Financial Services Commission
MAURITIUS

FINANCIAL SERVICES COMMISSION

AML/CFT Guidance Notes for Virtual Asset Service Providers & Issuers of Initial Token Offerings

Issued on 28 February 2022

Table of Contents

Acronyms

AML/CFT	Anti-Money Laundering and Combatting the Financing of Terrorism
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FIAMLA 2002	Financial Intelligence and Anti-Money Laundering Act 2002
FIAMLR 2018	Financial Intelligence and Anti-Money Laundering Regulations 2018
FATF	Financial Action Task Force
FSC	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
PEPs	Politically Exposed Persons
PII	Personally Identifiable Information
RBA	Risk-Based Approach
STR	Suspicious Transaction Reporting
UNSA 2019	United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
VAs	Virtual Assets
VAITOS Act 2021	Virtual Asset and Initial Token Offering Services Act 2021
VASPs	Virtual Asset Service Providers

1.0 INTRODUCTION

1.1 The Financial Services Commission, Mauritius (the "FSC") is established under the Financial Services Act 2007 (the "FSA") and is mandated to regulate the non-bank financial services and global business sectors. The FSC is, by virtue of section 5 of the Virtual Assets and Initial Token Offering Services ("VAITOS") Act 2021, responsible for regulating and supervising Virtual Assets Service Providers ("VASPs") and Issuers of Initial Token Offerings ("IITOs").

1.2 The Guidance Notes are issued by the FSC pursuant to its powers under Section 7(1)(a) of the FSA.

1.3 The Guidance Notes set out the measures which entities regulated under the VAITOS Act 2021 should apply for the prevention of Money Laundering and Terrorism Financing ("ML/TF") during the course of their business and operations.

1.4 The provisions of the Guidance Notes should be read in conjunction with the VAITOS Act 2021, the Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA 2002"), the Financial Intelligence and Anti-Money Laundering Regulations 2018 ("FIAMLR 2018") and the FSC's Anti-Money Laundering and Combatting the Financing of Terrorism ("AML/CFT") Handbook.

1.5 Terms used in these Guidance Notes shall, unless otherwise specified, have the same meaning as under the relevant Acts.

2.0 PURPOSE

2.1 The Guidance Notes are established to:

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

2.1.2 guide VASPs and IITOs with an understanding of their specific AML/CFT compliance obligations under the VAITOS Act 2021.

3.0 EFFECTIVE DATE

3.1 The Guidance Notes shall take effect as from 28 February 2022.

3.2 The Guidance Notes may be subject 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 Mauritius.

4.0 BACKGROUND OF VAITOS ACT 2021

4.1 The VAITOS Act 2021, which came into force on 7 February 2022, provides a comprehensive legislative framework for VASPs and IITOs in line with the international standards of Financial Action Task Force ("FATF") with respect to managing, mitigating and preventing any ML/TF risks.

4.2 The VAITOS Act 2021 designates the FSC as the prudential and AML/CFT supervisory authority, responsible for regulating and supervising the business activities of VASPs and IITOs respectively.

4.3 Any person carrying out the business activities of a VASP and IITO, in or from Mauritius, shall hold a licence or registration, as appropriate, issued by the FSC.

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

4.4.1 reflect the elements of the Guidance Notes in their internal policies, procedures and controls; and

4.4.2 consequently apply the Guidance Notes inter-alia for the assessment of persons managing, controlling, directing, owning or performing key functions within their entities.

5.0 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 last or updated FATF guidance: A risk based approach to Virtual Assets and Virtual asset service providers issued in October 2021.

5.4 Virtual Asset

5.4.1 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 Securities Act.

5.4.2 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.

5.5 Virtual Asset Service Provider

5.5.1 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:

5.5.1.1 Exchange between VAs and fiat currencies;

5.5.1.2 Exchange between one or more forms of VAs;

5.5.1.3 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)

5.5.1.4 Safekeeping and/or administration of VAs or instruments enabling control over VAs; and

5.5.1.5 Participation in, and provision of, financial services related to an issuer's offer and/or sale of a VAs.

5.5.2 The Second Schedule of the VAITOS Act 2021 provides for the different classes of VASP licence that may be issued by the FSC.

5.6 Initial Token Offering ("ITO")

5.6.1 ITO refers to an offer for sale to the public, by an IITO of a virtual token in exchange for fiat currency or another VA.

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

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

5.6.3 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.

6.0 NATIONAL RISK ASSESSMENT ("NRA")

6.1 Mauritius concluded its NRA with respect to the VA sector in November 2021. This risk assessment exercise relied upon the World Bank methodology and risk assessment tool.

6.2 The NRA has enabled for the identification and evaluation of the associated ML/TF threats and vulnerabilities with VAs/VASPs through a sectoral approach.

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

6.4 The combined ML/TF vulnerability ratings indicated a general tendency of "High to Very 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).

6.5 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.

6.6 VASPs and IITOs must ensure to take into account any relevant findings of the NRA when conducting their business risk assessments. A copy of the NRA report is available **here**.

7.0 RED FLAG INDICATORS (ML/TF)

7.1 This section of the Guidance Notes depicts the salient ML/TF red flag indicators which are associated with VAs. This will enable regulated entities under the VAITOS Act 2021 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.

7.2 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.

7.3 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 VAITOS Act 2021.

7.4 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.

7.5 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.

7.6 Anonymity

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

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

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

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

7.6.4 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.

7.6.5 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.

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

7.6.7 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.

7.7 Transactions

This second 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.

7.7.1 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.

7.7.2 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.

7.8 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.

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

7.8.2 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.

7.8.3 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.

7.8.4 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.

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

7.9 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.

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

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

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

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

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

7.10 Source 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:

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

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

7.10.3 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 deposits into credit cards.

7.10.4 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.

7.10.5 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.

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

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

7.10.8 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.

7.11 Geography

This last 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.

7.11.1 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.

7.11.2 These jurisdictions 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.

7.12 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.

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

7.14 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.

8.0 AML/CFT COMPLIANCE OBLIGATIONS

8.1 This final section of the Guidance Notes outlines the key AML/CFT compliance obligations to be observed by VASPs and IITOs once/after being licensed or registered, as appropriate, under the VAITOS Act 2021. A VASP and an IITO shall, under section 34 of the VAITOS Act 2021, in carrying out its respective business activities, have measures in place to comply with the Applicable Acts, namely the FIAMLA 2002, FSA and UNSA 2019. They must also comply with the FSC's AML/CFT Handbook.

8.2 Status of (VASPs/IITOs) as Financial Institutions

8.2.1 It is critically important to emphasise that, with the coming into force of the VAITOS Act 2021, the FIAMLA 2002 has been amended to enable for the categorisation of VASPs and IITOs as 'financial institutions'.

8.2.2 By virtue of this status, VASPs and IITOs will be required to be compliant with AML/CFT obligations similar to any other 'financial institutions' under the FIAMLA 2002.

8.3 AML/CFT Risk-Based Approach ("RBA")

8.3.1 Against the backdrop of the foregoing and specific ML/TF risks, vulnerabilities and threats for the VA sector (as detailed in section 7 of these Guidance Notes), it is therefore compelling for VASPs and IITOs, which are licensed or registered under the VAITOS Act 2021, 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.

8.3.2 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.

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

8.3.3.1 Identify areas where their products/services could be exposed to ML/TF risks; and

8.3.3.2 Take appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls.

8.3.4 VASPs and IITOs 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.

8.3.5 The documented risk assessments that are necessary to be undertaken pursuant to section 17 of the FIAMLA 2002 will, in fact, support VASPs and IITOs in developing their RBAs.

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

8.3.6.1 A VASP or IITO must, inter alia, under Section 17(1) of the FIAMLA 2002, identify, assess, understand and monitor ML/TF risks for its customers.

8.3.6.2 As stressed in the Guidance Notes and pursuant to Section 17(2) (b) of the FIAMLA 2002, a VASP or IITO shall also take into account the findings of the NRA for appropriate guidance in the adoption of its business risk assessment.

8.3.7 In accordance with Regulation 31 of the FIAMLR 2018, any risk assessment systems undertaken by 'financial institutions' (including VASPs and IITOs) should be further reviewed regularly to ensure an effective system is in place and swift action should be taken to remedy any identified deficiencies.

8.4 Customer Due Diligence

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

8.4.2 Pursuant to Section 17(C) of the FIAMLA 2002, VASPs or IITOs 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.

8.4.3 CDD is effectively the means by which regulated entities under the VAITOS Act 2021 will achieve such knowledge and is a key element of any internal AML/CFT system.

8.4.4 VASPs and IITOs must collect the relevant CDD information when they provide services to or engage in covered VA activities for or on behalf of their customers.

8.4.4.1 The CDD should help VASPs and IITOs, as well as, other obliged entities that engage in VA activities in assessing the ML/TF risks associated with covered VA activities.

8.4.4.2 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.

8.4.5 Following consequential amendments made to the FIAMLA 2002 under the VAITOS Act 2021, VASPs and IITOs will be, as reporting persons, able to undertake CDD measures by means of such reliable and independent digital identification system, where customers are not physically present.

8.4.5.1 VASPs and IITOs must assess the veracity of the controls inherent within these digital identification systems, in order to determine whether they can place reliance on the results produced, or if additional steps are necessary to complement the existing controls.

8.4.5.2 The FSC's AML/CFT Handbook highlights (at Section 5.10) the steps that should be taken by reporting persons (including VASPs and IITOs) to ensure that the electronic KYC documents are authentic and adequately verify that the customers are who they say they are.

8.4.6 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 section 19 of the VAITOS Act 2021.

8.4.6.1 Section 19(4) of the VAITOS Act 2021 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.

8.4.6.2 The Travel Rule requirements also extend to a financial institution when sending or receiving virtual asset transfers on behalf of a customer as they would have applied to a VASP.

8.4.6.3 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 FSC on a timely basis, upon request.

8.4.6.4 As far as occasional transactions are concerned, following consequential amendments made in the FIAMLA 2002, 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.

8.4.7 VASPs and IITOs are also expected to conduct CDD in line with Regulation 10 of the FIAMLR 2018 and in addition, adhere to compliance obligations as stipulated under Regulation 20 of the FIAMLR 2018.

8.4.8 All identification documents secured through the CDD measures should be retained by VASPs and IITOs for a period of at least 7 years as recommended under Chapter 11 of the FSC's AML/CFT Handbook.

8.4.9 The inadequacy or absence of satisfactory CDD measures can subject a VASP or IITO 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.

8.4.10 VASPs and IITOs 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.

8.4.11 In accordance with Regulation 3(1) (e) (ii) of the FIAMLR 2018, the requirement to conduct ongoing CDD will ensure that the regulated entities under the

VAITOS Act 2021 (i.e. VASPs and IITOs) are aware of any changes in the development of a business relationship.

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

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

8.5 Enhanced Due Diligence ("EDD")

8.5.1 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.

8.5.2 VASPs and IITOs will, pursuant to Regulation 12 of the FIAMLR 2018, 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.

8.5.3 VASPs and IITOs should also apply the requirements of Regulation 15 of the FIAMLR 2018 with respect to their business relationships with Politically Exposed Persons ("PEPs").

8.5.4 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 14 of the FIAMLA 2002.

8.6 Transaction Monitoring and Suspicious Transaction Reporting

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

8.6.2 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.

8.6.3 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.

8.6.4 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 Regulation 28(1) of the FIAMLR 2018:

a) obtain EDD, in accordance with Regulation 12 of the FIAMLR 2018; and

b) make an internal disclosure, in accordance with the procedures provided under Regulation 27 of the FIAMLR 2018.

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

8.6.6 The Money Laundering Reporting Officer should then consider the internal disclosure to assess whether a STR needs to be made to the Financial Intelligence Unit.

Please refer to the **FSC's AML/CFT Handbook** for additional information on AML/CFT obligations.