing process in the country. Their trading activities in VA may take place on platforms operating outside of Vanuatu's regulatory perimeter (or, as in one case, failing to comply with applicable laws and regulations) and see the opportunity to harness the unregulated market in Vanuatu. Although there is caution from VFSC on VASPs, some types of VA services are already being provided by ICs without a license.

17.6 Gaming Sector:

The development of VA has spread into the online gambling industry, and AML/CFT supervisors worldwide are not sufficiently equipped to conduct inspections of the online platform. The anonymity and decentralisation of such playing platforms are on the rise. There is also a surge in the popularity of VA games through decentralised apps built on the Ethereum network allowing users to purchase in-game items with Bitcoin, Ether or other VAs and to earn a game-specific VA through gameplay and to withdraw the VA they earned in-game for use elsewhere. Many online gambling services do not require KYC and CDD information.

17.7 DNFBP:

Under the VASP Act, DNFBPs that send, receive, and store VA are required to be licensed and supervised by the VFSC.

18.SCOPE OF LOCATION OF OPERATION OF THE SECTOR

18.1 Virtual Assets (VAs) and Pseudo-anonymous Exchange VAs.

These VAs are used as a means of exchange or a store of value and have high transactional and exchange liquidity which make them attractive to ML/TF/PF criminals.

Transactions with such VAs are traceable and balances are openly verifiable.

With the right tools and skillset, they can be linked to an entity's real-world identity.

However, anonymity can still be enhanced with anonymization tools like mixers and tumblers.

19. THESE VA TYPES ARE PRONE to ML/TF/PF ABUSE.

These VA types are designed to offer increased anonymity to users by default. With such VAs, it is impossible to trace and assess the transactions and balances of users; this makes them potentially attractive to ML/TF/PF criminals, criminals may be sceptical about using anonymous exchange VAs because only a few major exchanges offer to trade them (hard to off ramp).

19.1 Stablecoins:

- These are VAs whose market values are pegged to some external reference like the value of some fiat currency (USDC or Tether) and commodities like gold
- Asset backed stablecoins are less volatile than other VAs and potentially attractive to ML/TF/PF criminals. However, because stable coins are issued and monitored by governing entities, they are less prone to ML/TF/PF abuse.

19.2 Security Tokens:

- These are also known as ownership tokens and are usually offered through Security Token Offerings (STO's)
- They are a tokenized share of an asset -typically a share of a business but also represent ownership of real estate and other assets that have been verified on the blockchain.
- While ML/TF/PF criminals might view security tokens as an opportunity to layer illicit funds, they may still be unattractive due to their low liquidity

19.3 Utility Token:

- These tokens give holders access to special services or preferential treatments within an ecosystem.
- These tokens can also be swapped for other tokens, cryptocurrencies, or fiat.
- These tokens carry AML/CTF risk if KYC is not performed

19.4 Non-fungible Tokens (NFTs):

- These are blockchain-based tokens that represent unique assets like pieces of art, digital contents, or media.
- Recently, there has been a rising interest in NFT trading globally
- NFTs offer ML/TF/PF criminals the opportunity to purchase artifacts with illicit funds and sell them off later
- ML/TF/PF criminals may not find NFTs attractive since the artefacts are non-fungible and may be difficult to sell because potential buyers have to find it valuable before purchasing it.
- The blockchain technology also makes the purchase and sale of NFTs detectable because the marketplaces are centralised
- These limitations can be circumvented by:

  (1) self-laundering where an individual purchases an NFT with illicit funds and sells and resells to him/herself to show patronage on the blockchain
  (2) the use of non-custodial wallets for on the NFT marketplace

- Currently, there are attempts to develop decentralised NFT marketplaces (for example, Unique. One and Sologenic) which is expected to increase its ML/TF/PF vulnerabilities.

20. VASP SERVICES

Globally, VASPs offer diverse products and services to their clients since these products/services are available without borders over the internet.
While there is no agreed-upon categorisation for these products and services, based on FATF's definition of VASPs, and the VA value chain, the following products and services were considered:

20.1 Initial Coin offering (ICO)/Initial Exchange Offering issuance (IEO):

- With this service, the VASP matches prospective buyers with companies who want to raise funds to float a coin, an app or a service.
- This service is considered unattractive to ML/TF/PF criminals because it takes a while for the proposed coin, app or service to be floated

20.2 Custodial Wallets:

- Custodial wallet services are provided by VASPs to receive, safe keep and transfer VAs (which are potentially illicit or high-risk) on behalf of their clients.
- While these wallets provide ML/TF/PF criminals with an opportunity to store and move illicit funds, it is becoming less attractive due to three main reasons:

  (1) The service providers typically have KYC and CDD procedures and can freeze their funds or censor their transactions when necessary.

(2) Law enforcement agencies can bring down a wallet service provider and deny ML/TF/PL criminals access to the VAs.

(3) The advent of unhosted/non-custodial wallets make it possible for users to safe keep and administer their VAs themselves; it also makes it more difficult for transactions to be traced.

20.3 Centralised Exchange services:

- With this service, VASPs facilitate the exchange between virtual assets and fiat currencies, i.e., VA-to-VA, Fiat-to-VA and or VA-to-Fiat trades
- Globally, this is the most developed and patronised service in the VA world
- According to global reports –the growth rate re the number of global crypto users will reach the 1 billion marks by the end of 2023.
- Centralised exchanges offer cryptographically secure transactions thus pseudonymising the users and transactions-a feature that ML/TF/PF criminals find attractive
- With such service and the inherent complexity offered by VASPs, value can be structured in amounts that will not trigger AML identification and reporting requirements. Value can also be transferred across the globe in milliseconds

20.4 Centralised Peer-to-peer exchange services:

- Unlike in centralised exchange services where the VASPs act as the middlemen, peer-to-peer exchanges facilitate direct trade between two intending parties
- This service has become popular especially in jurisdictions where crypto trading is banned or not encouraged
- These services provide the traders or users with anonymity, especially when the exchange involves fiat, and this increases its vulnerability to ML/TF/PF abuse
- Global centralised peer-to-peer exchange service providers, demand KYC, can limit volumes of transactions, and ban suspected accounts
- Furthermore, bank transfers are needed to complete VA-fiat exchanges and they may be reported as suspicious transactions.
- These make them less attractive to ML/TF/PF criminals who would want to exchange huge sums without leaving traces.

20.5 Brokerage Services:

A Brokerage service provider offers three main kinds of services:

A. They allow traders to deposit collateral in exchange for various derivate products and trading opportunities including leverage positions, automated trading (dependent on the specific broker).

- This line of brokerage service provides ML/TF/PF criminals with an opportunity to invest in different VA types and to store illicit funds.

B. They make it possible for institutional and high net worth clients to exchange or liquidate large volumes of VAs at a set negotiated prices thus avoiding any loss associated with slippage.

- Chainalysis observed that brokers offering such service have less stringent KYC requirements than exchanges and some specialise in providing money-laundering services to criminals.

C. They facilitate trade between individual buyers and sellers when they don't want or cannot transact on an open exchange.

- This is also prone to abuse by ML/TF/PF criminals especially in collaboration with willing brokers.

20.6 Centralised NFT Marketplaces:

- These are platforms where NFTs can be minted, stored, displayed and/or traded.

- VASPs providing this service can act both as value custodians and value exchangers.

- Many NFT marketplaces do not require KYC, and they can allow the use of non-custodial wallets to purchase NFTs and to receive funds after the sale of NFTs.

This makes it very difficult to trace and assess such transactions and provides ML/TF/PF criminals an avenue to store and move illicit funds.

20.7 Anonymization services:

- Popularly known as coin mixers tumblers or mixers, they are used specifically to obscure transaction flows and to make VASP clients more anonymous.
- They allow users to split their funds into small parts and rewire them through thousands of micro transactions, sometimes into and out of a comingled pool to a new address, thereby making it difficult for anyone to follow the cryptocurrency.
- This service is attractive to ML/TF/PF criminals as it keeps their activities hidden from relevant authorities.

21. DECENTRALIZED APPLICATIONS AND FINANCING

- These refer to applications or financial services that operate on the blockchain with no central server or controlling entity.

- These services are like those discussed in the previous sections but without a controlling entity. As they are just software, powered by smart contracts and running on the blockchain, they cannot be considered as VASPs. However,

where an entity maintains control or sufficient influence on a DeFi arrangement, it should be considered a VASP.

22. VA ATMs

- These are devices or kiosks where VAs can be bought with fiat.
- It is potentially vulnerable to abuse by ML/TF/PF criminals because of the anonymity it provides. However, VA ATM service providers impose transaction limits which may make the service less attractive to ML/TF/PF criminals.

23. NATURE OF BUSINESS RELATIONSHIP WITH CLIENTS

- Globally, VASPs are vulnerable to ML/TF/PF abuse because of the borderless reach of their services even into the dark web, the different types of clients, and the difficulty in linking a client to the accounts that s/he may have across multiple VASPs.
- VASPs deal with retail and institutional clients; these institutional clients may be other VASPs, for example, brokers.
- Furthermore, the nature of the relationship with these clients depends on the type of VASP.
- VASPs that offer centralised services have established relationships with their clients, while those who provide decentralised services may have occasional relationships.
- Based on transaction volume, Chainalysis categorised VA clientele into:
    - Large institutions (transacts more than $10 million)
    - Institutions (transacts between $1 -$10 million)
    - Professional (transacts between $10,000 -$1 million)
    - Large retail (transacts between $1,000 - $10,000)
    - Small retail (transacts less than $1,000)

24. CUSTOMER STATUS

- VASP customers can be natural persons, legal persons or legal arrangements.
- To combat ML/TF/PF, Vanuatu must ensure that VASPs have CDD processes that meet global standards and domestic legal requirements, including clients' occupation or business:
    - VASPs services are diverse and borderless, thus are open to people of different professions and businesses.
- Geographic reach of sectors activities:
    - High risk jurisdictions:
    - Generally, VASPs have a global reach and are accessible from high-risk countries/jurisdictions

25. NATURE OF DELIVERY CHANNELS:

25.1 Anonymity:

- Inherently, VA transactions involving VASPs that offer centralised services are pseudo-anonymous; but with the right tools and skillset, they can be linked to the VASPs, and the entities involved.

- However, anonymity is increased when the transactions are executed over decentralised platforms, involves unhosted wallets, or passes through mixers/tumblers. These make it even more difficult for relevant authorities to track and assess when required.

25.2 Complexity of delivery channels:

- The delivery channels of Virtual assets are predominantly indirect (over the internet) and may involve intermediaries (where brokers are involved).

For VA-Fiat transactions, the fiat leg of the transaction can be completed using the internet/mobile banking. Peer-to-peer transactions can also be completed using fiat and value moved from one jurisdiction to another with ease.

26. THREATS AND VULNERABILITIES

This part looks at the Threat and Vulnerability of both VAs and VASPs. The approach uses a unique and relatively complex logic based on information gathered, and weighted averages in the assessment model. The assessment considers intermediate and input variables of threats and vulnerabilities from a domestic and international perspective ranging from large multinational VA providers with extensive customer bases to small VA businesses and a host of different types of VAs.

26.1 The Overall Threat Level

The overall ML/TF threat of VA and VASP in Vanuatu is considered as **High** due to illegal activities being carried out by an unlicensed entity on one of the islands. The number of licensed VASPs domiciled in Vanuatu is zero when this report is made.

26.2 Vanuatu's High level of ML/TF threats to VA and VASP is also due to the nature of the products that prevails in the international businesses. Although Vanuatu is currently not listed on the FATF list of non-cooperative jurisdiction, its inherent threat still persists since there is still a lack of robust financial and human resources, adequate training and sophisticated technology-based systems for combating ML/TF risks associated with VA and VASP. The lack of capacity of prosecutors and investigators for VA ML/TF matters and the absence of a

national strategy to combat VA ML/TF also contribute to Vanuatu's high threat level.

26.3 The investigations and successfully prosecutions of the unlicensed VA related case are still ongoing. The FIU, has not received any VA related STRs, hence the magnitude of the threat is assumed to be high.

Threats Analysis

27. VA NATURE AND PROFILE

27.1 Anonymity and pseudonymity (*Threat level: High*)

Vanuatu has recently enacted its VASP Act No.3 of 2025. The comprehensive legislative provides the legal basis for VASPs, ITOs and VASP sandbox to be licensed in the jurisdiction. The Act also provides for supervisory oversight of the licensed entities. Although the legal requirements are in place the possibility of Anonymity and pseudonymity still exists that criminals could still take advantage of.

27.2 (*Threat level: High*)

The unique characteristics of VA, coupled with the international financial activities in Vanuatu, may offer a conduit of cross-border transfer to high-risk jurisdictions as an input asset or output asset, or in the form of payment to individuals and entities who would not use the traditional system to conduct such transfer. The NRA has not uncovered activities at the peer-to-peer, but there is a threat that VA transfers could be happening on the internet outside the scrutiny of Vanuatu authorities in payment forms across frontiers by the high-profile foreign individuals or nationals from high-risk countries residing and/or operating businesses in Vanuatu. More extensive assessment needs to be carried out by Vanuatu authorities on the mechanism to transfer the VA's ownership (for example, centralised, peer-to-peer, decentralised, DeFi) and control over the ledger (for example, open to the public, open to specific parties, close to a limited number of authorised parties). These would assist in managing these threats and prevent the country from harbouring sanction circumvention.

27.3 Absence of face-to-face control (***Threat level: High***)

The absence of face-to-face is inherent in Vanuatu’s international financial activities, and the degree of anonymity/pseudonymity and the peer-to-peer transferability without proper monitoring present a high threat that non-face-to-face activities could lead to transactions

with high-risk individuals or entities, transfer of value, or undertaking third-party funding through virtual exchanges. Hence, VA-related activities represent a growing ML/TF threat.

27.4 Traceability (*Threat level: High*)

Blockchain technology provides transparency and traceability for all transactions. Nevertheless, an actor's true identity may never be known if the travel rule is not implemented. Although there are no obligations from Vanuatu authorities on the unlicensed VASPs to implement the 'travel rule', there are several attributes that law-enforcement agencies may use to trace users and uncover anonymity. These could be through unique Internal Protocol (IP) addresses and transaction history through blockchain forensics. VAs can be analysed through different criteria to understand their ML/TF risks. Nevertheless, VAs carry significant ML/TF threats due to the unavailability of dedicated tools at Vanuatu' disposal to effectively and efficiently traced VAs on the blockchain.

27.5 Speed of transfer (*Threat level: High*)

Although transactions involving VAs are, in most cases, quickly verified and permanently recorded on distributed ledgers publicly, the ability to send large volumes of value across borders is very much easier than through traditional financial institutions. With no control over the size and value that can be transferred, the system is vulnerable to abuse by criminals or unscrupulous actors. Also, the vulnerability is enhanced due to the lack of tools and training for law enforcement in Vanuatu to trace a financial transaction through a public ledger. The lack of potential to trace, monitor, and detect suspicious criminal activity encourages 'speed transfer' by service operators. The threat of evading investigations and probing from competent authorities is high.

Accessibility to Criminal

28. MINING BY CRIMINAL (Threat level: High)

VA markets is underpinned by various forms of intermediation without any KYC obligations that are outside the radar of regulators and law enforcement agencies and offer an attractive environment to criminals to exploit vulnerabilities in the ecosystems. The rise of centralised mining pools of VA permissionless blockchains could give rise to cryptojacking. The unlicensed VASPs offering applications for mining globally and in Vanuatu are a growing threat,

especially with the lack of computer security awareness and the lack of dedicated internet security policing by competent authorities. It should be noted that many cryptojacking enterprises are taking advantage of the scalability of cloud resources by breaking into cloud infrastructure and tapping into an even broader collection of computing pools to power their mining activity. Today, attackers are targeting cloud services by any means to mine more and more VAs, as cloud services can allow them to run their calculations on a larger scale than just a single local machine.

29. COLLECTION OF FUNDS (*Threat level: High*)

VAs have become magnets for illicit activities such as theft and fraud, and given the nature of VAs, there is a possibility that VAs might be used to fund terrorism or terrorist attacks more efficiently than is done today with fiat currencies. VAs might aid terrorists in the receipt of funding through various means. Supporters of extremist groups might donate their own VAs or use VAs to transfer funds through broker intermediaries. Funds could be collected through crowdfunding, a convenient way for the terrorist organisation to supply funding to the attacker.

30. TRANSFER OF FUNDS (*Threat level: High*)

As per the assessment of the nature and profile of VA, the transfer of money to high-risk regions where terrorist groups may operate could be an attractive medium as it is the same for individuals and entities under sanctions. These threats are consistent with the input variable, such as the 'Absence of face-to-face control' and 'Speed of transfer' indicated above. This input variable is perceived as very high.

31. DARK WEB AND DARKNET ACCESS (*Threat level: High*)

The existence of some VASPs operating through darknet market operations on platforms with greater anonymity, offered VAs as the preferred form of payment for illicit items or procurement of restricted or sanctioned items usually acquired for criminal activities. The service providers offer Web that relies on encrypted services to shield users' identifying information and communications.

32. EXPENDITURE OF FUNDS (*Threat level: High*)

The threat that criminals may integrate dirty money into new technologies that support the VA ecosystems. Given that many actors are exploring opportunities in the VA market for radical innovation and entrepreneurship in financial solutions without relying on government and central authorities, these mediums may encourage criminals to come on board to integrate dirty money with the least worry of being tracked by legal authorities.

Source of funding VA

33. BANK OR CARD AS THE SOURCE OF FUNDING VA (*Threat level: High*)

VASP platforms with insufficient AML/CFT controls may be more attractive to criminal proceeds where the source of VA funding could be tied to illegal activities.

34. CASH TRANSFERS, VALUABLE IN-KIND GOODS (*Threat level: High*)

The absence of Travel Rules enforcement and technological solutions for tracing transfers, especially for VAs that could be financed through proceeds of crime and those with unhosted wallets, could expose Vanuatu to high-risk VA activities. The country could also be exposed to a rise in thefts of valuable goods as the market for non-fungible tokens (NFTs) grows. The problem is that anyone can “mint” a digital file as an NFT, whether they have rights to it in the first place, as the process is anonymous.

35. USE OF VIRTUAL CURRENCY (*Threat level:* Low)

VAs is not legal tender in Vanuatu, however Vanuatu is currently being used as a safe haven by an unlicensed VASPs, trading in NFTs. All VA transaction is being carried out offshore.

Operational features of VA

36. REGULATED (Threat level: Medium)

The ICs are regulated entities in Vanuatu that fall within the ambit of AML/CFT under the FIU Act, but the threat for the country is that these entities provide services outside of Vanuatu. The VFSC’s regulatory powers could be limited and may not far-reaching, to enforce the laws

in a foreign jurisdiction. At this moment all licensed VASPs must have a physical presence in Vanuatu as required by the law.

37. DECENTRALISED ENVIRONMENT (*Threat level: High*)

Unhosted wallets and Decentralised Finance (DeFi) are the medium of the VA ecosystem aiming to reduce or eliminate transaction intermediaries through decentralised computer networks. The system works without intermediaries like VASPs, and banks. There is also NFT which operates through smart contracts.

Ease of Criminality

38. EVASION (Threat level: High)

This is a high threat for Vanuatu, where an unlicensed VASPs could be abused for activities that may generate illicit financial flow.

39. TERRORIST FINANCING (*Threat level: High*)

Although cases of terrorist financing through VA are not seen, the threat of this method of financing does exist especially when considering the 'absence of face-to-face control (High)', 'speed of transfer (High)' and unregulated sector (High), increases the exposure to other input variables.

40. DISGUISING CRIMINALPROCEEDS TO UNREGULATED VA (*Threat level: High*)

VA could be used as a means to facilitate cybercrime, ransomware, and other digital extortion activities. Ransomware perpetrators use VA as a preferred means of ransom payment, and they would use unrelated VASPs to assist them in converting to other forms of VA or fiat money.

41. TRACE AND SEIZE DIFFICULTIES (*Threat level: High*)

This is consistent with the input variable of 'Traceability' noted above, where blockchain inherent features provide the opportunity for law-enforcement agencies to trace and seize. However, the task is complicated as special blockchain forensics tools are required, and Vanuatu also lacks dedicated Blockchain specialists within law enforcement to successfully carry out this function.

42. CIRCUMVENTION OF EXCHANGE CONTROL (*Threat level: Medium*)

The threat of existing or unknown VASPs in Vanuatu could or may be involved in facilitating circumvention of exchange control overseas where this restriction exists and hence undermine government authority by circumventing capital controls imposed by it.

Economic Impact

43. UNDERGROUND ECONOMY – IMPACT ON THE COUNTRY'S MONETARY POLICY (*Threat level: High*)

Most VAs are within the control of private entities who may influence the money supply through market capitalisation and disturb Vanuatu's monetary policy. The threat is also high due to lack of or absence of law enforcement measures and other interventions that could make VAs more likely to be adopted on a Peer-to-Peer basis and encourage tax evasion domestically. As far as VASPs are concerned, their VA services may become attractive to countries where the size of the underground economy is huge or where confidence in monetary policy is low. Vanuatu may unwittingly offer a prospective appeal to criminals through unlicensed VASPs without passing a fit and proper test.

44. ALLOW FULL INTERGRATION WITH THE FINANCIAL SERVICES MARKET (*Threat level: High*)

As seen from the input variable above, the anonymity and cross-border reach of VAs raise genuine concerns from a financial integrity standpoint. As VAs can be used to conceal or disguise the illicit origin or sanctioned destination of funds, thus facilitating ML/TF and the evasion of sanctions, the threat is that VA may offer the layering and integration stages of ML in cyber-related criminal activity.

45. ABSENCE OF A HIGH LEVEL OF ACCOUNTABILITY OF PRODUCT PROVIDERS (*Threat level: High*)

The threat is high as the level of the inherent ML/TF risks of Vanuatu is also high because of the absence of dedicated law enforcement specialist to carry out the investigations. Also, the jurisdictions where the unlicensed VASPs operate may not have well-developed AML/CFT frameworks. The level of accountability also diminishes with the rise of

DeFi platforms where intermediaries are called to play a lesser role and hence the challenge for law-enforcement agencies to freeze, seize and confiscate illicit VAs

46. THE OVERAL VULNERABILITY

The overall national vulnerability for Vanuatu is rated **"High"** This is because the sector, although not huge, but it's being abused by an unlicensed VASP, offering VA services outside the VFSC's purview. Although the VASP is being assisted by a licensed CTSP and a reporting entity in Vanuatu and is subject to AML/CFT requirements under the AML Act, their VA activities are outside the scope of what VFSC and the FIU are mandated to supervise and regulate.

47. OVERALL VULNERABILITY EXPOSURE *(Vulnerability level: High)*

Vanuatu so far has not licensed any VASPs, however there is an unlicensed VASPs offering services in and outside of Vanuatu. At this point in time no other VASPs is being traced to be operating in Vanuatu. The existing legislative framework does not allow any unlicensed VASP to transact, domicile or operate from within Vanuatu. Also, the existing law does not allow players providing company services or securities (FDLs) and other investment services to operating as VASPs. In this context, it is practically possible for the VFSC to assess the fitness and propriety of the persons applying for a VASPs license and assess their knowledge and measures concerning ML/TF risk. However, given that we have an unlicensed VASPs operating in Vanuatu, it poses a risk where criminals from overseas may resort to using the unregulated VASP with weak AML/CFT controls to hide their illicit proceeds.

48. NATURE, SIZE, AND COMPLEXITY OF BUSINESS *(Vulnerability level: High)*

There is an unlicensed VASP domiciled in Vanuatu, attracting numerous risks to the finance sector with complex business structures and offering most, if not all, the products and services of VA. Given the above complexities and the borderless nature of VAs, it is possible that the unlicensed VASP is currently operating without imposing the Travel Rule requirements to identify customers that can be associated with ML/FT, and whether the size and nature of business do allow for ML/TF risks being adequately identified and managed on a risk-based approach. Based on the above, the Nature, Size, and complexity of business is assessed as having a very high level of vulnerability.

49. PRODUCTS/SERVICES (Vulnerability level: High)

The vulnerability of the VASPs depends on their services with varying high-risk characteristics such as NFTs, DeFi platforms, privacy coins being offered by the service providers, such as the unlicensed VASPs

providing NFTs products, that enable or allow for reduced transparency and increased obscurity of financial flows. The services could also be provided by some through the Darknet market. Considering their business activities, business model, delivery channels, customer profiles, the level of governance and the assessment of ML/TF risks, the products/Services is assessed as high vulnerability.

50. METHODS OF DELIVERY OF PRODUCTS/SERVICES *(Vulnerability level: High)*

The internet-based nature of VA activities, the non-face-to-face method and the offering of NFs, DeFi products through exchanges as a delivery method may be attractive to criminals, PEPs and high-net-worth individuals. These could offer a conduit to allow payments to be received from unknown or un-associated third parties. Also, exposure to Internet Protocol (IP) anonymisers may further obfuscate transactions or activities and inhibit a VASP's ability to know their customers and implement effective AML/CFT measures.

There is no assurance that enhanced due diligence measures and Recommendation 16 are in place to mitigate the potentially higher risks associated with the factors mentioned above. Based on these factors, the methods of delivery of products/services is assessed as high vulnerability.

51. CUSTOMER TYPES (Vulnerability level: High)

The VASP sector tends to be at a very high risk of exposure to criminals and organised crime, and the sector is considered attractive to this type of customer due to its reduced transparency. Terrorist financing risk is also significant - terrorist organisations, their supporters, and sympathisers are also continually looking for ways to raise and transfer funds without detection or tracking by law enforcement. As the service providers mostly operate in the offshore sector, it is very unlikely that Recommendation 12 is being applied as part of risk management systems to determine whether customers or beneficial owners are foreign politically exposed persons or related or connected to a foreign politically exposed person. And whether measures to establish the source of funds and wealth are carried out wherever relevant. On that basis, customer types are assessed as high vulnerability.

52. COUNTRY RISK (Vulnerability level: High)

The VASP sector has significant exposure to higher-risk jurisdictions through internet channels as it is borderless. Most VASPs offer their services globally, and are unsupervised (such as the Satoshi Island in Vanuatu) and may have limited or no AML/CFT obligations. Also, the VA sector is very new, and many of the operators are not familiar with the AML/CFT compliance measures and may be offering their products and services in jurisdictions deemed as high risks or listed on the

international sanctions and embargo list. It is also much easier for the unlicensed VASPs to conduct transactions with countries having significant levels of organised crime, corruption, or other criminal activity or countries where illegal drugs, human trafficking, smuggling, and illegal gambling are rife. The VASP vulnerability in relation to country risk is assessed to be high.

53. INSTITUTIONS DEALING WITH VASP *(Vulnerability level: High)*

Given the size of the transfer made by the unlicensed Vanuatu domiciled VASPs, the number of non-VASPs actors could be massive. It is noted that millions of transfers were made to this VASPs. With the above observations, the level of risk in relation to institutions dealing with VASPs is rated as highly vulnerable.

54. VA (ANONYMITY/PSEUDONYMITY) *(Vulnerability level: High)*

The unlicensed VASPs is offering VA with enhanced anonymity and also offering privacy coins and citizenship. As already established with the threat variables above, these VAs are attractive to criminals and make it harder for law-enforcement agencies to successfully trace the private key and the holder. Consistent with the rating of the threat of VA, this risk of anonymity/ pseudonymity is also assessed as highly vulnerability.

55.RAPID TRANSACTION SETTLEMENT *(Vulnerability level: High)*

The transactions in VAs are executed rapidly due to the elimination of interbank payments and settlements. With the rise of stablecoins, the vulnerability of Rapid Transaction Settlement is considered very high and is consistent with the speed of transactions threat identified for VA above.

56. DEALING WITH UNREGISTERED VASPs FROM OVERSEAS *(Vulnerability level: High)*

The unlicensed VASPs in Vanuatu sits at the intersection between the anonymity of VA transactions and operating without overseas regulatory scrutiny and authorisation. Regulators in advanced economies may not be able to trace or investigate this unauthorised VASPs operation, hence this variable is assessed as high.

57. AML/CFT COMPLIANCE OBLIGATIONS

This final section outlines the key AML/CFT compliance obligations to be observed by VASPs and IITOs once/after being licensed or registered, as appropriate, under the Virtual Asset Act.

58. STATUS OF (VASPs/ITOs) AS REPORTING ENTITIES

It is critically important to emphasise that, with the coming into force of the Virtual Asset Act the AML act will be amended to enable for the categorisation of VASPs and IITOs as 'Reporting entities.

By virtue of this status, VASPs and ITOs will be required to be compliant with AML/CFT obligations similar to any other 'financial institutions' under the AML Act

59. AML/CFT RISK-BASED APPROACH ("RBA")

59.1 Against the backdrop of the foregoing and specific ML/TF risks, vulnerabilities and threats for the VA sector, it is therefore compelling for VASPs and ITOs, which are licensed or registered under the Virtual Asset Service Providers Act, to systematically apply a RBA whenever considering to establish or continue business relationships with other VASPs and IITOs, customers involved in VA activities or other outsourced/third parties, in general.

The application of a RBA provides a strategy for VASPs and IITOs to manage potential risks by enabling them to subject customers to proportionate controls and oversight.

59.2 A key component of their RBAs will entail that they should:

(i) Identify areas where their products/services could be exposed to ML/TF risks; and
(ii) Take appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures, and controls.

59.3 VASPs and ITOs should apply the RBA properly and should not resort to the wholesale termination or exclusion of business relationships within their sector or operations, without an appropriately targeted risk assessment.

59.4 The documented risk assessments that are necessary to be undertaken pursuant to relevant sections of the Act, Regulations or guidelines, will, in fact, support VASPs and ITOs in developing their RBAs.

59.5 A risk assessment should typically take into account all of the risk factors that the VASP or ITO consider relevant, including the types of services, products, transactions or technologies involved; customer risks; geographical factors; types of VAs traded, among other factors.

59.6 A VASP or ITO must, inter alia, under relevant section of the AML Act identify, assess, understand, and monitor ML/TF risks for its customers.

59.7 As stressed in the Guidance Notes (and pursuant to relevant section of the AML act) a VASP or ITO shall also take into account the findings of the NRA for appropriate guidance in the adoption of its business risk assessment.

59.8 Any risk assessment systems undertaken by 'VASPs and ITOs" should be further reviewed regularly to ensure an effective system is in place and swift action should be taken to remedy any identified deficiencies.

60. CUSTOMER DUE DILIGENCE (CDD)

60.1 VASPs and ITOs should maintain accurate and up-to-date customer information. This would include scrutinising their source of funds and wealth.

60.2 Pursuant to relevant section the VASP Act and the AML Act, VASPs or ITOs have the obligation to identify their customers, and where applicable, their beneficial owners and then verify their identities, which is essential for the prevention of ML/TF.

60.3 CDD is effectively the only means by which regulated entities under the Virtual Asset Service Providers Act will achieve knowledge on background information on their customers and is a key element of any internal AML/CFT system.

60.4 VASPs and ITOs must collect the relevant CDD information when they provide services to or engage in VA-related activities for or on behalf of their customers.

60.5 The CDD should help VASPs and ITOs, as well as other obliged entities that engage in VA-related activities in assessing the ML/TF risks associated with such activities.

60.6 This process comprises of identifying the customers and, where applicable, the customers' beneficial owner(s) and also understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations.

60.7 As far as occasional transactions are concerned, following consequential amendments made in the AML ACT, a VASP is required to:

(i) apply CDD measures in respect to an occasional transaction in an amount equal to or above 1000 US dollars or an equivalent amount in foreign currency where the exchange rate to be used to calculate the US dollar equivalent shall be the selling rate in force at the time of the transaction, whether conducted as a single transaction or several transactions that appear to be linked; and

(ii) record, in respect to an occasional transaction in an amount below 1000 US dollars, the name of the originator and the beneficiary; and the virtual asset wallet address for each or a unique transaction reference number.

61. CDD IN LINE WITH THE AML/CTF ACT

61.1 VASPs and ITOs are also expected to conduct CDD in line with the requirements of the AML act and in addition:

A. All identification documents secured through the CDD measures should be retained by VASPs and ITOs for a period of at least 6 years as required by the AML Act.

B. The inadequacy or absence of satisfactory CDD measures can subject a VASP or ITO to serious customer and counterparty risks, as well as reputational, operational, legal, and regulatory risks, any of which can result in significant financial cost to its business.

C. VASPs and ITOs must consider, on a regular frequency, the risks that all such relationships pose to them and the manner in which those risks can be limited.

61.2 The extent of the ongoing CDD measures applied by VASPs and ITOs should be determined on a risk-sensitive basis.

61.3 However, VASPs and ITOs should be aware that as a business relationship develops, the ML/TF risks may change.

62. ENHANCED DUE DILIGENCE ("EDD")

62.1 Due to the potential for increased anonymity or obfuscation of VA financial flows and the challenges associated with conducting effective supervision and CDD, including customer identification and verification, VA activities may be regarded as posing higher ML/TF risks that may potentially require the application of monitoring and EDD measures, where appropriate.

62.2 VASPs and IITOs will, pursuant to Parts 4, 5 and 6 of the AML/CTF Act No.13 of 2014, be required to implement internal controls and other procedures to combat ML/TF, including EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat ML/TF. Where the ML/TF risks are identified to be higher, a financial institution shall take EDD measures to mitigate and manage those risks.

62.3 VASPs and ITOs should also apply the requirements of Section 12 of the AML/CTF Act N0. 13 of 2014 with respect to their business relationships with Politically Exposed Persons ("PEPs").

62.4 In case where a VASP or IITO is not able to undertake the required EDD, the latter shall terminate the business relationship and file a suspicious transaction report under section 20 of the AML/CTF Act No. 13 of 2014.

62.5. Transaction Monitoring and Suspicious Transaction Reporting

62.6 The transaction recording of VA transactions is often linked to, or based on, Distributed ledgers.

62.7 VASPs and IITOs are required to develop, implement, and maintain effective transactional monitoring systems to determine the origin of a VA and to monitor its destination, and to apply strong KYC measures that enable detection of possible ML/TF activities.

62.8 VASPs and IITOs are expected to act responsibly and always be vigilant in ensuring that their business activities are not subject to any misuse by participants transacting with VAs and to report any suspicious activity.

62.9 Where a VASP or IITO identifies any suspicious activity or has reasonable ground to suspect that a transaction is suspicious in the course of a business relationship or occasional transaction, it should, pursuant to Section 20 of the AM/CTF Act No.13 of 2014

a) file a suspicious activity report to the FIU

b) cease to carry on business relationship with the person.

62.10 The reporting procedures, as outlined above, must also apply to prospective customers and transactions that were attempted but that did not take place.

63. TRAVEL RULE (FATF Rec 16)

63.1 The requirements of 'Travel Rule', as recommended by FATF for VASPs, that is, the obligation to obtain, hold, and transmit required and accurate originator and beneficiary information, as the case may be, immediately and securely, when conducting any virtual asset transfers has further been provided under the Virtual Asset Service Providers Act.

63.2 The Travel Rule (FATF REC 16) requirements also extend to a financial institution, acting as intermediary, when sending or receiving virtual asset transfers on behalf of a customer as they would have applied to a VASP.

63.3 Section 27 of the VASP Act expressly provides that an originating VASP shall not execute a transfer of a VA where the required and accurate information, as the case may be, has not been obtained.

64. USE OF SOFTWARE

64.1 VASPs would be expected to make use of relevant software to:

(i) Perform robust due diligence or KYC process on counterpart institutions.

(ii) Identify counterparty wallet type (pre-transaction);

(iii) Identify risk-related details about the beneficiary through blockchain analytics and sanctions screening providers.

(iv) Allow to safely send or receive encrypted customer's Personally Identifiable Information ("PII") through various messaging protocols.

(v) Store encrypted customer's PII for up to seven years; and

(vi) Allow to generate reports to the VFSC on a timely basis, upon request.

65. ONSITE INSPECTION

65.1. In accordance with Section 51of the VASP Act, VFSC is required to conduct ongoing onsite inspection on VASPs and ITO to ensure that the regulated entities are compliant with the law and are aware of any changes in the development of a business relationship.

66. TARGETED FINANCIAL SANCTIONS ("TFS")

66.1 The UNSA provides the legal framework for the implementation of UN sanctions as adopted by the UNSC under Chapter VII of the UN Charter. VASPs, ITOs or any other financial institution engaged in VA-related activities are required to ensure compliance with the United Nations Sanctions Act No.6 of 2017 (UNSA).

66.2 In line with section 16 of the UNSA No. 6 of 2017, VASPs and ITOs are required to implement internal controls and other procedures to effectively comply with their obligations thereof. As such, VASPs and IITOs should establish effective and up-to-date systems to screen clients and transactions appropriate to the nature, size, and risk of the business in accordance with the UN Sanctions List and list of designated parties issued by the National Sanctions Secretariat.

66.3 The screening system should enable VASPs and IITOs to maintain an up to date understanding of its clients through the life cycle of the client relationship and, whenever a client's identification data changes. Screening should be undertaken when establishing a new relationship at and subsequently, regular but sufficiently frequent intervals, and upon trigger events (for instance when there is a change in directorship or ownership) and when the UN and/or domestic sanctions lists are updated.

66.4 Sanctions apply to all clients and transactions, and there is no minimum financial limit or other threshold to conduct screening. VASPs, IITOs or other financial institutions engaging in VA-related activities should ensure that they are screening clients and transactions relating to VA transfers to ensure compliance with their TFS obligations.

66.5 The ordering and beneficiary institutions should screen their customer's name for compliance with TFS obligations at the time of on-boarding (and upon name changes).

66.6 The beneficiary's name (the name of the person who will own the virtual asset on completion of a transfer as per Virtual Asset Act) or the originator's name (with 'originator' having the same meaning as in the Virtual Asset Act) should also be screened when conducting the VA transfer.

66.7 Considering the nature of VAs, illicit actors may abuse VASPs for sanctions evasions. Therefore:

- Each incoming and outgoing transaction should be screened for a potential match with the sanctions lists; and
- The screening should be focused on the transaction where detection of sanctions risk is actionable, where a transaction can be stopped and funds are frozen, if required, and before a potential violation occurs.

66.8 For a VASP and IITO to transmit the required information (i.e. on the originators and beneficiaries) to another VASP and IITO, as the case may be, it is necessary to identify their counterparty VASP. A VASP and IITO would also need to conduct due diligence on their counterparty VASP/IITO before they transmit such information to avoid dealing with illicit actors or sanctioned actors unknowingly.

66.9 VASPs and IITOs should have adequate procedures to swiftly identify whether name matches are a true match and for freezing assets, where appropriate.

66.10 If a match is detected and if a VASP and IITO, as a reporting person, maintains accounts, or otherwise holds or controls funds and other assets of listed and designated parties (or any person who holds, controls or has in his custody or possession any funds or other assets of a designated or listed party or acting on behalf of or, at the direction of a designated or listed party), it should immediately, without delay and within 24 hours:

- not deal with those funds and other assets, pursuant to section 11 of the UNSA No.6 of 2017.
- not make those funds and other assets available to or for the benefit of designated and listed parties available in accordance with section 12 of the UNSA; and
- investigate further and take necessary measures in line with the relevant sections of the UNSA, alert senior management, report to the FIU and the VFSC (section 16 of the UNSA), and file a STR (section 20 or 21 of the AML/CTF Act) In line with section 16 of the UNSA,