MAURITIUS

MONEY LAUNDERING/TERRORIST FINANCING RISK ASSESSMENT OF VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

PUBLIC REPORT

FEBRUARY 2022

TABLE OF CONTENTS

Foreword by the Minister of Financial Services and Good Governance

Mauritius has positioned itself as a renowned international financial centre with a robust Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulatory and supervisory framework. Mindful of the dynamic nature of the financial sector and its growing challenges, the jurisdiction has consistently adopted a proactive approach by diligently identifying emerging threats and taking appropriate measures to address them.

In this endeavour, the country has remained staunchly guided by the Financial Action Task Force (FATF) Recommendations. As at date, the jurisdiction is '*Compliant*' or '*Largely Compliant'* with 39 out of the 40 FATF Recommendations.

In addition to the technical compliance upgrades, major reforms were brought to enhance the effectiveness of the AML/CFT regime. Two major factors have contributed to this accomplishment, namely, the political commitment at the highest level, coupled with the engagement of competent authorities enabling Mauritius to make a gigantic leap in consolidating the resilience of its AML/CFT regime. This synergy has also been instrumental in the delisting of the country from the FATF list of "*Jurisdictions under Increased Monitoring*" in October 2021, ahead of the set deadline.

The authorities are alert to new challenges and threats, such as those posed by Virtual Assets (VAs)/Virtual Asset Service Providers (VASPs). The rapid growth of the VAs/VASPs, with its intrinsic Money Laundering (ML)/Terrorist Financing (TF) risks, have been a matter of concern for the FATF and has led to the amendment of FATF Recommendation 15 and the FATF Methodology. These amendments require VASPs to be licenced or registered and be subjected to an effective system of monitoring or supervision for AML/CFT purposes.

Mauritius has, in its quest for maintaining the integrity of its jurisdiction, embarked on a VA/VASP risk assessment exercise in order to identify, assess and understand the ML/TF risks faced by the country in relation to VAs and VASPs. This risk assessment exercise has laid the foundation for the enactment of the Virtual Asset and Initial Token Offering Services Act in December 2021. The Act provides for the Financial Services Commission to regulate and supervise the VASPs and issuers of initial token offerings, and the application of a risk-based approach covering VAs/VASPs activities.

I strongly believe that this risk assessment exercise along with the new piece of legislation, which have been spearheaded by my Ministry, will constitute fundamental tools to guide competent authorities, businesses and financial institutions in their own risk assessment and the implementation of appropriate control measures.

I wish to express my appreciation to all stakeholders for their contribution to this risk assessment exercise, the World Bank and the members of the Risk Assessment Working Group as well as the staff of my Ministry for successfully completing this exercise.

Honourable Mahen Kumar Seeruttun
Minister of Financial Services and Good Governance
February 2022

EXECUTIVE SUMMARY

Virtual Assets (VAs) have grown exponentially over the past few years, with record prices and heightened activity in the VA ecosystem attracting the attention of regulators and other stakeholders. The Financial Action Task Force (FATF), as the global standard-setter for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction, acknowledges both the potential of VAs for financial innovation and their propensity for criminal use through money laundering (ML) and terrorism financing (TF).

This risk assessment stems from the obligations of the FATF Recommendation 15 which requires countries to identify, assess and understand the ML/TF risks emerging from VA activities and the activities or operations of Virtual Asset Service Providers (VASPs). Subsequently, this risk assessment provides the basis for implementing a risk-based approach to ensure that the preventive and mitigating measures are commensurate with the ML/TF risks identified.

Mauritius adopted the World Bank's methodology and tool to identify and assess the combined ML/TF risks of VAs and VASPs in its eco-environment.

Key Findings

1. The World Bank tool provides for 27 VASP channels through which there could be potential interaction with different sectors in Mauritius and the analysis revealed that 12 different VASP channels were applicable to only three sectors (some channels cutting across more than one sector):

   (i) **2 channels for the Banking sector: -**

   - Virtual Asset Exchanges: – Channels: (i) Fiat to Virtual and (ii) Virtual to Fiat;

   (ii) **5 channels for the Non-Bank Financial Institution (NBFI) sector: -**

   - Virtual Asset Wallet Providers: – Channel: (i) Hot wallet;
   - Virtual Asset Management Providers: – Channels: (ii) Fund Management; (iii) Compliance, Audit and Risk Management; and
   - Virtual Asset Investment Providers: – Channels: (iv) Platform Operators, and (v) Investment into VA-related commercial activities.

   (iii) **8 channels for the Informal sector: -**

   - Virtual Asset Wallet Providers: - Channels: (i) Hot wallet; (ii) Cold wallet;
   - Virtual Asset Exchanges: Channels: (iii) Peer-to-Peer; (iv) Platform to Business; (v) Fiat to Virtual; (vi) Virtual to Fiat; (vii)Virtual to Virtual; and
   - Virtual Asset Broking: Channel: (viii) Merchants.

   At the time of the assessment, the Designated Non-Financial Businesses and Professions (DNFBPs) did not interact with any VASP channel.

2. The combined ML/TF threat ratings across the 12 channels show a general tendency of "**Medium to High**" driven by such factors as the nature and profile of VAs, their source of funding, the ease with which VA channels are accessible to criminals and their economic impact.

3. The analysis also revealed that drug trafficking and fraud are the main predicate offences associated with the VA/VASP ecosystem in the jurisdiction.

4. The combined ML/TF inherent vulnerability ratings across the 12 channels show a general tendency of **"High to Very High"** driven by such factors as the nature and complexity of the VASP business, country risk, customer types, the products and services of the VA ecosystem and their operational features – anonymity, speed of settlement and whether the VASPs were registered.

5. The combined ML/TF residual risk ratings across the 12 channels show a general tendency of **"High to Very High"** after considering mitigating measures.

An action plan, with high and medium priority measures, and quick wins, was devised to address among others the regulatory, administrative and operational gaps identified during the assessment so that Mauritius remains a credible and trustworthy international financial centre. The Virtual Assets and Initial Token Offering Services Act was enacted in December 2021.

1. INTRODUCTION

The Global reach of VAs

Over the past years, VAs have grown exponentially. In 2013, there were 66 VAs worldwide[1], and in November 2021, there were 7,557[2]. As of November 2021, the total market capitalization of all crypto assets, including stablecoins and tokens, amounted to almost US$ 2.6 trillion[3] and it is reasonable to expect that this upward trend will continue.

The FATF[4] highlights that '*the monitoring of new and emerging risks, including the risks relating to new technologies, should inform the risk assessment process of countries and obliged entities and, as per the risk-based approach, should guide the allocation of resources; as appropriate to mitigate these risks.'*

As VA transactions are not constrained by geographic boundaries and remain unregulated in many countries, they present enhanced ML/TF risks. In 2019, more than USD10 billion worth of VAs were used for ML purposes.[5] Funds generated by VA-related crimes are estimated to exceed many countries' Gross Domestic Product (GDP), thereby creating an imbalance between the legitimate and illegitimate economies[6] and posing significant challenges for VASPs, supervisors and Law Enforcement Agencies (LEAs).

VAs appear to be here to stay. Some jurisdictions have fragmented VA regulatory regimes, whilst others advocate their outright ban. In June 2021, El Salvador became the first country to accept Bitcoin as legal tender and others, such as Japan and Canada are also moving towards adopting VAs as a method of payment. However, other jurisdictions such as China and South Korea are cracking down on their use.

Regimes vary greatly, depending on how VAs are used. For example, the Inland Revenue Authority of Singapore has stated, "*Businesses that choose to accept digital tokens such as Bitcoins for their remuneration or revenue are subject to normal income tax rules. They will be taxed on the income derived from or received in Singapore. Tax deductions will be allowed, where permissible, under our tax laws*."

[1] Statista, *"Market capitalization of Bitcoin from April 2013 to February 6, 2022*." https://www.statista.com/statistics/377382/bitcoin-market-capitalization/
[2]Statista, *"Market capitalization of Bitcoin from April 2013 to February 6, 2022*." https://www.statista.com/statistics/377382/bitcoin-market-capitalization/
[3] CoinMarketCap, "*Global Cryptocurrency Charts Total Cryptocurrency Market Cap*", https://coinmarketcap.com/charts/
[4] FATF, Updated Guidance for a Risk-Based Approach to, Virtual Assets And Virtual Asset Service Providers, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html
[5] ML/TF Vertical Risk Assessment, *"Virtual Asset Service Providers"*, December 2020, https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf
[6] ESAAMLG *"Domestic Coordination, International Cooperation and Information Sharing in the Eastern and Southern African Anti-Money Laundering Group*" (July 2021)

VA/VASP Ecosystem in Mauritius

Mauritius offers investors the advantages of an international financial centre with a comprehensive AML/CFT legislative and supervisory framework for traditional business activities. However, the VA/VASP sector was not yet regulated at the time of the risk assessment.

VAs can store value, like fiat currency, despite their volatility and complexity[7]. However, their global reach, transaction speed, potential anonymity, the absence of gatekeeping financial intermediaries, and the use of tumbling or mixing services also make them attractive to ML/TF[8].

The Bank of Mauritius (BOM) has been very cautious towards VAs. In December 2013 and August 2017, it warned the public to be extremely careful and diligent when dealing with virtual currencies, to be aware that unregulated ones offer no protection, and that it would not accept responsibility for cryptocurrency losses.

Mauritius has undertaken a number of initiatives to position itself as a sound and competitive Fintech hub within the African region. As a politically stable and forward-looking country of the region, it has proactively responded to the adoption of emergent technologies, such as Blockchain and artificial intelligence, in the financial services sector. The Financial Services Commission (FSC), in particular, recognised VA as an investible asset class for sophisticated investors and professional/expert funds since 2018. The FSC subsequently introduced a bespoke licensing regime for custodians of VAs.

Following the completion of the risk assessment, the Virtual Asset and Initial Token Services Act was enacted in December 2021 to provide a comprehensive legislative framework to regulate and supervise the business activities of different classes of VASPs (such as a market place or exchange, broker-dealer, etc.) and Issuers of Initial Token Offerings (ITOs), in accordance with the international standards to mitigate and prevent identified ML/TF risks.

Mauritius has noted the diverse regulatory stance worldwide to VAs and adopted a phased approach to their regulation.

The future of VAs is not certain and predictions regarding VAs differ widely; some professionals believe that Bitcoin is a bubble about to burst, whilst others believe the price of Bitcoin will keep rising over the coming years.[9] The spectacular price swings of VAs have also attracted investors anxious for returns, particularly in the low-interest rate environment prevailing in recent years.

New or emerging technologies and the innovative use of existing technologies increasingly feature in the financial services sector and potential VA abuse concerns national authorities. Currently, websites advertise informal peer-to-peer VA exchanges in which cash transactions and anonymity feature prominently, and large, uncommercial buy and sell spreads indicate high ML/TF risks. The FATF and Bank for International Settlements (BIS) have set or are now in the process of setting standards for mitigating risks of VAs and VASPs.

---

[7] UK, *National Risk Assessment of Money Laundering and Terrorist Financing 2020*, https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

[8] Financial Stability Institute (FSI) of the Bank for International Settlements (BIS) on policy implementation, "*Supervising cryptoassets for anti-money laundering*", April 2021, https://www.bis.org/fsi/publ/insights31.htm

[9] Mondaq, "*Mauritius: Cryptocurrency - Developments In Mauritius*", 26 March 2018, https://www.mondaq.com/fin-tech/686384/cryptocurrency--developments-in-mauritius

1.1. VA AND VASP DEFINITION

Virtual Asset

According to the FATF, the term 'Virtual Asset' refers to any digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities, and other financial assets.

VAs have unique technological properties that enable pseudo-anonymous and anonymous transactions, fast cross-border value transfer and non-face-to-face business relationships. Those properties have the potential to improve multiple financial products and services such as trade financing, cross-border payments and financial instrument settlement.

International typologies related to VAs show that organised crime organisations may use them to access 'clean cash' (paying in and paying out). Not only cybercriminals use VAs – other organised crime groups such as drug traffickers use them to move and launder the proceeds of crime. VAs allow such groups to access cash anonymously and obscure the transaction trail. Criminals may acquire private keys for e-wallets or withdraw cash from cashpoint machines.

VAs, such as Monero, are designed as privacy coins to obfuscate the identities of the sender, the recipient, and the transaction itself. These VAs directly confront customer due diligence (CDD) measures and therefore are particularly appealing to criminals. Transactions using mixing and tumbling services, infer attempts to obscure illicit funds flows between wallet addresses and darknet markets.

Virtual Asset Service Provider

"Virtual Asset Service Provider," according to the FATF, is a natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets;
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

1.2. OBJECTIVES

In October 2019, the FATF amended its methodology to provide guidance on how to assess requirements relating to VAs/VASPs. Recommendation 15 requires, among others, that countries '*should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.*

This VA/VASP risk assessment contributes towards meeting the requirements of Recommendation 15 to identify, assess and understand the ML/TF risks which the VA/VASP ecosystem could pose for Mauritius. It also aims to:

- inform authorities on the prioritisation and allocation of resources as well as actions to be taken at national and sectoral levels to prevent or mitigate the ML/TF risks identified;
- enhance the understanding of stakeholders on ML/TF risks associated with VA/VASPs in Mauritius; and
- inform the ML/TF risk assessment of regulated entities and their risk management approaches.

2. METHODOLOGY

Mauritius adopted the World Bank's methodology and risk assessment tool to identify and assess the combined ML/TF risks of VAs and VASPs in its eco-environment. The risk assessment identifies and evaluates the ML/TF threats and vulnerabilities of VA/VASPs through a sectoral approach and reaches a residual risk rating after factoring in mitigating measures. As a last step, an action plan is formulated to propose additional mitigating measures to be implemented both at national and sectoral levels.

Establishment of a Risk Assessment Working Group

In accordance with the World Bank methodology, Mauritius established a Risk Assessment Working Group composed of all relevant competent authorities. The working group comprised representatives from the Ministry of Financial Services and Good Governance, the Attorney General's Office (AGO), the Bank of Mauritius (BOM), the Financial Services Commission (FSC), the Integrity Reporting Services Agency (IRSA), the Mauritius Police Force (MPF), the University of Mauritius (UOM), the Financial Intelligence Unit (FIU), the Mauritius Revenue Authority (MRA), the Counter Terrorism Unit (CTU), the Asset Recovery Investigation Division (ARID), the Independent Commission Against Corruption (ICAC), the Mauritius Institution of Professional Accountant (MIPA), the Gambling Regulatory Authority (GRA) and the Registrar of Companies (ROC). Consultations were also held with the private sector, which provided useful data, trends and reflections, for the purpose of analysis and formulation of recommendations for this risk assessment.

Risk Assessment Tool

The key components embedded in the World Bank methodology are described hereunder:

a) Assessment of applicable VASP channels in Mauritius

The starting point is to identify the relevant VASP channels with which the reporting entities, in the different sectors in Mauritius as well as the informal sector, interact. The tool provides for 27 VASP Channels (refer to Table 1). Section 3 provides a detailed insight into the nature of the interaction between, on the one hand, Traditional Obliged Entities (TOE) and VA/VASP and, on the other, between the informal sector and VA/VASP.

Table 1: The 27 VASP Channels

VASPs	Types of Services	Sub-type (Channels)
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	1. Hot Wallet
	Non-Custodial Services	2. Cold Wallet
VIRTUAL ASSET EXCHANGES	Transfer Services	3. P2P
		4. P2B
	Conversion Services	5. Fiat-to-Virtual
		6. Virtual-to-Fiat
		7. Virtual-to-Virtual
VIRTUAL ASSET BROKING	Payment Gateway	8. ATMs
		9. Merchants
		10. Cards
VIRTUAL ASSET MANAGEMENT PROVIDERS	11. Fund Management	
	12. Fund Distribution	
	13. Compliance, Audit & Risk Management	
INITIAL COIN OFFERING (ICO) PROVIDERS	Fund Raising	14. Fiat-to-Virtual
		15. Virtual-to-Virtual
	Investment	16. Development of Products & Services
	Other Offerings	17. Security Token Offerings (STOs)
		18. Initial Exchange Offerings (IEOs)
VIRTUAL ASSET INVESTMENT PROVIDERS	Trading Platforms	19. Platform Operators
		20. Custody of Assets
		21. Investment into VA-related commercial activities
		22. Non-Security Tokens & Hybrid Trading Activities
		23. Stablecoins
	Emerging Products	24. Crypto Escrow service
		25. Crypto-custodian Services
VALIDATORS/MINERS/ ADMINISTRATORS	Proof of work	26. Fees
		27. New Assets

Table 2: Definition of the VASPs

VASPs	
VIRTUAL ASSET WALLET PROVIDER	An entity that provides a VA wallet for holding, storing and transferring bitcoins or other VAs. A wallet provider facilitates participation in a VA system by allowing users, exchangers, and merchants to conduct virtual asset transactions more easily. The wallet provider maintains the customer's virtual asset balance and generally also provides storage and transaction security. Some well-known Wallet providers are Bitcoin Core protocol, Electrum, Exodus, Jaxx, Coinbase, Blockchain etc.
VIRTUAL ASSET EXCHANGES	An entity engaged in the business of VA exchange for fiat currency, funds, or other forms of virtual asset for a commission. The exchangers accept a wide range of payments, such as cash, wire transfers, credit cards, and other virtual assets. Individuals typically use exchangers to deposit and withdraw money from virtual asset accounts. Some of the well-known exchangers are Kraken, Bitfinex, Coinbase, Bitstamp, Binance, Coinmama, CEX.IO etc.
VIRTUAL ASSET BROKING	Arranging transactions involving virtual assets or involving virtual assets and fiat currency. VA Broking involve ATMs (Automated Teller Machines), Merchants and Cards. An ATM dealing with VAs is a kiosk that allows a person to purchase VAs by using cash or debit card. Some VA ATMs offers bi-directional functionality enabling both the purchase of virtual assets as well as the sale of virtual assets for cash. Merchants exchange fiat to VA.
VIRTUAL ASSET MANAGEMENT PROVIDERS	VA Management Providers involve Fund managers investing in VAs; Firms which distribute funds that invest (wholly or partially) in VAs; and Support over guidance on risk management, management of liquid capital, segregation of assets, custodianship, funds structure, and other legal aspects.
INITIAL COIN OFFERING (ICO) PROVIDERS	Involve issuing and selling VAs to the public and may also involve participating in and providing financial services relating to the ICO. Further provide for services such as Security Token Offerings (STOs) offering equity in the form of tokens.
VIRTUAL ASSET INVESTMENT PROVIDERS	Providing an investment vehicle enabling investment in/ purchase of VAs (i.e. via a managed investment scheme or a derivatives issuer providing virtual asset options, or via a private equity vehicle that invests in virtual assets).
VALIDATORS / MINERS/ ADMINISTRATORS	An entity that receives VA rewards for being the first to validate transactions in a decentralized VA ledger. Miners use very high computing power in a distributed proof system to run complex algorithms which solve the highly challenging mathematical equations required to validate transactions.

b) Interaction between VASP channels and Sectors (Formal and Informal) in Mauritius

The Risk Assessment Working Group considered the interaction of VASP channels with two ecosystems which will likely require different strategies to counter ML/TF threats. One ecosystem is the formal TOE regulated sector that accommodates AML/CFT regulations and its compliance. The other ecosystem - informal sector - captures players, actors, entities, platforms and tokens that fall outside the traditional AML/CFT sector within a much less developed or non-existence AML/CFT compliance framework and with little to no corporate accountability to regulators that could open the doors to illicit financing.

The different formal TOE sectors such as the Banking, NBFI, Trust and Company Service Providers, Casinos, Dealers in Precious Metals and Stones, Real Estate Agents, Accountants, and Legal Professions were assessed against all the 27 VASP channels. Only two sectors, Banking and NBFI, were identified as interacting with 7 VASP channels, as detailed in Table 3 below.

Table 3: Sector interaction with the VASP Channels

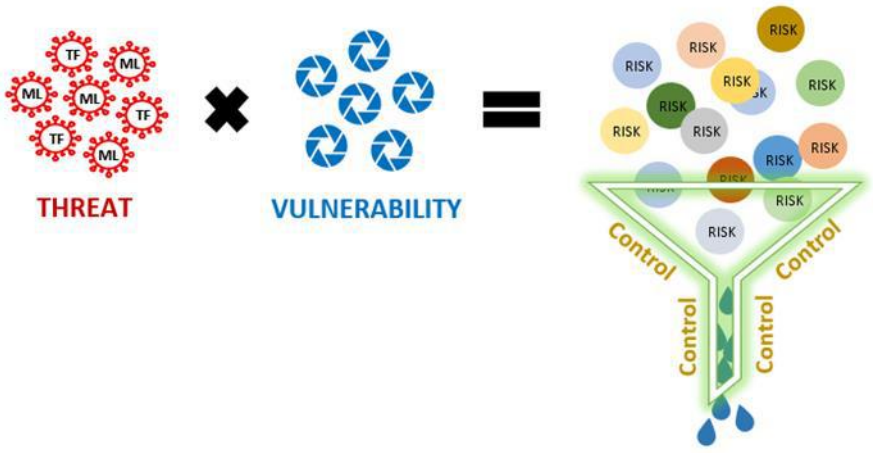
27 Channels			Banks	NBFI	Informal Sector	Accountants	Legal Professionals	Trust & Company Service Providers	Casinos, Gaming & Betting	Dealers in Precious Metals & Stones	Real Estate Agents
VIRTUAL ASSET WALLET PROVIDERS	1	Hot Wallet	-	●	●	-	-	-	-	-	-
	2	Cold Wallet	-	-	●	-	-	-	-	-	-
VIRTUAL ASSET EXCHANGES	3	P2P	-	-	●	-	-	-	-	-	-
	4	P2B	-	-	●	-	-	-	-	-	-
	5	Fiat-to-Virtual	●	-	●	-	-	-	-	-	-
	6	Virtual-to-Fiat	●	-	●	-	-	-	-	-	-
	7	Virtual-to-Virtual	-	-	●	-	-	-	-	-	-
VIRTUAL ASSET BROKING / PAYMENT PROCESSING	8	ATMs	-	-	-	-	-	-	-	-	-
	9	Merchants	-	-	●	-	-	-	-	-	-
	10	Cards	-	-	-	-	-	-	-	-	-
VIRTUAL ASSET MANAGEMENT PROVIDERS	11	Fund Management	-	●	-	-	-	-	-	-	-
	12	Fund Distribution	-	-	-	-	-	-	-	-	-
	13	Compliance, Audit & Risk Management	-	●	-	-	-	-	-	-	-
INITIAL COIN OFFERING (ICO) PROVIDERS	14	Fiat-to-Virual	-	-	-	-	-	-	-	-	-
	15	Virtual-to-Vitual	-	-	-	-	-	-	-	-	-
	16	Development of Product & Services	-	-	-	-	-	-	-	-	-
	17	Security Token Offerings (STOs)	-	-	-	-	-	-	-	-	-
	18	Initial Exchange Offerings (IEOs)	-	-	-	-	-	-	-	-	-
VIRTUAL ASSET INVESTMENT PROVIDERS	19	Platform Operators	-	●	-	-	-	-	-	-	-
	20	Custody of Assets	-	-	-	-	-	-	-	-	-
	21	Investment into VA-related commercial activities	-	●	-	-	-	-	-	-	-
	22	Non-Security Tokens & Hybrid Trading Activities	-	-	-	-	-	-	-	-	-
	23	Stablecoins	-	-	-	-	-	-	-	-	-
	24	Crypto Escrow service	-	-	-	-	-	-	-	-	-
	25	Crypto-custodian Services	-	-	-	-	-	-	-	-	-
VALIDATORS / MINERS/ ADMINISTRATORS	26	Fees	-	-	-	-	-	-	-	-	-
	27	New Assets	-	-	-	-	-	-	-	-	-

c) Total Combined ML/TF Risk Rating for each applicable Channel

The combined ML/TF threat and ML/TF inherent vulnerability rating for each channel were used to produce a total risk level rating before considering mitigating measures, such as Government measures, VASP measures and FI/DNFBPs measures.

d) Residual Combined ML/TF Risk Rating for each applicable Channel

A residual combined ML/TF risk rating for each applicable channel has been computed based on the total combined ML/TF risk after taking into consideration Government measures and FI/DNFBPs measures. In the absence of locally domiciled VASPs, the associated VASP mitigating measures were not relevant.



The risk ratings have been categorised as follows: Very High, High, Medium, Low and Very Low.

The ratings for assessing mitigating measures have been categorised as follows: Very High Mitigation, High Mitigation, Medium Mitigation, Low Mitigation, Very Low Mitigation and Does Not Exist.

e) ML/TF Threat Assessment for each applicable Channel

In determining the ML/TF threats associated with VAs and VASPs, Mauritius considered those activities which led to criminal intent to launder money or financing of terrorist activities through VAs/VASPs, both in terms of the domestic threat and the cross-border threat.

In addition, the threat level for each VASP channel was assessed based on the following different input variables:

Table 4: Input Variable for ML/TF Threat Assessment

Input Variables	Features
VA Nature and Profile	▪ Anonymity/ pseudonymity ▪ P2P Cross-Border Transfer and Portability ▪ Absence of face-to-face contact ▪ Traceability ▪ Speed of Transfer
Accessibility to Criminal	▪ Mining by criminal ▪ Collection of funds ▪ Transfer of funds ▪ Dark Web Access ▪ Expenditure of funds
Source of funding VA	▪ Bank or card as source of funding VA ▪ Cash transfers, valuable in-kind goods ▪ Use of virtual currency
Operational features of VA	▪ Regulated ▪ Anonymity/ pseudonymity ▪ P2P Cross-Border Transfer and Portability ▪ Absence of face-to-face contact
Ease of criminality	▪ Traceability ▪ Speed of Transfer ▪ Mining by criminal ▪ Collection of funds
Economic Impact	▪ Transfer of funds ▪ Dark Web Access ▪ Expenditure of funds

For example, the **ML/TF threat** rating for **VASP channel 3 - P2P** will depend on such factors as how far that specific channel is easily accessible to criminals, whether the channel protects or hides the identity of the participants (anonymity), whether the channel can easily be used for criminal activity (ease of criminality) or whether the channel operates in an unregulated environment. Each input variable will therefore be assessed to determine the extent to which that input variable contributes to the threat rating for the channel under consideration.

An overall combined ML/TF threat rating was derived for the VA/VASP ecosystem based on the ML/TF threat rating for each applicable channel.

f) ML/TF Inherent Vulnerability Assessment for each applicable Channel

The ML/TF inherent vulnerability refers to the relative exposure of an industry sector to ML/TF. The FATF uses the following definition for vulnerability: they are "weaknesses or gaps that may be exploited by the threat or may facilitate its activities."

The Risk Assessment Working Group examined the inherent vulnerability of each of the 12 applicable VASP channels described above, based on the nature of products and services and the types of VAs offered. The following factors were taken into consideration:

- Licensed in the country or abroad;
- Nature, size and complexity of business;
- Products and Services;
- Methods of delivery of products/ services
- Customer types;
- Country risk;
- Institutions dealing with VASP;
- VA (anonymity/pseudonymity);
- Rapid transaction settlement; and
- Dealing with unregistered VASP from overseas.

By way of example, if **VASP channel 3 - P2P** is an unregistered VASP from abroad and offers products and services and methods of delivery which enhance anonymity and favour rapid transaction settlement, then that particular channel is likely to be very vulnerable to ML/TF risks.

An overall combined ML/TF vulnerability rating was derived for the VA/VASP ecosystem based on the ML/TF inherent vulnerability rating for each applicable channel.

g) Overall ML/TF Risk associated with the VA/VASP Ecosystem

An overall combined ML/TF risk rating was derived for the VA/VASP ecosystem based on the risk rating after mitigating measures for each applicable channel.

Table 5 – Dashboard of the Identified Channels and Assessing Factors

Interaction between Reporting Entities, informal sector and the VA ecosystem has revealed the identification of 12 VASP channels	Virtual Asset Wallet Providers		Virtual Asset Exchanges					Virtual Asset Broking	Virtual Asset Management Providers		Virtual Asset Investment Providers	
	Channel 1:	Channel 2:	Channel 3:	Channel 4:	Channel 5:	Channel 6:	Channel 7:	Channel 8:	Channel 9:	Channel 10:	Channel 11:	Channel 12:
	Hot Wallet	Cold Wallet	P2P	P2B	Fiat to Virtual	Virtual to Fiat	Virtual to Virtual	Merchants	Fund Management	Compliance, audit and risk management	Platform operators	Inventment into VA related commercial activities
THREAT ASSESSMENT	*The Threat Rating for each channel* ***(Very High, High, Medium, Low, Very Low)*** *depends on the assessment of the 6 input variables and their corresponding factors as detailed below:*											
Input Variables used for Threat:												
1. VA Nature and Profile	Factors that will be considered to **rate the input variable for each channel** are: anonymity, cross border transfer, portability, absence of face to face contact, speed of transfer and traceability.											
2. Accessibility to Criminals	Factors that will be considered to **rate the input variable for each channel** are: mining by criminals, transfer of funds, dark web access											
3. Source of VA Funding	Factors that will be considered to **rate the input varible for each channel** are: bank or card as a source of VA funding, cash transfers, use of virtual currency											
4. Operational Features of VA	Factors that will be considered to **rate the input variable for each channel** are: regulated or unregulated environment, centralised or decentralised environment											
5. Ease of Criminality	Factors that will be considered to **rate the input variable for each channel** are: tax evasion, terrorist financing, disguising criminal proceeds into VA, circumvent exchange control											
6. Economic Impact	Factors that will be considered to **rate the input variable for each channel** are: underground economy, extent to which there is full integration beteen VA ecosystem and financial services market											
VULNERABILITY ASSESSMENT	*The Vulnerability Rating for each channel* ***(Very High, High, Medium, Low, Very Low)*** *depends on the assessment of the input variable and its corresponding factors as detailed below:*											
Input variable used for Vulnerability:												
1. Product and services provided and the types of VAs	Factors that will be considered to **rate the input variable for each channel** are: VASP licenced in the country or abroad, nature, size and complexity of business, products and services, methods of delivery, customer types, country risk, institutions dealing with VASPs, VA anonynity, rapid transaction settlement, dealing with unregistered VASPs from abroad											
TOTAL RISK RATING	***Threats rating combined with Vulnerability rating for each Channels***											
ASSESSMENT OF THE EFFECTIVENESS OF MITIGATING MEASURES	*The score for effectiveness of Mitigating measures* ***(Very High, High, Medium, Low, Very Low, Does not exist)*** *depends on the assessment of the 3 input variables*											
Government Measures, VASP measures and Measures by reporting entities (FIs and DNFBPs)												
RESIDUAL RISK RATING	***Total risk rating after considering Mitigating Measures for each Channels***											

Data Collection

The following data and information sources were used for completing the assessment:

- Information collected through survey questionnaires;
- Information from off-site analysis and on-site AML/CFT inspection reports of TOEs;
- Statistics (national and international);
- Intelligence;
- Reports produced by LEAs;
- Interviews and focus group meetings with relevant authorities;
- Informal discussions with selected private sector participants;
- Articles and reports based on academic research;
- Reports from international standard-setting bodies;
- International case studies;
- Relevant Government reports; and
- Media, social media, internet and other sources of public information.

Challenges and Limitations

a) The overwhelming majority of respondents stated that they did not offer services nor engage in VA related activities. One plausible reason for this could be that the VA ecosystem is relatively new in the Mauritian landscape, and there seems to be a lack of general understanding of how VAs operate.

b) The fact that in most instances the formal sectors in Mauritius were not directly engaging with the VA/VASP ecosystem, coupled with the lack of a legal framework regulating VA-related activities have contributed to a scarcity of officially compiled VA/VASP data. Focus group discussions with several authorities and private sector were held to complement the analysis for this risk assessment. In addition, given that the utility of VA in ML/TF methods and the VA's ecosystem is still unclear, international case studies where VAs were used as a medium of ML/TF or to facilitate criminal activities were used to have a better appreciation of the threat and vulnerabilities associated with VAs and VASPs. [10]

   The analysis was also based on reported or detected cases and on information relating to unreported or undetected cases. These limitations mean that the actual number of predicate offences and their proceeds are broad estimates at best.

   Where information was missing, the assessed level of ML/TF risk was increased to conform with the conservative approach adopted by the Risk Assessment Working Group.

c) The Covid-19 pandemic is another factor that affected this risk assessment. The Government implemented a range of containment measures during the outbreak to support the economy. The second phase of lockdown – from March to April 2021 disrupted data collection and delayed the risk assessment.

[10] FATF Risk, Trends and Methods Group – Virtual Asset – Updated Case Studies. February 2020

3. VA/VASP INTERACTION WITH TRADITIONAL OBLIGED ENTITIES AND INFORMAL SECTOR IN MAURITIUS

This Section of the report describes the interaction of the Banking, the NBFI and the informal sectors, which are the only sectors identified as interacting with the VA/VASP ecosystem.

3.1. BANKING SECTOR

Overview

Banks licenced and governed by the Banking Act 2004 dominate the financial sector. The BOM's mandates include ensuring the stability and soundness of the Mauritian financial system. The BOM is both the prudential and AML/CFT regulator and supervisor of banks, which includes the conduct of risk-based supervision, ensuring that its licensees comply with AML/CFT legislation and guidelines, and maintain sound corporate governance practices as well as effective risk management frameworks.

Interaction of the Banking Sector and the VA/VASP sector

Out of the 12 identified channels, two channels, namely *Fiat to Virtual* and *Virtual to Fiat* have been identified as applicable to the Banking Sector and pertain to conversion services at Virtual Asset Exchanges. The remaining channels were deemed as not applicable.

Risk Appetite

The spectacular upswings of VAs, especially Bitcoin, have attracted widespread interest from customers worldwide and in Mauritius for this type of investment, the more so as interest rates have significantly declined over time. However, at the time of this assessment, banks seemed reluctant towards engaging in VA/VASP related activities, mainly because there was no applicable legislative framework in Mauritius for such activities. Banks stated that they do not own investments in VAs or shares in entities dealing with VAs, nor engage in proprietary trading in VAs.

Product & Delivery Channel Risk

Notwithstanding the fact that banks do not offer VA products/services to their customers, some bank customers are using bank products and services to convert fiat currency to VAs and vice versa through VA Exchanges. Bank products such as credit/debit/prepaid cards, wire transfers, PayPal accounts are used to purchase/invest in VAs, particularly Bitcoins. Nonetheless, as per available data, amounts were not deemed as significant, and were commensurate with customers' profiles. All wire transfers are supported by SWIFT messages which record the beneficiary and originator names, in line with FATF requirements.

Customer Risk and Sanctions risk

Bank customers are subject to CDD procedures at on-boarding, and periodic customer risk-based reviews as part of the monitoring process. Banks promptly update their databases, based on changes made to the United Nations Sanctions Lists, and sanctions risk is mitigated by screening tools.

Transaction Risk

A CipherTrace Cryptocurrency Intelligence Report published in October 2020[11] revealed that a typical large US bank processes over USD 2 billion annually in undetected VA-related transfers. The absence of properly configured monitoring systems and software for VA-related transactions conducted through banks and their products/delivery channels implies that VA transaction trails are not currently being comprehensively captured.

Counterparty Risk

In the absence of VA monitoring processes, banks may face significant counterparty risks when their customers engage with VASPs, due to insufficient visibility of transaction trails and decentralised virtual asset systems which make them particularly vulnerable to anonymity risks. Counterparty risk is further heightened if customers interact with high risk VASPs located in jurisdictions with weak AML/CFT regimes.

Country Risk

Country risk arises when criminals use jurisdictional arbitrage to send funds to VASPs located in countries lacking effective AML/CFT regimes to obfuscate their trails and beneficiaries. This vulnerability exposes banks to heightened ML/TF risks. The CipherTrace Cryptocurrency Intelligence Report referred to above states that 57 per cent of VASPs had weak or porous KYC processes, which make them attractive for laundering criminal proceeds and obfuscating tracing of funds. These VASPs were in jurisdictions without strategic deficiencies in their AML/CFT regimes and are not considered as high-risk countries for conventional cross-border transactions. The report also states that this demonstrates the ease and volume of potential off-ramps for money launderers. Such a statement implies that a positive conventional country risk rating does not guarantee that the country has mitigated its VA-related ML/TF risks.

[11] *CipherTrace "Cryptocurrency Intelligence - Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019,* https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report

Customer protection issues

The interaction of the banking sector with the VA/VASP sector also gives rise to customer protection issues. Traditional banking investments are considered to be relatively safe investments, however the general risks associated with VAs are far higher for customers. For instance, for traditional cross-border transfers, safeguards are embedded in the banking system to mitigate the risk of misappropriation of funds. However, in the VA ecosystem, if VAs are sent to the wrong wallet, they cannot be recovered.

Furthermore, unfamiliarity with the VA ecosystem exposes customers to the risk of fraud, with the possibility of their investments disappearing from their wallets through hacking and other criminal activities. The Mt Gox case (Case 1 below) illustrates such a scenario - a massive hack of 850,000 Bitcoins (6% of all Bitcoins in existence at that time, valued at the equivalent of EUR460 million) which caused substantial and permanent losses to investors[12]. A defalcation of this magnitude might cause systemic losses in Mauritius.

There are also risks which arise from VA price volatility, which could potentially undermine the financial position of consumers.

Case 1 – Massive Hack – Mt. Gox

The victim of a massive hack, Mt. Gox lost about 850,000 bitcoins (6% of all bitcoin in existence at the time), valued at the equivalent of €460 million at the time and over $3 billion at October 2017 prices. An additional $27 million was missing from the company's bank accounts. Although 200,000 bitcoins were eventually recovered, the remaining 650,000 have never been recovered.

[12] Wired, "*The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster"*, 3 March 2014, https://www.wired.com/2014/03/bitcoin-exchange/

3.2. NON-BANK FINANCIAL INSTITUTIONS

NBFIs in Mauritius are supervised by the FSC and are subject to AML/CFT requirements under the Financial Intelligence and Anti-Money Laundering Act (FIAMLA), United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act (UNSA), Financial Intelligence and Anti-Money Laundering Regulations (FIAMLR) and the FSC AML/CFT Handbook. All NBFIs under the purview of the FSC must apply a reasonable and proportionate risk-based approach in respect to AML/CFT. Furthermore, FIs are subject to risk-based supervision through FSC's offsite and onsite AML/CFT annual supervisory programme. This ensures that FIs adopt mitigating measures commensurate with the risks identified.

In addition, the FIAMLA stipulates that prior to launching a new product or business practice or the use of a new or developing technology, a reporting person or a supervisory authority shall identify and assess the ML/TF risks that may arise and respond appropriately to manage and mitigate these risks.

Licensable Activities

At the time of the assessment and further to the report of the Regulatory Committee on Fintech and Innovation-Driven Financial Services, the FSC had undertaken several initiatives to position Mauritius as a fintech hub. These included two licensable activities, namely:

- the Custodian Services (Digital Assets); and
- the Digital Asset Marketplace.

Custody Services (Digital Assets)

The holder of a Custody Services (Digital Assets) License conducts the business of securing and preserving digital assets held in custody through the generation and securing of seeds and keys. It also manages wallets for digital assets including recovery processes for corrupted or compromised seeds and keys.

Digital Asset Marketplace

A digital asset marketplace, also known as an exchange, is an entity engaged in facilitating the buying, selling and exchange of digital assets for fiat currencies or other forms of digital assets and vice versa, for a commission. Digital asset marketplaces offer services by providing liquidity and the ability to trade digital assets. Through the process known as "on-ramp," digital asset marketplaces may enable the conversion of fiat currencies to digital assets. Through the "off-ramp", digital asset marketplaces allow a person to exchange a digital asset for fiat currencies.

A regulatory framework for Digital Asset Marketplace has not yet been established, nor have any licences been granted.

Digital Assets and VAs as an Asset-Class

VAs prices may be extremely volatile, investments in VAs are considered high-risk. Nevertheless, the regulatory authority recognises that Digital Assets[13] including VAs may constitute an asset-class for investment by:

- Sophisticated Investors[14];
- Expert Investors[15];
- Expert Funds[16];
- Specialised Collective Investment Schemes[17]; and
- Professional Collective Investment Schemes[18].

As at date of the assessment none of the investors/licensees identified above had invested in digital/VAs nor has the FSC approved any such structures.

Interaction of the NBFI Sector and the VA/VASP Sector

The risk assessment identified the following VASPs interacting with NBFIs in the Mauritian ecosystem.

Investment Advice – Compliance, Audit and Risk Management Support

The FSC issues Investment Adviser Licences to allow FIs to provide investment advice to its clients as its core activity. These are 2 categories of licences;

(i) Investment Adviser (Restricted); and

(ii) Investment Adviser (Unrestricted).

Through the survey it was noted that, in two cases, Investment Advisers provided restricted investment advice (not portfolio management) to their clients in respect of investment in VAs.

Case 2 – Investment Adviser and Client based in Mauritius

The Adviser provided non-binding investment advice to the client, whose board approved the investment in VAs. Following which an amount of USD 2 million was invested in VA through a Special Purpose Vehicle set up as an investment holding company incorporated in Mauritius.

[13] Mauritius considers as a Digital Asset, any token, in electronic/binary form, which is representative of either the holder's access rights to a service or ownership of an asset. A Digital Asset, in this respect, includes a digital representation of value which: is used as a medium of exchange, unit of account, or store of value but which is not legal tender, even if it is denominated in legal tender; represents assets such as debt or equity in the promoter; or provides access to a blockchain-based application, service or product.
[14] The term "Sophisticated Investor" is defined in section 2 of the Securities Act 2005.
[15] The term "Expert Investor" is defined in regulation 78(a) of the Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008.
[16] The term "Expert Fund" is defined in regulation 2 of the CIS Regulations 2008.
[17] The term "Specialised Collective Investment Scheme" is defined in regulation 77 of the CIS Regulations 2008.
[18] The term "Professional Collective Investment Schemes" is defined in regulation 75 of the CIS Regulations 2008

Case 3 – Investment Adviser based in Mauritius

An Investment Adviser, based in Mauritius, provided non-binding advice for investment of MUR 2 billion in VA to a client based in Sub-Saharan Africa. The client is authorised by the regulatory body of the jurisdiction in which it operates.

Virtual Asset Investment Provider

a) Investment into VA-related commercial activities

The definition of Virtual Asset Investment Provider provides for an investment vehicle enabling investment in/purchase of VAs. The survey revealed two cases whereby FIs licensed by the FSC were used as Investment Vehicle to invest in VAs as underlying assets.

Case 4 – Investment through a licensed platform

A licensee set up as a Protected Cell Company (PCC) held investment in VAs. The amount of the investment was of around USD 2 million which represented roughly 0.8 % of the overall investment of the PCC.

The Cell has invested in Bitcoin, Litecoin, Tezos, Ethereum and Dash through a regulated platform. The platform conducted CDD on the Cell prior to transacting. The VAs were stored on a platform-held hot wallet.

Case 5 – Investment using cold wallet through a licensed platform

An External Insurer (FI) providing life insurance and investment-linked long term insurance products to international intermediaries, had invested approximately MUR 2 million in Bitcoins, representing 0.02 percent of its total business.

The VA purchase was made through a regulated exchange using a Trezor- cold wallet. AML Checks were conducted by the FI.

b) Platform Operators

Virtual asset trading platforms are online platforms which match buyers' and sellers' orders for trading in VA, and they perform functions similar to traditional securities brokers, stock exchanges and private trading venues[19].

Case 6 – Investment through a licensed platform

An FI has terms of business on a non-disclosed basis with a regulated exchange. Through the terms of business with the exchange, the FI operates an application software that allows buying, selling and exchange of VAs such as Bitcoin, Ethereum and Litecoin.

[19] *Stevenson, Wong & Co., Further Development of Regulatory Approach towards Virtual Asset Portfolio Managers, Fund Distributors and Trading Platform Operators, 12 June 2019,* https://www.sw-hk.com/news-20190612-1/

Management Companies

Management Companies (MCs) which are considered as traditional obliged entities are regulated and supervised by the FSC and fall under the definition of FIs. They help their clients to set up, manage, and administer their affairs. Both MCs and Global Business Companies (GBCs) are subject to a rigorous licensing and supervisory regime under the oversight of the FSC. MCs are subject to a full scope of AML/CFT measures set out in the FIAMLA and FIAMLR and the FSC supervises them as FIs. MCs may be potentially exposed to ML/TF risks stemming from clients' interaction with VAs/VASPs.

Interactions of MCs with their clients are by nature non-face-to-face and may include PEPs or high net worth individuals investing into VAs. There is also a vulnerability in the indirect interaction of MCs with regulated/unregulated VASPs which operate in jurisdictions having inadequate AML/CFT regimes.

3.3. DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

The DNFBP AML/CFT supervisors in Mauritius comprise the AGO, the MIPA, the GRA, the FIU and the ROC.

The GRA is the licensing, regulatory and supervisory body for the Mauritian Gambling sector which includes casinos, gaming houses, bookmakers for horse racing and for foreign football matches, and lotteries.

The AGO licenses and regulates Law Firms (local and foreign) and Joint Law Ventures.

The MIPA licenses, regulates and supervises Professional Accountants, Public Accountants and Member Firms, who provide accounting, audit, tax management, consultancy and insolvency services.

The ROC is the Authority responsible for the incorporation of companies in Mauritius, the registration of Foundations, Limited Partnerships and Limited Liability Partnerships, and is also the AML/CFT supervisory authority for Company Service Providers (CSPs).

The FIU is the AML/CFT Supervisory body for Dealers in Precious Metals and Stones, Real Estate Agents and Individual Legal Professionals (Attorneys, Barristers and Notaries).

Although this risk assessment reveals that the DNFBPs do not offer VA-related services or interact with VASPs, law firms could also be providing advice on the legal aspects of investing in VAs. On the other hand, Mauritians could individually be engaging with VA/VASPs. For example, the GRA licensees do not offer online gambling or VA-related gambling but there is no legal restriction preventing individuals from accessing online betting platforms which accept bets in VAs. Gambling is a cash-intensive business, and cash can be easily converted into VAs.

3.4. INFORMAL SECTOR

The assessment showed that the Informal Sector interacts with 8 of the 12 identified channels as detailed in Table 3 in Section 2. The lack of a regulatory framework for Mauritius, at the time of this assessment, poses very high ML/TF risks for this sector.

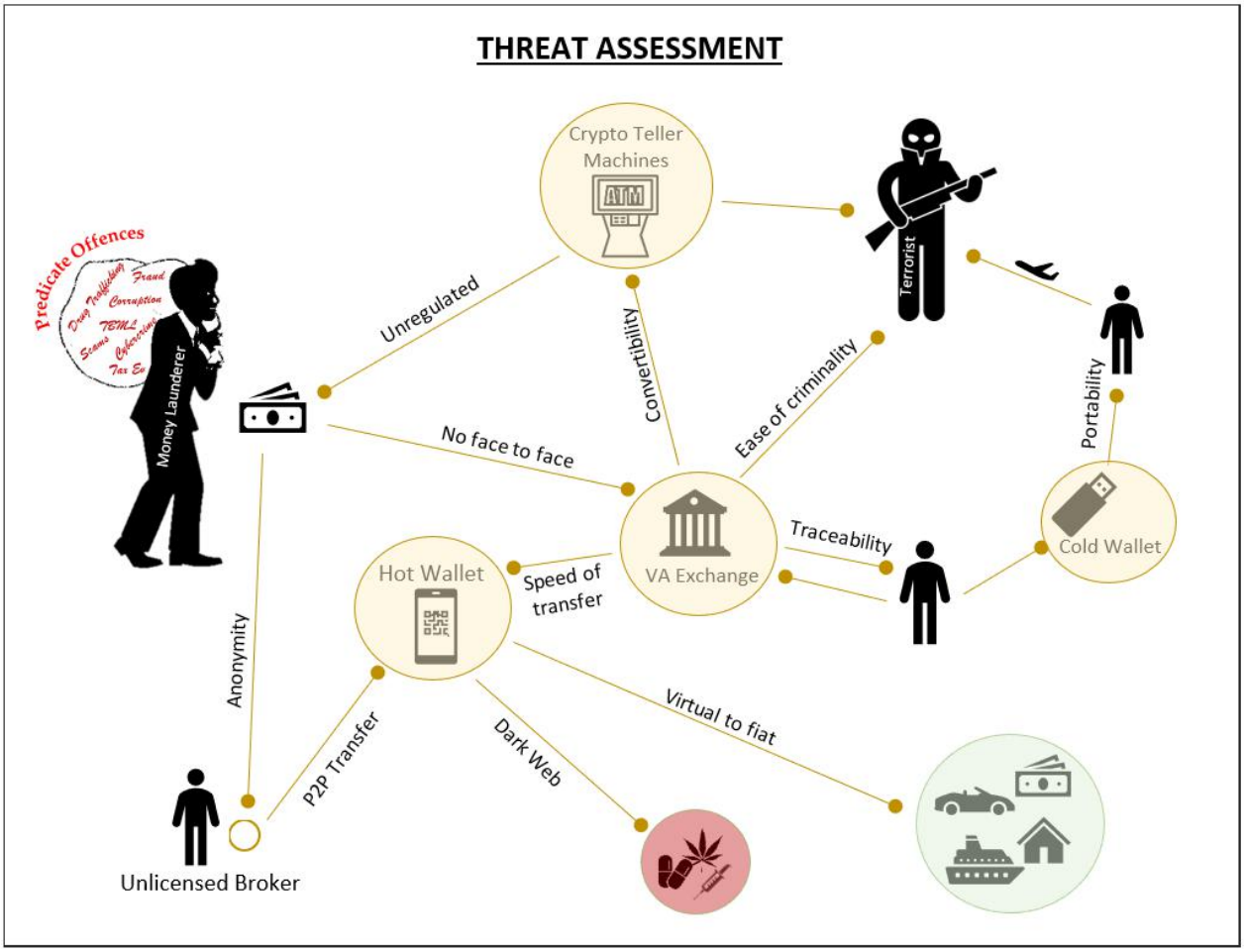
Information from other sources showed that VA transactions have been occurring in Mauritius over several years, indicating that this is an informal but well-established activity. Field intelligence identified a peer-to-peer platform offering Bitcoin, Ethereum and Tether trading to the Mauritian market through multiple payment channels which could potentially provide easy ML opportunities for criminals. Although payment methods included bank transfers, credit and debit cards, PayPal, online wallets and mobile payments, twenty-five percent of the merchants on the platform accepted cash only against high commission rates. The preference for cash accompanied by high commission rates constitutes ML/TF red flags.

From information gathered, crypto enthusiasts in the informal sector invest in both the established VAs and nascent ones such as DogeCoin and Shiba Inu. Shiba Inu, created anonymously in August 2020, is a decentralized cryptocurrency modelled off Dogecoin (Shiba Inu is a Japanese breed of dog)[20].

The P2P platform also allows for anonymity, rapid transfers, absence of face-to-face contact and lack of traceability, which further heighten ML/TF risks. Information shows the sector interacts with illicit or high-risk entities and with jurisdictions lacking effective regulatory VA/VASP frameworks. These interactions include wallet transfers from Mauritius to European Bitcoin Teller Machines (BTMs) where they have subsequently been redeemed for fiat currency. The analysis further revealed that Bitcoins have been transferred from an exchange, BTC-e (a high-risk exchange) and transacted over a four-year period through a chain of wallets, via IP addresses linked to Mauritius. BTC-e was closed down on 26th July 2017 by the U.S. Attorney's Office, Northern District of California and its Russian co-founder Alexander Vinnik was charged under a 21-Count Indictment for operating an alleged International Money Laundering Scheme and allegedly laundering funds from the 2014 USD 460 million hack of Mt. Gox (Case box 1). The exchange was also alleged to have previously received deposits of over USD 4 billion.[21]

[20] https://en.wikipedia.org/wiki/Shiba_Inu_(cryptocurrency)
[21] Financial Crimes Enforcement Unit, FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales, https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

4. ML/TF THREAT ASSESSMENT



The ML/TF threat emanates from predicate offences associated with the VA/VASP ecosystem and the threat level for each VASP channel was assessed based on the different input variables. The inherent features of VAs could easily be exploited by criminals to facilitate ML/TF, given the complexity of VA-related ML/TF investigations and the exposure of Mauritius to the global threats posed by VAs and foreign-based VASPs.

Identified Predicate Offences associated with the VA/VASP Ecosystem

The features of VAs and VASPs imply that proceeds from all predicate offences, identified in the 2019 NRA, can be laundered through them. This Section details the identified predicate offences associated with the VA/VASP ecosystem based on, *inter alia*, domestic reported cases to LEAs, intelligence and international case studies[22].

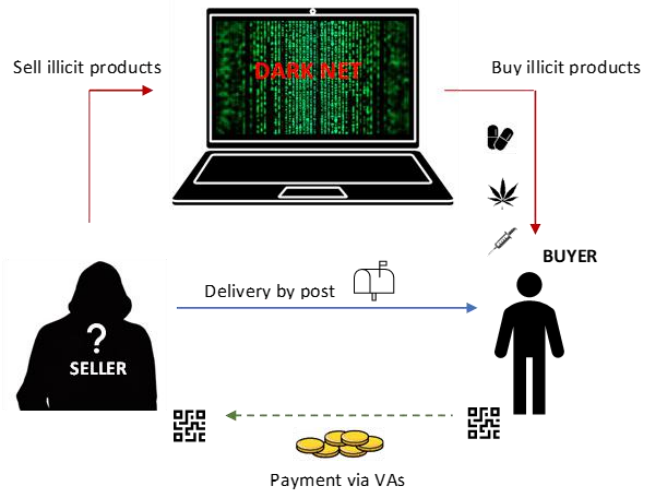
[22] FATF, Updated Guidance for a Risk-Based Approach to, *Virtual Assets and Virtual Asset Service Providers*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

Drug Trafficking

The 2019 NRA identified drug trafficking as having a high ML threat in Mauritius. During the past two years, Mauritius has witnessed record-high drug seizures worth MUR 7 billion[23]. It is apparent that there is a well organised cross-border drug trafficking network of both local and foreign nationals. Domestically, drug syndicates are becoming increasingly organized, well-funded and adept.

Drug traffickers are continuously exploring new avenues to avoid detection, including the use of technology and the virtual space is attractive to them, especially the dark net.

The "darknet" is a rising and resilient global threat, especially in relation to drug trafficking. The yearly sales of drugs linked to the "darknet" internationally amounted to almost USD 800 million in 2019, representing a 70% growth when compared to 2018[24]. Multiple online "darknet" markets provide a virtual space for drug dealing. These web-based platforms ensure anonymity and facilitate peer to peer transactions.



Very few cases were identified in Mauritius where drug traffickers have used Bitcoins to buy drugs on the darknet. However, it can be expected that drug traffickers and their facilitators will increasingly make use of the darknet and unregulated exchanges to avoid detection thus, exacerbating the risk of funds derived from drug trafficking being laundered.

Fraud

VA/VASP- related frauds are usually characterised by faked coin offerings, fraudulent investment schemes and faked exchangers using imposter websites[25]. The threat assessment identified two cases of VA-related fraud in Mauritius (Case 7 and Case 8 below). These include cases where victims have been induced to pay into fraudulent VA investment schemes promoted by foreign criminals who claimed links with dubious foreign-based VASPs. The illicit funds obtained were allegedly laundered through multiple countries. Additionally, some websites have been falsely

[23] Source: Mauritius Police Force
[24] Chainalysis, *"The Chainalysis 2020 Crypto Crime Report" January 2020*, https://go.chainalysis.com/2020-crypto-crime-report
[25] Gadgets 360, Cryptocurrency, "*Crypto Scam Websites Registered 9.6 Million Visits From India in 2021: Report"*, 17 January 2022, https://gadgets.ndtv.com/cryptocurrency/news/india-crypto-scam-websites-chainalysis-2712975

promoting Mauritius as VA friendly investment jurisdiction[26]. Given the increasing publicity and appetite for VAs in Mauritius it can be reasonably expected VA-related frauds and their corresponding ML/ TF threats will increase.

Case 7 – Phishing Attack

A Mauritian national accessed an email link to an alleged VA platform and transacted twice, believing that he was accessing his usual VA platform. Later, he found out that it was a phishing attack and that his funds had been moved to wallets in Asia.

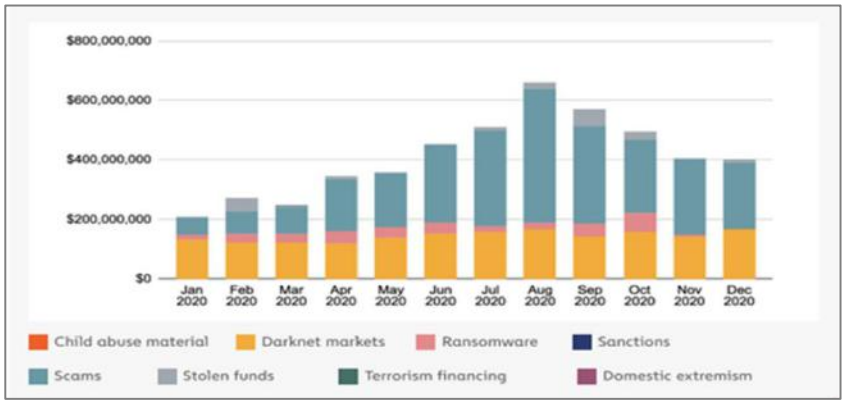
Case 8 – Illegal VA related Ponzi Schemes

A person alleging that he is a representative of a new technology company organised a promotional campaign during which he introduced the concept of OneCoin and encouraged attendees to invest in this token. An interested Mauritian attendee invested EUR 1,790 but never received any OneCoin Tokens. The campaign was a VA-related Ponzi scheme and OneCoin was found to be an international multibillion-dollar pyramid scheme selling education packages that included "tokens".

Predicate Offences and Emerging Threats identified in International Typologies

The chart below illustrates the different threats in the global VA ecosystem which could potentially affect Mauritius. It demonstrates the pervasiveness of dark net usage throughout 2020 and the increasing magnitude of scams.

Total Cryptocurrency Value Received by Illicit Entities in 2020



Source: *The 2021 Crypto Crime Report by Chainalysis*

[26] Buy Bitcoin Worldwide, "*Buy Crypto & Bitcoin in Mauritius*" 10 December 2021, https://www.buybitcoinworldwide.com/mauritius/

Corruption

The VA ecosystem is potentially attractive to corrupt PEPs. For example, the VASP BTC-e, headquartered in Russia, laundered proceeds of crime by knowingly facilitating transactions involving public corruption, ransomware, computer hacking, tax refund fraud schemes and drug trafficking. However, no cases of corruption linked to VAs had been reported in Mauritius at the time of the assessment.

Tax Evasion

Based on documented typologies and trends, including the FATF red flag indicators, there is evidence that VA/VASPs are used to evade tax globally. There were no reported cases of tax evasion using VAs/VASPs in Mauritius at the time of the assessment.

Trade-Based Money Laundering

Trade-Based Money Laundering (TBML) is reportedly occurring in the VA sphere globally. According to the US Drug Enforcement Administration (DEA), drug traffickers and money launderers are increasingly underpinning TBML schemes with VAs as they become more widely adopted.[27] However, no cases of TBML linked to VAs have been reported in Mauritius at the time of the assessment.

Emerging threats

The rapidly evolving landscape of VASPs implies that some threats will become more relevant in the future, which requires authorities to analyse them in detail. This Section describes the emerging trends based on international typologies.

Cybercrime

Cybercrime includes a range of criminal activities such as hacking, ransomware, extortion and denial of service which can generate huge illicit VA proceeds that may be almost impossible to trace and recover. Cybercriminals can remain anonymous/pseudo-anonymous, preventing effective investigation of both the predicate offence and its associated money laundering. In 2018, hackers reportedly stole private keys to a billion dollars' worth of VAs from hot wallets, which despite being intrinsically insecure are still used by many custodians to provide a pool of easily accessible liquidity[28].

[27] Trade Based Financial Crime News, "*Virtual currencies increasingly feeding TBML operations says DEA*", 8 March 2021, https://amlnewsflow.coastlinesolutions.com/2021/03/08/virtual-currencies-increasingly-feeding-tbml-operations-says-dea/
[28] CipherTrace "*Cryptocurrency Intelligence - Cryptocurrency Anti-Money Laundering Report, 2019 Q3*", November 2019, https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/

Extortion /Sextortion

Internationally there has been an uptrend in cases of extortion/sextortion in which criminals have demanded payment in VAs, particularly during the COVID 19 Pandemic[29]. There have been a few cases in Mauritius of individuals being blackmailed after they sent sexually explicit photos or videos of themselves to individuals with bogus social media profiles. Payment in the reported cases was demanded in Mauritian Rupees. However, no such cases related to VAs have been reported in Mauritius at the time of the assessment.

Child sexual exploitation

Virtual assets can be used in darknet markets to access child sexual abuse material[30]. At the time of the assessment, no cases of any such activity have been confirmed in Mauritius but this is an emerging global threat.

In 2019, 132,676 URLs or web pages were confirmed by the Internet Watch Foundation (IWF) – UK's national reporting hotline – to contain links to child sexual abuse imagery across almost 5000 domains spanning 58 countries.[31] In 2019 the IWF also identified 288 new dark web sites selling Child Sexual Exploitation Material (CSEM), 197 of which only accepted payment in VAs[32], indicating that VAs are increasingly becoming the preferred choice of payment for such criminal activities.

For example, in 2019, Chainalysis, a blockchain data platform, tracked payments in Bitcoin and Ethereum aggregating approximately USD930,000 to addresses associated with child sexual exploitation material providers, which represented a 32% increase compared to 2018.[33]

ML through VAs/VASPs

At the time of the assessment, there were no known VA/VASP related ML cases in Mauritius. However, based on international typologies, VASPs are exposed to the conventional ML stages of: placement – the entry of the illegal proceeds into the financial system; layering – transactions intended to distance illicit funds from their source; and integration – reintroducing laundered funds as legitimate funds.[34]

[29] News 18, "*Online Sextortion Attacks Increased During Pandemic, Demanded Ransom in Cryptocurrencies*",19 February 2021,https://www.news18.com/news/buzz/online-sextortion-attacks-increased-during-pandemic-demanded-ransom-in-cryptocurrencies-3451043.html
[30] Internet Watch Foundation, "*Annual Report 2019 – Zero Tolerance*", 2019, https://www.iwf.org.uk/report/iwf-2019- annual-report-zero-tolerance
[31] Internet Watch Foundation, "*Annual Report 2019 – Zero Tolerance*", 2019, https://www.iwf.org.uk/report/iwf-2019- annual-report-zero-tolerance
[32] The International Centre for Missing & Exploited Children and Standard Chartered, "*Cryptocurrency and the Trade of Online Child Sexual Abuse Material*", February 2021, https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf
[33] Chainalysis, "*Making Cryptocurrency Part of The Solution to Human Trafficking*", 21 April2020, https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020
[34] Financial Action Task Force (FATF), *"Money Laundering Frequently Asked Questions.",* 20 June 2021, https://www.fatf-gafi.org/faq/generalquestions/

- **In placement**, illicit funds, which may be either in the form of VAs or fiat emanating from drug sales on darknet markets, enter the eco-system through either VA exchanges, peer-to-peer transfers and over-the-counter brokers.
- The **layering** step involves employing a variety of techniques to obfuscate the transaction flow by using multiple VA Exchanges including anonymization tools.
- The **Integration** step involves using fiat eventually placed in banks or other FIs or exchanges to invest in assets and buy goods and services.

In exchange for commissions, fees, or other benefits, professional money launderers provide expertise to criminals to disguise the nature, source, location, control, and destination of illicit funds. And all the avenues available to conventional ML, such as trade-based ML are also potentially available to operators in the VA and VASP space.

TF through VAs/VASPs

TF differs from ML because funds used for financing terrorism may also arise from legitimate sources and only the ultimate use of the funds renders the transaction illegal. VA/VASPs can assist terrorism financiers to avoid detection and tracing of funds. The transnational VA space allows worldwide access to unregulated VASPs which increase the threat of TF. The difficulty in tracking VAs and unregulated VASPs further obfuscates the identity of terrorism funders who typically send small amounts of VAs to proscribed organisations. International typologies indicate that terrorist groups and their supporters are increasingly soliciting "donations" in VA, and that terrorist organisations such as ISIS and Al Qaeda have received "donations" in Bitcoins[35]. However, there were no reported TF-related cases involving VAs in Mauritius.

Assessment of the Input Variables through the Threat Product Dimension

In Mauritius, LEAs have found that VA investments are being made through overseas cryptocurrency exchanges, indicating an appetite for VAs. As mentioned above, the use of VAs via the dark net has been identified in drug trafficking cases. It is apparent that the inherent features of VAs make them more attractive to criminals.

The input variables have been assessed for each VASP channel. The threat ratings in the below table portray general tendencies across all 12 VASP channels combined, among which, the "dark web access", "unregulated environment" and "decentralised environment" have been assessed as "**Very High**".

The other variables as well carry a high threat rating with the exception of few variables such as "Mining by Criminals" which was deemed to be unlikely due to the high price of electricity in

[35] Middle East Media Research Institute, "*The Coming Storm – Terrorists Using Cryptocurrency",* August 2019, https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency

Mauritius and the complex technology required. "Expenditure of Funds", "Regulated", "Centralised Environment" and "High level of accountability product provider" were assessed as 'Low' given that the VA Expenditure was regarded as being unlikely to be widespread in Mauritius and since the VA ecosystem was not regulated and such had no central database for VA transactions.

Table 6: ML/TF Threat Ratings by Input Variables

Characteristics of VAs	Features	Threat (General tendencies across 12 Channels)
VA Nature and Profile	Anonymity/ pseudonymity	High
	P2P Cross-Border Transfer and Portability	High
	Absence of face-to-face contact	High
	Traceability	High
	Speed of Transfer	High
Accessibility to Criminal	Mining by criminal	Low
	Collection of funds	High
	Transfer of funds	High
	Dark Web Access	Very High
	Expenditure of funds	Low
Source of funding VA	Bank or card as source of funding VA	Medium
	Cash transfers, valuable in-kind goods	High
	Use of virtual currency	High
Operational features of VA	Regulated	Low
	Unregulated	Very High
	Centralised Environment	Low
	Decentralised Environments	Very High
Ease of criminality	Tax evasion	High
	Terrorist financing	High
	Disguising criminal proceeds to VA not regulated	High
	Trace and Seize Difficulty	High
Economic Impact	Underground economy – Impact on the country's monetary policy	Medium
	Allow full integration with the financial services market	Medium
	High level of the accountability product provider	Low

Each of the mentioned features has been mapped against the 12 VASP channels to assess their respective risk exposure. The ML/TF threat rating assigned to each identified channel is provided below:

Table 7: ML/TF Threat Ratings by VASP Channels

VASPs	Types of Services	Sub-type	Threat Rating
VIRTUAL ASSET WALLET PROVIDERS	**Custodial Services**	Hot Wallet	High
	Non-Custodial Services	Cold Wallet	High
VIRTUAL ASSET EXCHANGES	**Transfer Services**	P2P	High
		P2B	Medium
	Conversion Services	Fiat-to-Virtual	Medium
		Virtual-to-Fiat	High
		Virtual-to-Virtual	High
VIRTUAL ASSET BROKING	**Payment Gateway**	Merchants	High
VIRTUAL ASSET MANAGEMENT PROVIDERS	**Fund Management**		Medium
	Compliance, Audit & Risk Management		Low
VIRTUAL ASSET INVESTMENT PROVIDERS	**Trading Platforms**	Platform Operators	Medium
		Investment into VA-related commercial activities	Medium

The above table clearly shows that 6 VASP channels- Hot wallet, Cold wallet, P2P, Virtual-to-Fiat, Virtual-to-Virtual and Merchants- stand out as representing a high level of threat. VA Wallet Providers and VA Broking are more exposed to the ML/TF threats compared to VA Management Providers and VA Investment Providers. The lower threat level for these two VASPs in the NBFIs is driven by an operating environment characterized by CDD procedures, known source of funding and non-anonymous interactions. The threat level for the channel Fiat-to-Virtual (Conversion Services) has been rated as **"Medium"** since most transactions are carried out through the banking system.

The ML/TF threat for the Hot wallet channel has been rated as High because even though hot wallets might be under the purview of regulated supervisors, there is a real possibility for criminals to use *unregulated* hot wallets to conceal and eventually transfer illicit funds. Furthermore, transacting using P2P platforms often take place in an unregulated and unsupervised environment which therefore renders this channel particularly attractive for money laundering activities.

Cold Wallets enable the contents of the digital wallets to be stored on a platform or in a manner that is not connected to the internet thereby protecting the wallet from unauthorised access. This is why, even within a regulated environment, cold wallets lack traceability, visibility and are easily transferable from one owner to another, and are therefore highly attractive to money launderers.

Merchants may operate as informal or unlicensed brokers offering VA products in a peer-to-peer manner and thus avoid any supervisory or regulatory oversight.

5. ML/TF INHERENT VULNERABILITY ASSESSMENT

At the time of the assessment, there was no domestically licenced VASP operating in Mauritius, however, authorities are aware of VA transactions taking place and interactions between the formal/informal sector and VASP Channels. Foreign licensed or unlicensed VASPs are transacting with Mauritian individuals or legal persons, but this information is difficult to monitor as there is no universal comprehensive list of licensed VASPs to verify their good standing and licencing status. An analysis of interactions with VASPs shows that the Mauritian market is exposed to both licensed/regulated VASPs and unlicensed/unregulated VASPs.

These include a VASP which the Financial Crimes Enforcement Network (FinCEN) banned in 2019 on regulatory grounds. The exchange then opened a separate exchange registered with the FinCEN to comply with all applicable laws.[36] However, in mid-2021, Bloomberg News reported that the exchange was under investigation by the US Department of Justice and US Internal Revenue Service for suspected money-laundering and tax evasion.[37]

Criminals in Mauritius may, therefore, be able to hide their illicit proceeds through access to regulated, unregulated/licensed and unlicensed VASPs in jurisdictions with weak AML/CFT controls.

Although, at the time of the assessment, there were no licensed VASPs in Mauritius, the banking sector, the NBFI sector and the informal sector interacted with the VA/VASP ecosystem as described in Section 3. The ML/TF inherent vulnerability assessment has been based on the following criteria:

- Licensed in the country or abroad;
- Nature, size and complexity of the business;
- Products and services;
- Methods of delivery of products/services;
- Customer types;
- Country risks;
- Institution dealing with VASPs;
- VA (anonymity) and pseudonymity;
- Rapid transaction settlement; and
- Dealing with unregistered VASPs from overseas.

[36] CapitalCoin.com, "*Binance vs Binance US: What are the differences between the exchanges?*" Sarah, Wurfel, 8 November 2020.
[37] Bloomberg News, "*Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths*", Schoenberg, Tom , 13 May 2021.

Table 8: ML/TF Inherent Vulnerability Ratings by VASP Channels

VASPs	Types of Services	Sub-type	Inherent Vulnerability Rating
VIRTUAL ASSET WALLET PROVIDERS	**Custodial Services**	Hot Wallet	High
	Non-Custodial Services	Cold Wallet	Very High
VIRTUAL ASSET EXCHANGES	**Transfer Services**	P2P	Very High
		P2B	High
	Conversion Services	Fiat-to-Virtual	Very High
		Virtual-to-Fiat	Very High
		Virtual-to-Virtual	Very High
VIRTUAL ASSET BROKING	**Payment Gateway**	Merchants	Very High
VIRTUAL ASSET MANAGEMENT PROVIDERS	**Fund Management**		High
	Compliance, Audit & Risk Management		Low
VIRTUAL ASSET INVESTMENT PROVIDERS	**Trading Platforms**	Platform Operators	High
		Investment into VA-related commercial activities	Medium

The 10 input variables for the vulnerability entity dimension have been assessed for each of the 12 channels. The ML/TF inherent vulnerability associated with channels such as Hot Wallet, Cold Wallet, P2P, P2B, Fiat-to-Virtual, Virtual-to-Fiat, Virtual-to-Virtual, Merchants and Platform Operators was rated as ranging from "**High**" to "**Very High**" while others were rated between "**Low**" to "**Medium**". Input variables such as "Dealing with unregistered VASP from overseas", "VA (Anonymity/Pseudonymity)", "Institution dealing with VASP" and "Rapid Transaction Settlement" increase the inherent vulnerability of the first 8 VASP channels of the above table.

VA Wallet Providers

Wallet Providers are vulnerable to ML/TF abuse because criminals may use them to store and transfer illicit proceeds. Globally, there are multiple Wallet Providers that may provide custody of very high-risk VAs, such as pseudo-anonymous or anonymous VAs. For instance, criminals could use unregulated Hot Wallets to conduct P2P transactions. Similarly, Cold Wallets, even within a regulated environment, lack traceability and visibility, and are easily transferable from one person to another.

The absence of regulatory oversight of VASPs in Mauritius coupled with the lack of visibility of the extent of funds' flows to and from wallets could attract overseas VASPs seeking opportunities for jurisdictional arbitrage.

VA Exchanges

Transfer Services – P2P and P2B

P2P exchanges facilitate transactions between two parties through a platform that neither requires KYC nor imposes any restrictions on trades. Transaction matching is conducted via computer algorithms and clients do not typically need to disclose their identities. P2P exchanges may also act simply as an anonymisation tool, hence increasing the vulnerability to ML/TF abuse. Chainalysis 2020 State of Crypto Crime report highlighted that those factors are increasing the adoption of P2P exchanges by criminals for ML/TF purposes[38].

Conversion Services

VA Exchanges facilitate fiat-to-VA, VA-to-fiat and/or VA-to-VA conversions between customers by matching prospective buyers and sellers. VA Exchanges also typically offer VA custodial services which enable customers to deposit and store their VAs with the Exchange.

Mauritian customers have also used licensed and unlicensed wallet service providers to store their VAs and have subsequently used conversion services to convert VA to fiat and *vice-versa*.

The VA ecosystem allows for near real-time transactional settlements at low cost with minimal KYC in stark contrast to the traditional banking system. These rapid transaction settlement systems are highly attractive to money launderers based on international typologies.

VA Broking

VA Broking is a service which arranges transactions involving VAs and fiat currency through VA Teller Machines, Merchants, and Cards. Globally, reports show that some VA brokers may knowingly provide services to criminals. They purposefully have low KYC requirements and trade their clients' VAs on exchanges. Although the Exchange may have conducted CDD on the broker, the broker's clients and their activities will be unknown to the Exchange. Chainalysis, a VA forensics company, identified that the hundred most active brokers knowingly laundering funds for criminals received more than $3 billion in 2019[39]. Furthermore, PlusToken, the most massive pyramid scheme in 2019, laundered at least $185 million through twenty-eight brokers[40].

The VA/VASP risk assessment exercise showed that a few NBFIs, as well as the informal sector, had or may have had interactions with VA Broking.

[38] Chainalysis, "*The Chainalysis 2020 Crypto Crime Report"*, January 2020, https://go.chainalysis.com/2020-crypto-crime-report
[39] Chainalysis, "*The Chainalysis 2020 Crypto Crime Report"*, January 2020, https://go.chainalysis.com/2020-crypto-crime-report
[40] Chainalysis, "*The Chainalysis 2020 Crypto Crime Report"*, January 2020, https://go.chainalysis.com/2020-crypto-crime-report

Virtual Asset Management provider

Virtual Asset Management Provider includes:

a) Fund Management – Investment fund that focuses on VAs as underlying assets.
b) Compliance, Audit & Risk Management Support – guidance (investment advice) on risk management, management of liquid capital, segregation of assets and custodianship.

Fund Management

In Mauritius, Fund Management operates within a framework which recognises digital assets[41] as an asset-class[42] suitable for specific classes of investors. The VA/VASP risk assessment exercise did not identify any cases of Fund Management related to VAs. Nevertheless, the assessment took into consideration the inherent vulnerability of Funds in relation to VAs.

Funds can invest in a wide variety of products, ranging from traditional securities to more complex products such as derivatives and digital assets. Although traditional Fund Management is well regulated, the assessment showed there was no specific VA/VASP AML/CFT training for staff of FIs.

Compliance, Audit & Risk Management- (investment advice) on risk management, management of liquid capital, segregation of assets, custodianship.

The FSC issues Investment Adviser Licences (Restricted or Unrestricted) to allow FIs to provide investment advice to clients as their core activity. Investment advisers do not hold any VA, nor do they interact directly with VASPs.

The assessment is based on the above interaction of the Investment Advisers with VAs. In two cases identified, the Investment Advisers are providing restricted investment advice to their clients for such VA investments as Bitcoin, Dash, and crypto tokens. There is a risk that Investment Advisers may not be fully conversant with the inherent risks of VAs when extending such advice to their clients.

Virtual Asset Investment Provider

Investment into VA-related commercial activities

The vulnerability of investment vehicles stems from a combination of factors which include: client base (PEPs, high-risk jurisdictions and institutional investors); and the use of complex legal structures (which may obscure beneficial ownership and transaction trails). The assessment showed that the percentage of investment in VAs was insignificant.

[41] The FSC has adopted the definition of the term "Cryptocurrency" provided by the Financial Action Task Force (FATF) in its publication entitled Virtual Currencies – Key Definitions and Potential AML/CFT Risks, June 2014. According to the FATF, Cryptocurrencies, a category of Digital Assets, are a math-based, decentralised convertible virtual currency which are protected by cryptography and are used as a medium of exchange and/or a unit of account and/or a store of value but do not have legal tender status.
[42] Guidance Recognition of Digital Assets as an asset-class for investment by Sophisticated and Expert Investors

Platform Operators

Virtual asset trading platforms are online platforms which match buyers' and sellers' orders for trading in VAs, and they perform functions like traditional securities brokers, stock exchanges and private trading venues[43]. The assessment identified one case for Platform Operators interacting with an FI but the size and nature of the business were minimal, compared to the overall activity of the FI itself.

The Assessment of NBFI's Vulnerability

FIs are already subject to the full range of applicable obligations under the FIAMLA, however it is possible that the traditional licensing requirements might not cover pertinent characteristics of VAs. Existing licensing criteria, at the time of the risk assessment, did not evaluate FIs' capacity in terms of resources, qualified staff and compliance requirements to perform the function of a VASP, nor did the internal control mechanisms evaluate their capacity to effectively deal with unlicensed VASPs.

As mentioned above, pursuant to the FIAMLA, FIs must identify UBOs of their customers, verify their identities, and maintain up to date customers' information. Nevertheless, most FIs, particularly those dealing in the Global Business sector, target an international client base, where there can be non-face-to-face business relationships. Since the non-face-to-face transactions entail higher risks, the FI would need to increase the level of transaction monitoring.

Furthermore, as an underlying investment of Funds, VAs, such as Monero, have anonymity-enhanced features which increase opacity and concomitantly the vulnerability of the FI.

The assessment revealed that the identified FIs interacted with VAs such as *Bitcoin, Litecoin, Tezos, Ethereum and Dash* which are traceable on the blockchain. However, the use of mixers and tumblers may obscure the VA transaction trail and FIs may be vulnerable to ML/TF risks if they lack skilled staff or the required technology for transaction monitoring.

The client profile of the FIs is deemed high risk because the client base includes PEPs, clients from high-risk jurisdictions, institutional investors and complex legal structures which may obscure beneficial ownership.

In most identified cases, transactions in VAs emanated from countries which were not regarded as high-risk jurisdictions. Nevertheless, with the ever-changing dynamics in the VA/VASP space, criminals may exploit countries with weak or non-existent AML/CFT measures for VAs by creating layers of complex structures to integrate illicitly derived funds into the financial system.

The risk assessment further assessed whether FIs could have interactions with different VASPs such as Wallet Providers and Asset Exchanges, which may or may not be regulated/ licensed, and therefore may not be subject to supervision. In the absence of any guidance to FIs concerning unregulated VASPs, FIs are vulnerable to VA/VASP ML/TF risks.

[43] Stevenson, Wong & Co,"*Further Development of Regulatory Approach towards Virtual Asset Portfolio Managers, Fund Distributors and Trading Platform Operators*", 12 June 2019, https://www.sw-hk.com/news-20190612-1/

6. OVERALL ML/TF RISK

The table below depicts the VA/VASP ML/TF threat, inherent vulnerability and residual risk ratings *vis-à-vis* the VASP channels.

Table 9: Summary of ML/TF Risk Rating by VASP Channels

VASPs	Types of Services	Sub-type	Threat Rating	Inherent Vulnerability Rating	Total Risk Rating	Residual Risk Rating
VIRTUAL ASSET WALLET PROVIDERS	**Custodial Services**	Hot Wallet	High	High	High	High
	Non-Custodial Services	Cold Wallet	High	Very High	Very High	Very High
VIRTUAL ASSET EXCHANGES	**Transfer Services**	P2P	High	Very High	Very High	Very High
		P2B	Medium	High	High	High
	Conversion Services	Fiat-to-Virtual	Medium	Very High	Very High	Very High
		Virtual-to-Fiat	High	Very High	Very High	Very High
		Virtual-to-Virtual	High	Very High	Very High	Very High
VIRTUAL ASSET BROKING	**Payment Gateway**	Merchants	High	Very High	Very High	Very High
VIRTUAL ASSET MANAGEMENT PROVIDERS	**Fund Management**		Medium	High	Medium	Medium
	Compliance, Audit & Risk Management		Low	Low	Low	Low
VIRTUAL ASSET INVESTMENT PROVIDERS	**Trading Platforms**	Platform Operators	Medium	High	Medium	Medium
		Investment into VA-related commercial activities	Medium	Medium	Medium	Medium

Based on the risk ratings across all the channels, the overall ML/TF residual risk associated to VA/VASP is considered to be **"Very High"** after considering mitigating measures at the time of assessment.

7. CONCLUSION AND WAY FORWARD

The findings and ratings in this report are based on the prevailing conditions and the regulatory landscape as at end November 2021, when the risk assessment was completed. This exercise culminated in an ML/TF risk rating of **"Very High"** pertaining to VA/VASP related activities.

Given the evolving nature of new technologies and after the recent changes in the regulatory landscape, the risk rating assigned in this assessment may well change in the next VA/VASP risk assessment exercise.

This VA/VASP risk assessment led to the development of an action plan to be implemented in phases and which incorporates high and medium priority measures, and quick wins, spanning VA/VASP-related strategic, regulatory, operational, and supervisory measures to holistically mitigate ML/TF risks in the country.

One of the main shortcomings identified was the lack of a comprehensive legislative framework governing the VA/VASP ecosystem. The Virtual Asset and Initial Token Services Act, which came into force on 7th February 2022, has now made good that shortcoming and designates the FSC as the VASP supervisory authority. All VASPs are subject to risk-based supervision by FSC. VASPs are categorised as FIs and must apply a reasonable and proportionate risk-based approach in respect to AML/CFT.

Proposed actions to address the gaps identified during the risk assessment exercise include, *inter alia*:

- All entities conducting VA/VASP related activities should be registered and licenced as VASP by the FSC and comply with FIAMLA, FIAMLR, UNSA and AML/CFT Guidance;
- Supervised institutions should also implement risk management systems proportionate to the scale and complexity of VA related activities, conduct internal risk assessments, give staff training relevant to VA/VASP sector, and have the appropriate tools and processes to monitor VA transactions and identify their originators and beneficiaries;
- As VAs are highly volatile and speculative assets, financial institutions[44] should help customers and stakeholders towards avoiding excessive exposure to VA/VASP risks that might jeopardise their financial wellbeing. It is therefore necessary for financial institutions to increase customers' and investors' understanding of VAs and their education should be prioritised as a key strategy;
- LEAs and Supervisory staff should continuously undergo appropriate VA/VASP related training to enhance their investigating and monitoring capabilities; and
- Mauritian intelligence agencies and competent authorities should also enhance cooperation protocols and MOUs for exchanging VA/VASP related information and cooperation with each other and with their foreign counterparts.

[44] *Financial institutions include banks and FSC's licensees*

GLOSSARY

Terms	Definition
AEC	Anonymity-Enhanced Coin
AGO	Attorney General's Office
AML	Anti-Money Laundering
BIS	Bank for International Settlements
BOM	Bank of Mauritius
CSEM	Child Sexual Exploitation Material
CDD	Customer Due Diligence
CFT	Combatting the Financing of Terrorism
CSP	Company Service Provider
DPMS	Dealer in precious metals and stones
DNFBP	Designated Non-Financial Businesses and Professions
EDB	Economic Development Board
FATF	Financial Action Task Force
FI	Financial Institution
FIAMLA	Financial Intelligence and Anti-Money Laundering Act
FIAMLR	Financial Intelligence and Anti-Money Laundering Regulations
FIU	Financial Intelligence Unit
FSA	Financial Services Act
FSC	Financial Services Commission
GDP	Gross Domestic Product
GRA	Gambling Regulatory Authority
IA	Investment Adviser
ICAC	Independent Commission Against Corruption
ICC	Interagency Coordination Committee
IRSA	Integrity Reporting Services Agency
KYC	Know Your Customer
LEA	Law Enforcement Authority
MC	Management Company

Terms	Definition
MIPA	Mauritius Institute of Professional Accountants
ML	Money Laundering
MOU	Memoranda of Understanding
MPF	Mauritius Police Force
MRA	Mauritius Revenue Authority
MUR	Mauritian Rupee
NBFI	Non-Bank Financial Institution
NRA	National Risk Assessment
NRSL	National Regulatory Sandbox License
P2P	Peer-to-Peer
P2B	Platform-to-Business
PEP	Politically Exposed Person
PF	Proliferation Financing
RBS	Risk-Based Supervision
REA	Real Estate Agent
ROA	Registrar of Associations
ROC	Registrar of Companies
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCSP	Trust and Corporate Service Providers
TF	Terrorism Financing
TOE	Traditional Obliged Entity
UBO	Ultimate Beneficial Owner
UNSC	United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions
URL	Uniform Resource Locator
USD	United States Dollar
VA	Virtual Asset
VARA	Virtual Asset Risk Assessment
VASP	Virtual Asset Service Provider

REFERENCES

1. Bloomberg NewsSchoenberg, Tom (13 May 2021) "Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths", Schoenberg, Tom, 13 May 2021, Bloomberg News. Retrieved 27 June 2021.
2. Buy Bitcoin Worldwide, “Buy Crypto & Bitcoin in Mauritius” 10 December 2021, https://www.buybitcoinworldwide.com/mauritius/
3. CapitalCoin.com, "Binance vs Binance US: What are the differences between the exchanges?" Sarah, Wurfel, 8 November 2020.
4. Chainalysis, “Making Cryptocurrency Part of The Solution to Human Trafficking”, 21 April 2020, at https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020
5. Chainalysis, “The Chainalysis 2020 Crypto Crime Report”, January 2020, https://go.chainalysis.com/2020-crypto-crime-report
6. Chainalysis, “The Chainalysis 2020 Crypto Crime Report” January 2020, https://go.chainalysis.com/2020-crypto-crime-report
7. CipherTrace “Cryptocurrency Intelligence - Cryptocurrency Anti-Money Laundering Report, 2019 Q3”, November 2019, https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/
8. CoinMarketCap, “Global Cryptocurrency Charts Total Cryptocurrency Market Cap”, https://coinmarketcap.com/charts/
9. Financial Action Task Force (FATF), “Money Laundering Frequently Asked Questions.”, 20 June 2021, https://www.fatf-gafi.org/faq/generalquestions/
10. Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to, Virtual Assets and Virtual Asset Service Providers, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html
11. Financial Crimes Enforcement Unit, FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales, https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware
12. Financial Intelligence Unit, “Guidance Note - Suspicious Transaction Reports”, Updated November 2020, http://www.fiumauritius.org/English/Seminars/Documents/8June20/Guidelines%20DPMS%20FInal.pdf
13. Financial Stability Institute (FSI) of the Bank for International Settlements (BIS)FSI Insights on policy implementation, “Supervising cryptoassets for anti-money laundering”, April 2021, https://www.bis.org/fsi/publ/insights31.htm
14. Gadgets 360, Cryptocurrency, “Crypto Scam Websites Registered 9.6 Million Visits From India in 2021: Report”, 17 January 2022, https://gadgets.ndtv.com/cryptocurrency/news/india-crypto-scam-websites-chainalysis-2712975

15. Internet Watch Foundation, "Annual Report 2019 – Zero Tolerance", 2019, https://www.iwf.org.uk/report/iwf-2019- annual-report-zero-toleranceInternet
16. Middle East Media Research Institute, "The Coming Storm – Terrorists Using Cryptocurrency", August 2019, https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency
17. ML/TF Vertical Risk Assessment, "Virtual Asset Service Providers", December 2020, https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf
18. Mondaq, "Mauritius: Cryptocurrency - Developments In Mauritius", 26 March 2018, https://www.mondaq.com/fin-tech/686384/cryptocurrency--developments-in-mauritius
19. News 18, "Online Sextortion Attacks Increased During Pandemic, Demanded Ransom in Cryptocurrencies",19 February 2021, https://www.news18.com/news/buzz/online-sextortion-attacks-increased-during-pandemic-demanded-ransom-in-cryptocurrencies-3451043.html
20. Statista, "Market capitalization of Bitcoin from April 2013 to February 6, 2022." https://www.statista.com/statistics/377382/bitcoin-market-capitalization/
21. Stevenson, Wong & Co, "Further Development of Regulatory Approach towards Virtual Asset Portfolio Managers, Fund Distributors and Trading Platform Operators", 12 June 2019, https://www.sw-hk.com/news-20190612-1/
22. The Financial Intelligence and Anti-Money Laundering Act 2002
23. The Financial Intelligence and Anti-Money Laundering Regulations 2018
24. The International Centre for Missing & Exploited Children and Standard Chartered, "Cryptocurrency and the Trade of Online Child Sexual Abuse Material", February 2021, https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf
25. The Securities Act 2005
26. The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008
27. The United Nations(Financial Prohibitions, Arms Embargo and Travel Ban)Sanctions Act 2019
28. The Virtual Asset and Initial Token Offering Services Act 2021
29. Trade Based Financial Crime News, "Virtual currencies increasingly feeding TBML operations says DEA", 8 March 2021, https://amlnewsflow.coastlinesolutions.com/2021/03/08/virtual-currencies-increasingly-feeding-tbml-operations-says-dea/
30. UK, National Risk Assessment of Money Laundering and Terrorist Financing, https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020
31. Wired, "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster", 3 March 2014, https://www.wired.com/2014/03/bitcoin-exchange/