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

Co-operative Republic of Guyana

AML/CFT/PF National Coordination Committee

July 2023 (Updated August 20230

EXECUTIVE SUMMARY

Guyana, although a small country in South America with a primarily cash-based economy, is well aware of the phenomenon, related to virtual assets (VAs) and Virtual Assets Service Providers (VASPs).

The rapid development of VAs is a worldwide phenomenon which in turn has fueled the growth of VASPs. However, while VAs and VASPs are fast becoming part of the financial landscape throughout the Caribbean region, there is presently no single source of information outlining the various regulatory, legal or other approaches concerning ML/TF/PF and related risk mitigation for VAs and VASPs that have been taken, if any, regulatory, legal or otherwise, within the region.

Further. there has been worldwide recognition of virtual assets, and as a result, focus on this area has increased, and these assets have become the focus of attention for all users, regulators and decision makers, including the Financial Action Task Force, the global standard-setter for combating money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

Following the recommendations of the Financial Action Task Force (FATF) and its amendments, especially Recommendation No. (15), which requires countries , among many things , to identify, assess and understand the ML/TF risks emerging from activities of virtual assets (VA) and the activities of Virtual Asset Service Providers (VASPs), the report contributes towards meeting these requirements, which was prepared by an assessment team composed of all relevant competent authorities, including the Bank of Guyana, the Guyana Securities Council, the Financial Intelligence Unit, the Guyana Revenue Authority and law enforcement agencies such as the Special Organised Crime Unit (SOCU) and the Office of the Director of Public Prosecutions (DPP).

Private sector engagement was also key, with participation from financial institutions, and DNFBPs such as trust and company services providers, as well as a payment services provider (PSP).

The authorities in Guyana are alert to new challenges and threats, such as those posed by VAs and 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. Guyana has, in preparation for its 4th Round Mutual Evaluation by the Caribbean Financial Action Task Force (CFATF), and to prepare its financial sector for facing any circumstances related to VAs and VASPs, 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 is based on the World Bank tool and will enable Guyana to fully prepare itself in dealing with VA and VASP related issues. Based on this methodology, and where the FATF determined that the ML/TF risks related to the activities of VAs and VASPs must be evaluated, the above methodology was relied upon to determine the activities that should be evaluated, whether those related to VAs or VASPs.

Key Findings

The assessment team noted in the VASP Assessment Perimeter of the Risk Assessment Tool, that there were 7 types of VASPs to choose from that are operating in your jurisdiction, with or without licence. These VASPs are as follows:-

- Virtual Asset Wallet Providers
- Virtual Asset Exchanges
- Virtual Asset Broking / Payment Processing
- Virtual Asset Management Providers
- Initial Coin Offering (ICO) Providers
- Virtual Asset Investment Providers and
- Validators / Miners/ Administrators.

Each of these VASPs provide a number of channels such as, Hot Wallet, Cold Wallet, Custodial and Non-Custodial services, which amount to 27 channels.

Whilst Guyana does not have any VASP operations, the assessment team found it prudent to do strategically perform the assessment in terms of the types of products and services that may be offered by the VASPs, in relation to the mitigating measures which Guyana has.

Guyana has also, based on the Guyana Compliance Commission Act No 14 of 2023, will place advertisements out to the general public to detect the operation of VASPs in the jurisdiction.

Whilst variables were inputted for all types of VASPs, the assessment team found the most applicable ones were as follows -

TYPE OF VASP	# OF CHANNELS	TYPE OF CHANNELS	RELATED SECTORS
Virtual Asset Exchanges	5	• Fiat to Virtual • Virtual to Fiat • Virtual to Virtual • Peer-to-Peer and • Platform to Business	• Banking • Informal • Designated Non Financial Business and Professions (DNFBPs)
Virtual Asset Wallet Providers	2	• Hot Wallet • Cold Wallet	• Non Bank Financial Institutions (NBFIs) • Informal • DNFBPs
Virtual Asset Management Providers	2	• Fund Management • Compliance, Audit and	• NBFIs

		Risk Management	
Virtual Asset Investment Providers	2	• Platform Operators • Investment into VA-related commercial activities	• NBFIs
Virtual Asset Broking	1	• Merchants	• Informal • DNFBPs

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

The analysis also indicated, in keeping with the 2021 ML/TF National Risk Assessment, that drug trafficking and fraud are the main predicate offence risks associated with the VA/VASP ecosystem in Guyana.

The combined ML/TF inherent vulnerability ratings across the 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, whether in Guyana (which is not currently permitted) or outside of Guyana, inclusive of whether that VA was registered at all.

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

A strategic plan will be necessary to address the regulatory, administrative and operational gaps identified during the assessment.

TABLE OF CONTENTS

1. INTRODUCTION

The Global reach of Virtual Assets (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 June 2023, the total market capitalization of all crypto assets, including stablecoins and tokens, amounted to almost US$ 1.6 trillion[3]; in a downward trend after it reached over USD 2.6. trillion around November 2021; however, it is expected that at some point, it will pick back up and an upward trend will be likely. continue.

The FATF 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 USD $10 billion worth of VAs were used for ML purposes. 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 economies6 and posing significant challenges for VASPs, supervisors and Law Enforcement Agencies (LEAs).

Virtual Assets (VAs) appear to be here to stay. Some jurisdictions have fragmented VA regulatory regimes, whilst others advocate the outright ban of VAs and VASPs.

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-

[1] Statista, "Market capitalization of Bitcoin from April 2013 to June 14 2023." https://www.statista.com/statistics/377382/bitcoin-marketcapitalization/
[2] Supra
[3] https://coinmarketcap.com/charts/

"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."

VA/VASP Ecosystem in the Caribbean region

Among the CFATF member jurisdictions, the Bahamas, Bermuda and the Cayman Islands were the first countries to regulate VASPs. Bermuda passed the DAB Act in 2018, and created one of the first FinTech-specific regulatory regimes. The Cayman Islands, with its Virtual Asset Service Providers Act, and The Bahamas with its DARE Act, followed later on.

The Bahamas, Bermuda and the Cayman Islands have each built a legal and regulatory architecture to bring balance between encouraging innovators, while demonstrating soundness, safety, and the protection of customers' interests and the VAs ecosystem.

Jurisdictions in the Caribbean have also been following suit in the passage of VA and VASP related legislation. In June 2023, Dominica's passed the Virtual Assets Business Act 2023 into law. The British Virgin Islands also has such legislation, entitled the Virtual Assets Service Providers Act 2022. St. Vincent and the Grenadines also followed suit with a Virtual Assets Act 2022. Anguilla has a Utility Token Act 2018 and are currently undergoing consultations for a Digital Assets Business Bill 2023.

Belize, however, has taken the step to restrict VAs and VASP activities by way of section 81 of its Financial Service Commission Act 2023.

VA and VASP Definition

Virtual Assets – Definitions; Regulated and Unregulated activities

The FATF uses the term "virtual asset" to refer to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value.

The FATF emphasises that virtual assets are distinct from fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which is the money of a country that is designated as its legal tender.

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.

Such 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.

The VAs have many potential benefits. They can make payments easier, faster, and cheaper; and provide alternative methods for those without access to regular financial products. However, without proper regulation, they create new opportunities for criminals and terrorists to perpetrate predicate offences , launder their proceeds or finance their illicit activities.

Even though regulating VASPs is challenging, national authorities need to develop skills to understand the technology involved, while the VASPs have to learn about and abide by the regulatory rules that now apply to their sector.

In October 2018, the FATF updated its Standards to extend AML/CFT requirements to VAs and VASPs. In June 2019, the FATF adopted an INR.15 to clarify how the FATF requirements apply in relation to VAs and VASPs.

The FATF recommends all countries to apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF/PF risks are commensurate with the risks identified in their respective jurisdictions.

VASP

The FATF defines VASPs within its Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (updated June 2023) as follows: -

'Any natural or legal person who is not covered elsewhere under the 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.'

2. OBJECTIVES

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 Guyana. 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 Guyana; and

▪ inform the ML/TF risk assessment of regulated entities and their risk management approaches

3. METHODOLOGY

Guyana 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, Guyana established a Risk Assessment Working Group composed of all relevant competent authorities.

The working group comprised representatives from the Bank of Guyana (BOG), the Attorney General's Chambers, the Gaming Authority, the Guyana Securities Council, the Special Organised Crime Unit of the Guyana Police Force (SOCU), the Financial Intelligence Unit (FIU), the Guyana Revenue Authority (GRA), and the Commercial and DeedRegistry.

Consultations were also held with the private sector, inclusive of a survey questionnaire which provided useful data, trends and reflections, for the purpose of analysis and formulation of recommendations for this risk assessment, inclusive of two commercial banks, three trust and securities companies, and a payment service provider.

Risk Assessment Tool

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

a) *Assessment of applicable VASP channels in Guyana*

The starting point is to identify the relevant VASP channels with which the Traditional Obliged Entities (TOE), in the different sectors in Guyana as well as the informal sector, interact.

The tool provides 27 VASP Channels (refer to Table 1).

The Report will also provide a detailed insight into the nature of the interaction between, on the one hand, Traditional Obliged Entities (TOE) and VAs/VASPs and, on the other, between the informal sector and VAs/VASPs.

Table: 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
		15. Virtual-to-Virtual
	Investment	16. Development of Products & Services
		14. Fiat-to-Virtual
		10. Cards
VIRTUAL ASSET MANAGEMENT PROVIDERS	11. Fund Management	
	12. Fund Distribution	
	13. Compliance, Audit & Risk Management	
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
INITIAL COIN	Fund Raising	

OFFERING (ICO) PROVIDERS	Other Offerings	17. Security Token Offerings (STOs) 18. Initial Exchange Offerings (IEOs)
19. Platform Operators VIRTUAL ASSET INVESTMENT PROVIDERS	Trading Platforms	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 : 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 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 Guyana

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 Commercial Banks, NBFIs, Trust and Company Service Providers, Casinos, Dealers in Precious Metals, Precious and Semi Precious Stones, Real Estate Agents and Brokers, Accountants/Auditors, and Attorneys-at-Law were assessed against all the 27 VASP channels.

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 in the risk assessment tool 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, Guyana 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 refers to vulnerability as "*weaknesses or gaps that may be exploited by the threat or may facilitate its (the threats) activities*."

The Risk Assessment Working Group examined the inherent vulnerability of each of the 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.

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 reporting entities;
- 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, regional and domestic policies and legislation;
- 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 VAs related activities. One plausible reason for this could be that the VA ecosystem is relatively new in the Guyanese 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 Guyana 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.

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.

The analysis was also based on information since Guyana did not determine any VA activities, nor were there unreported or undetected cases. There was, however, open source information indicated that a Guyanese national launched a cryptocurrency project entitled 'Andotoken', and it skyrocketed to a whopping US$300,000 market cap just within a few days of launching[4].

The news article indicated that '*the team at AndoToken are not just creating a crypto, for example Bitcoin, but a whole ecosystem of utilities that would create demand for $Ando – the native token of the project. These utilities include several blockchain video games which would be launched on iOS and Android; a social media platform, a non-fungible token (NFT) market place, their own Metaverse, and several DeFi projects for cryptocurrency transactions. Their aim is to build "a one-stop-shop" for all the crypto needs of potential crypto enthusiasts. This means a person can carry out all their transactions without leaving the AndoToken site*.'

[4] https://www.inewsguyana.com/andotoken-a-cryptocurrency-project/

Case Study

A couple accused of fraud, money laundering, acting as a securities company without a licence and facilitating a ponzi scheme which swindled approximately USD $20 million from the pockets of Guyanese indicated their desire to repay debts owed by cryptocurrency.[5] GD, the principal stated in a message to investors who were awaiting repayment, that using cryptocurrency was the best option since cash and cheques are not an option due to the difficulties getting access to the accounts.

In the message, the investors were told that,

"Mr. GD will use an app called CoinZoom where he will transfer bitcoin to the marketers' e-wallet and from there you will immediately sell the bitcoin for US dollars." "Afterwards, you can wire transfer the money to your bank account without any issue. Therefore, I will send a link for you to register on CoinZoom to activate your e-wallet. When you are called in by ACF for your payment, you can walk with your CoinZoom information to do the transfer.'[6]

This was not allowed by the Government of Guyana, who advised all persons that cryptocurrency is not legal tender in Guyana.[7]

As we can see, there was very few examples of matters relating to cryptocurrencies in Guyana. 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.

[5]https://www.kaieteurnewsonline.com/2020/11/11/accused-ponzi-operators-want-to-repay-investors-using-cryptocurrency/
[6] Supra
[7] https://www.kaieteurnewsonline.com/2020/11/12/accelerated-must-know-cryptocurrency-is-not-legal-in-guyana-ag/

4. BANKING SECTOR

Overview

The Banking Sector represents the major area of the financial system where money laundering and terrorist financing activities can be perpetuated and consisted for the six commercial banks, the building society and the deposit taking trust company.

Given the nature of its products and services, the banking sector can be utilized by money launderers and terrorist financiers to transport, disguise and effect financing of their criminal activities.

The banking sector comprises the largest contributor to the non-oil & gas GDP. By the end of December 2022, thefinancial sector remained a significant contributor to GDP with the total financial sector assets equivalent to 92.6 percent of Guyana's non-oil GDP. The banking sector assets were equivalent to 60.5% of non-oil GDP[8].

.

Commercial Banks in Guyana are licenced and governed by the Financial Institutions Act dominate the financial sector.

The Bank of Guyana (BOG)'s mandates include ensuring the stability and soundness of Guyana's financial system. The BOG 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.

[8] Bank of Guyana Annual Report 2022

Risk Appetite

The spectacular upswings and downswings of VAs, have attracted widespread interest from customers worldwide and in Guyana for this type of investment, however, there was skepticism after the various crashes which took place last year.

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 Guyana 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, there was an indication that it was possible that customers could be using services to purchase VAs.

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.

Nonetheless, as per available data, amounts were not deemed as significant, and were commensurate with customers' profiles. All wire transfers 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[9] revealed that a typical large US bank processes over USD 2 billion annually in undetected VA-related transfers.

[9] CipherTrace "Cryptocurrency Intelligence - Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report Risk Assessment Report of VAs & VASPs Page 20 of 45

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.

Case study

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. [10]

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

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 above) illustrated 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.

A defalcation of this magnitude might cause systemic losses in Guyana. There are also risks which arise from VA price volatility, which could potentially undermine the financial position of consumers.

5. NON BANK FINANCIAL INSTITUTIONS

NBFIs in Guyana are supervised by the BOG and the Guyana Securities Council and are subject to AML/CFT requirements under the (list subject legislation and AML/CFT legislation).

All NBFIs under the purview of the BOG and the GSC, must apply a reasonable and proportionate risk-based approach in respect to AML/CFT.

Furthermore, NBFIs are subject to risk-based supervision through BOG's and GSC's offsite and onsite AML/CFT annual supervisory programme. This ensures that NBFIs adopt mitigating measures commensurate with the risks identified.

In addition, the AML/CFT Act 2009 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, no licensable activity was permitted. A policy decision was made to prohibit VA and VASP related activities. The Guyana Compliance Commission Bill, with the Commission being looked upon as a future regulator in this area, prohibits the use and exchange of VAs, as well as VASP related operations and activities in Guyana.

VA and VASP activities were designated as activities for AML/CFT Supervision by way of amendment to the AML/CFT Act 2023, thus ensuring that the activities fall under the requisite requirements.

6. DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

The DNFBP AML/CFT supervisors in Guyana comprise the GRA, the Guyana Gold Board, The Guyana Geology and Mines Commission, the Chief Cooperatives and Development Officer, the Registrar of Friendly Societies and the Gaming Authority.

The GRA is the AML/CFT supervisory body for auto dealers, real estate agents and pawnbrokers. It is intended that eventually, the AML/CFT supervision of Real Estate Agents and Brokers will come under the Real Estate Agents' Authority.

The Gaming Authority licenses and supervises casinos in Guyana, as well as any other gambling forum.

The GGB is the licensing authority for dealers in precious metals, and performs AML/CFT supervision over that sector.

The GGMC is the licensing body for miners, as well as traders in precious metals, precious and semi precious stones, and dealers in precious an semi precious stones, of which there is AML/CFT supervisory authority.

The CCDO is the licensing and supervisory authority for Cooperatives and Credit Unions.

The RFS is responsible for the formation of friendly societies and the AML/CFT Supervision of charities, friendly societies and any other non profit organsations.

The Commercial and Deeds Registry is responsible for the formation and regulatory supervision of companies, charities, non profit organisations as well as trusts and trust deeds.

The Guyana Compliance Commission under the Guyana Compliance Commission Act, has been designated as the AM/CFT/CPF supervisory authority for Attorneys-at-Law, Accountants, Auditors, Notaries and Trust and Company Service Providers. It is also intended to eventually become the AML/CFT/CPF Supervisory Authority for specific non profit organizations who, on a risk based approach, have been identified in line with the FATF Recommendation 8.

Whilst not an AML/CFT supervisor, a number of DNFBPs report to the FIU, as well as the Guyana Gold Board.

Although this risk assessment reveals that the DNFBPs do not offer VA-related services or interact with VASPs, it is possible that law firms could also be providing advice on the legal aspects of investing in VAs, as seen in the case study above.

On the other hand, Guyanese could individually be engaging with VA/VASPs. For example, the GRA/GA 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.

7. INFORMAL SECTOR

The lack of a regulatory framework for Guyana for VAs and VASPs, at the time of this assessment, poses very high ML/TF risks for this sector.. From information gathered, crypto enthusiasts in informal sectors all over the world, would invest in both the established VAs and nascent ones such as DogeCoin and Shiba Inu. Shiba Inu[11], created anonymously in August 2020, is a decentralized cryptocurrency modelled off Dogecoin.

[11] The Shiba Inu is a breed of canine from Japan

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.

Case study

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[12].

Notable questionnaire responses

VAs nor VASPs are NOT currently regulated. At this time, Guyana must recognize the lack of its technological infrastructure and weaknesses. VAs and VASPs should be prohibited at this time. However, Financial and Non-Bank Financial Institutions should be alert and put measures in place to detect threats related to VAs.

The very nature of VAs allows persons from any jurisdiction to hold a wallet and conduct transactions thus, institutions should be aware of the added risk in their KYC processes.

When Guyana's infrastructure including its legal framework has improved, and all necessary resources are available, Guyana may consider the regulation of VASPs as a first step with respect to ML/TF/PF.

In this way regulation of mainly the subjects that provide access to the blockchain to third parties through transactions with virtual assets, which under VASPS include exchangers, traders or crypto banks.

[12] 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

One financial institution indicated that the only cryptocurrencies native to Guyana/Guyanese appears to be AndoToken, which was launched in 2022, but only has a current market cap of US$3,341, thus illustrating the volatility of cryptocurrencies.

However, Bitcoin and any other cryptocurrencies can be bought by all Guyanese, once they get an account on a cryptocurrency exchange that caters to Guyanese. Any cryptocurrency asset can be traded/exchanged in Guyana via existing cryptocurrency exchanges that allow Guyanese traders.

The bank's policy, however, is to prohibit accounts for and wire transfers to/from VASPs. With the AML/CFT Amendment Bill 2023 proposing a ban on VASPs until 2025, we think our company's stance is in line with regulatory expectations. Our company does, however, allow buying/selling of cryptocurrency via VISA card transactions by our customers.

By viewing VISA transactions conducted on merchant codes attributed to cryptocurrency exchanges and other similar businesses, yes, the Bank can theoretically detect if a customer is transacting business on a cryptocurrency exchange.

The Bank, however, would not be able to say definitively if the transaction occurring on the VASP is a cryptocurrency purchase/sale, as these transactions are not conducted on the VISA card itself, but on the blockchain or inside the app itself. This is similar to the limitation that while the Bank might know that a customer is transacting business on Amazon, the Bank cannot know what the customer is actually buying on Amazon.

The FIU indicated that it is possible to purchase Virtual assets in Guyana but only through the use of an international exchange, However, there is little to no conclusive information to confirm trading volumes locally at this time.

The GRA also indicated that it is not equipped to adequately recover taxes related to crypto currency, but based on the income Tax Act, such activities would be taxable in the framework of the law in Guyana.

Respondents to the Questionnaire were also of the opinion that either the Guyana Securities Council or the Bank of Guyana could be the best AML/CFT supervisory authority for VAs and VASPs related activities.

It was indicated that AML/CFT Supervision of VASPs should entail the same principles of regulations for traditional FIs, but specifically catered for VASPs. These include:

1. Registration and licensing of all qualifying VASPs

2. CDD Requirements for all VASP customers similar to CDD requirements for existing FIs.

3. Suspicious Transaction Reporting, including internally within the VASP to their Compliance Officer, and external reporting to the regulator and FIU.

4. AML/CFT Training of all VASP staff on red flags specific to the VASP industry and product lines.

5. Applicable record-keeping requirements, even if done digitally.

6. Sanctions screening of all transactions.

7. Risk Assessment of all products, services, geographies, and customer types etc.

8. Enabling international cooperation since virtual assets are often borderless.

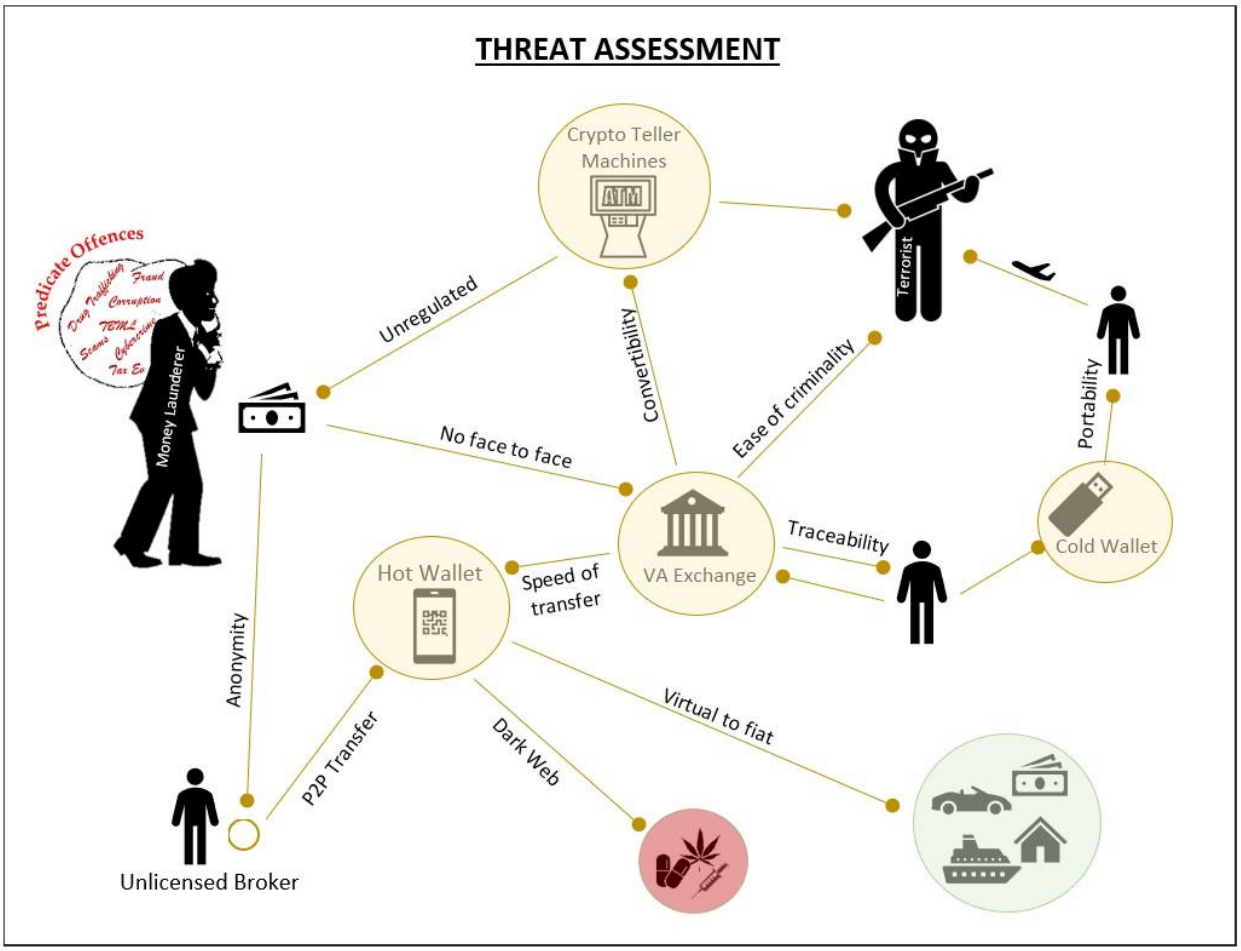
9. Investments in related technology by the regulator, such as in blockchain analytics and

10.A strong enforcement regime that fines, sanctions, and closes VASPs for repeat violations, especially sanctions related issues.

As it stands, with the powers conferred on various agencies and possible conflicts with legislation, the Bank of Guyana and the Guyana Securities Council are the appropriate agencies to regulate and supervise. Considerations to the capacity and restrictions in each regulator's legislation must be considered.

The Guyana Compliance Commission is being considered as the regulator for this industry, however, requisite training and capacity building will be necessary.

8. 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 Guyana 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 2021 NRA, can be laundered through them.

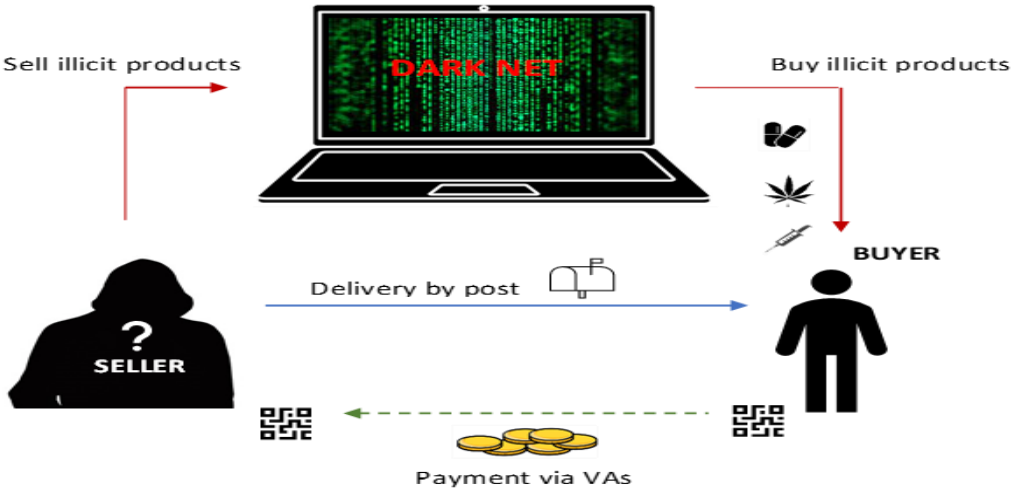
This section details the identified predicate offences associated with the VA/VASP ecosystem based on, inter alia, domestic reported cases to LEAs, intelligence and international case studies[13].

Drug Trafficking

The 2021 NRA identified drug trafficking as having a high ML threat in Guyana[14]. Guyana is still primarily a cash-based society; however, drug traffickers all over the world 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[15].

Multiple online "darknet" markets provide a virtual space for drug dealing. These web-based platforms ensure anonymity and facilitate peer to peer transactions.



[13] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html
[14] Guyana's 2nd National Risk Assessment 2021 pp 14-15
[15] https://go.chainalysis.com/2020-crypto-crime-report

There were no cases identified in Guyana where drug traffickers have used VAs 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

Fraud also was identified as a predicate offence with a high threat for ML[16]. For the review period, the Guyana Police Force (GPF) recorded 116 convictions for fraud related offences. A depiction of this can be seen in the table below-

FRAUD CONVICTIONS COUNTRY-WIDE FOR 2018-2023

OFFENCES	2018	2019	2020	2021	2022	2023
Obtaining Money By False Pretense	17	14	4	8	3	1
Obtaining Credit by Fraud	0	6	6	0	0	0
False Pretence	2	26	0	0	0	1
Fraudulent Conversion	0	0	0	7	0	0
Fraudulent Misappropriation	1	1	3	0	0	0
Falsification of Accounts	1	0	0	0	0	0
Forgery	1	7	0	3	2	2

[16] Page 16 - Guyana's 2nd NRA 2021

TOTAL	**22**	**54**	**13**	**18**	**5**	**4**

VA/VASP related fraud

VA/VASP- related frauds are usually characterised by faked coin offerings, fraudulent investment schemes and faked exchangers using imposter websites. The threat assessment identified one cases of possible VA-related fraud in Guyana, as discussed in the case study above.

These include cases where victims have been induced to pay into fraudulent VA investment schemes promoted by a foreign national. (Also see case study above).

Corruption /bribery

Corruption/bribery has a medium-high ML threat in Guyana[17]. 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 Guyana 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 Guyana at the time of the assessment.

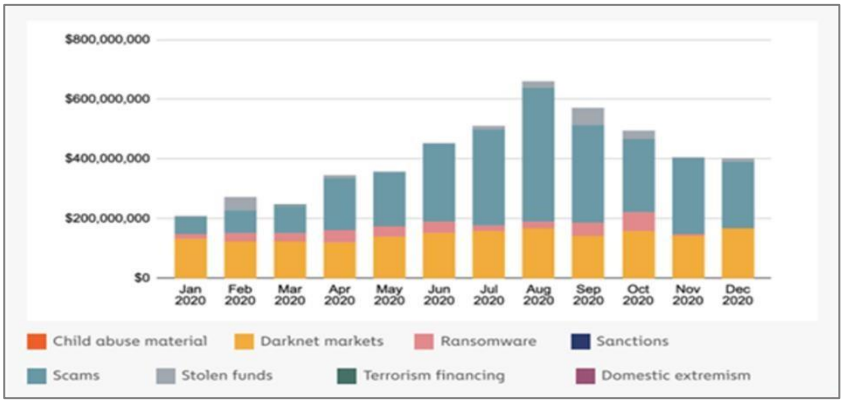
The GRA indicated that the current tax laws do not specifically address virtual assets and will need to be updated/amended in the future to take into account new developments and to establish a connection between taxation and virtual assets due to the fact that tax evasion is a predicate offence with a high ML threat.[18]

[17] Guyana's 2nd NRA, supra
[18] Supra

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 Guyana. It demonstrates the pervasiveness of dark net usage throughout 2020 and the increasing magnitude of scams.

Chart: Total Crypto-currency values received by Illicit Entities in 2020



Source: *The 2021 Crypto Crime Report by Chainalysis*

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.[19] However, no cases of TBML linked to VAs have been reported in Guyana 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.

[19] 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/

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.[20]

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[21]. No such case was detected in Guyana.

Child sexual exploitation

Virtual assets can be used in darknet markets to access child sexual abuse material [22]. At the time of the assessment, no cases of any such activity have been confirmed in Guyana 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.[23]

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[24] , indicating that VAs are increasingly becoming the preferred choice of payment for such criminal activities. For example, in 2019,

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

[21] 9 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-cryptocurrencies3451043.html

[22] Internet Watch Foundation, "Annual Report 2019 – Zero Tolerance", 2019, https://www.iwf.org.uk/report/iwf-2019- annual-report-zerotolerance

[23] Supra

[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-SexualAbuse-Material_03.17.21-publish-1.pdf

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.[25]

ML through VAs/VASPs

At the time of the assessment, there were no known VA/VASP related ML cases in Guyana, other than the case study indicated earlier, which did not directly involve cryptocurrency ML, but an offer to repay in cryptocurrency.

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.[26]

Placement

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-topeer transfers and over-the-counter brokers.

Layering

The layering step involves employing a variety of techniques to obfuscate the transaction flow by using multiple VA Exchanges including anonymization tools.

Integration

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.

[25] https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020
[26] Financial Action Task Force (FATF), "Money Laundering Frequently Asked Questions.", 20 June 2021, https://www.fatfgafi.org/faq/generalquestions/

Further, all the avenues available to conventional ML, such as trade-based ML are also potentially available to operators in the VA and VASP space.

Terrorism Financing (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 Bitcoin[27] .

However, there were no reported TF-related cases involving VAs in Guyana.

Assessment of the Input Variables through the Threat Product Dimension

In Guyana, the LEAs have found that VA investments could be made through overseas cryptocurrency exchanges, which would indicate 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" or "High".

[27] 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

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 lack of stability, coupled with the high price of electricity in Guyana and the complex technology required.

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

Table : 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	High
	Collection of funds	High
	Transfer of funds	High
	Dark Web Access	Very High
	Expenditure of funds	High

Source of funding VA	Bank or card as source of funding VA	High
	Cash transfers, valuable in-kind goods	High
	Use of virtual currency	High
Operational features of VA	Regulated	High
	Unregulated	Very High
	Centralised Environment	High
	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	High
	Allow full integration with the financial services market	High
	High level of the accountability product provider	High

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 : 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	High
	Conversion Services	Fiat-to-Virtual	High
		Virtual-to-Fiat	High
		Virtual-to-Virtual	High
VIRTUAL ASSET BROKING	**Payment Gateway**	Merchants	High
VIRTUAL ASSET MANAGEMENT PROVIDERS	**Fund Management**		High
	Compliance, Audit & Risk Management		High
VIRTUAL ASSET INVESTMENT PROVIDERS	**Trading Platforms**	Platform Operators	High
		Investment into VA-related commercial activities	High

The above table clearly shows that the VASP channels-stand out as representing a high level of threat.

The ML/TF threat for the Hot wallet channel has been rated as High because even though hot wallets could be under the purview of regulated supervisors, there is still a real possibility for criminals to use unregulated hot wallets to conceal and eventually transfer illicit funds.

Further, transacting using P2P platforms often take place in an unregulated and unsupervised environment which may render this channel particularly attractive for ML 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 persons involved in ML.

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.

9. ML/TF INHERENT VULNERABILITY ASSESSMENT

At the time of the assessment, there were no domestically licenced VASPs operating in Guyana. Criminals in Guyana 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.

At the time of the assessment, there were no licensed VASPs in Guyana, and the banking sector, the NBFI sector, the DNFBP sector and the informal sector indicated that they did not interact with the VA/VASP ecosystem as described above.

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.

Table: 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	High
VIRTUAL ASSET EXCHANGES	**Transfer Services**	P2P	High
		P2B	High
	Conversion Services	Fiat-to-Virtual	High
		Virtual-to-Fiat	High

		Virtual-to-Virtual	High
VIRTUAL ASSET BROKING	**Payment Gateway**	Merchants	High
VIRTUAL ASSET MANAGEMENT PROVIDERS	**Fund Management**		High
	Compliance, Audit & Risk Management		High
VIRTUAL ASSET INVESTMENT PROVIDERS	**Trading Platforms**	Platform Operators	High
		Investment into VA-related commercial activities	High

The 10 input variables for the vulnerability entity dimension have been assessed for each of the 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".

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 Guyana 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 – Peer to Peer (P2P) and Peer to Business (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[28] .

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. If using VAs, it is possible that Guyanese 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.

[28] Chainanalysis, supra

Chainalysis, a VA forensics company, identified that the hundred most active brokers knowingly laundering funds for criminals received more than $3 billion in 2019 [29].

Furthermore, PlusToken, the most massive pyramid scheme in 2019, laundered at least $185 million through twenty-eight brokers [30].

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.

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

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.

[29] Supra
[30] Supra

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

The GSC issues Investor Advisor Licences to allow FIs to provide investment advice to clients as their core activity. It was found, based on discussions that the Guyana Securities Council Industry Sensitisation Exercise in August 2023, that investment advisers do not hold any VAs, nor do they interact directly with VASPs.

However, it was recognized that there is a risk that Investment Advisers may not be fully conversant with the inherent risks of VAs if 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 through domestic FIs was insignificant to non existent.

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[31].

The Assessment of NBFIs' and DNFBPs' Vulnerability

FIs and NBFIs are already subject to the full range of applicable obligations under the BOG and GSC respectively however it is possible that the traditional licensing requirements might not cover pertinent characteristics of VAs. This is also the case for DNFBPs.

Existing licensing criteria, at the time of the risk assessment, did not evaluate DNFBPs, FIs' and NBFIs' capacity in terms of resources, qualified staff and compliance requirements to perform the

[31] 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/

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 AML/CFT Act 2009 and its regulations (as amended), DNFBPs, FIs and NBFIs must identify UBOs of their customers, verify their identities, and maintain up to date customers' information.

Non face to face transactions

Since non-face-to-face transactions entail higher risks, the FI would need to increase the level of transaction monitoring. 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.

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.

10.VA and VASP Usage in The Caribbean Region

Usage in the region VAs: Extent of usage

Based on the CFATF Project Report on VAs and VASPs[32], there appears to be relatively limited usage of VAs among CFATF members. Of the 15 respondents to the CFATF survey, a small proportion (6.7%) indicated that there was moderate usage of VAs in their jurisdictions. 13.3% of CFATF respondent jurisdictions reported no usage of VAs in their jurisdiction, and 60% indicated little usage of VAs.

[32] CFATF (2023) Money Laundering & Terrorism Financing Risks Through the use of Virtual Assets and Virtual Asset Service Providers - Implications In The Caribbean Region, page 14

A further 20% of responding CFATF member jurisdictions stated that the volume of usage was not known. This suggests a significant knowledge gap around the popularity and utility of VAs among CFATF members.

Ten (10) CFATF members were able to provide a reasonable estimate of how many residents own or have dealt in VAs. Of the ten (10), 70% assessed that only 6% of residents own or have dealt in VAs, 20% assessed this value at 2% and finally, 10% indicated that just 1% of residents have engaged in this type of activity.

This indicates that even where VAs are utilised, there are only a small proportion of users relative to population size.

VAs: Types of usage

Of 15 responses from CFATF members, VAs are mostly used for investment purposes (46.7%) and to a lesser extent (20%), payment purposes. However, 33.3% of the 15 respondents said the purpose was not known. This demonstrates a further lack of data about general usage in the region.

VAs: Profile of users

Of the 14 responses to the question on what the primary uses of VA were, it was discerned VAs are mostly used by individual non-institutional customers and investors (53.3%).

No corporate entities or companies were identified as using VAs and only 21.4% of responding jurisdictions said that VAs are mostly used by institutional investors. The current usage of VAs is therefore different to traditional fiat financial products and services with a greater emphasis on individual and retail (e.g. non-institutional) customers.

VASPs: Nature, size and complexity

Of 15 CFATF members that responded, 93.3% indicated that they applied the FATF definitions to define VASPs. From the information provided by seven (7) responding CFATF members, VASP entities take various forms, including stand-alone VASPs, commercial banks, offshore banks, trust and Company service providers and administrators. There are also state actors such as the Crypto Asset Treasury of Venezuela.

The Nature of VAs & VASPs

The following factors have been identified as being relevant in the consideration of the risk, based on the nature of the VAs & VASPs:

• Anonymity/pseudonymity;

• Traceability; • Transfer speed;

• P2P transactions;

• Decentralized or centralized exchanges; and

• Convertible/non-convertible.

A lack of centralized control within certain services and structures may increase the risk of anonymity as there is no intermediary oversight.

In the conclusion of the CFATF Report[33], among the participating CFATF members, there is little to no usage of VAs in the region. However, there is a knowledge gap in relation to the popularity and utility of VAs among CFATF members.

VAs are used mostly for investments and payment purposes and are mostly used by individual retail customers and investors. As a result, VA trading platforms and exchanges appear to be the most common type of activity in the region. VASPs appear to be operating in most responding jurisdictions, and in some instances, unlicensed and unregistered.

11.DOMESTIC LEGISLATIVE FRAMEWORK

The AML/CFT (Amendment) Act 2023 places VAs and VASPs under regulated business activity to be supervised under the framework of AML/CFT. This however, cannot take place until at least January 1 2026, as there is a prohibition on the use of VAs and the operation of VASPs in Guyana by way of section 72 of the Guyana Compliance Commission Act.

It is likely that the Compliance Commission will be the licensing and supervisory body for VAs and VASPs in Guyana if there is a policy decision to allow the operation of VAs and VASPs.

[33] Page 33, supra

One of the main shortcomings identified was the lack of a comprehensive legislative framework governing the VA/VASP ecosystem. Legislatively, both the AML/CFT and Securities legislation should be amended to cater for the various virtual asset scams.

These include ponzi schemes, fake initial coin offerings, phishing, fake exchanges, cloud mining scams, pump and dump schemes, investment clubs, and rug pulls. In addition to this, the regulatory framework should be setup in such a way where consumers can have their funds returned in some instances.

As a result, the Government of Guyana has taken a policy decision to prohibit the use of virtual assets and VASPs in Guyana, until policy and legislative measures can be put in place to ensure adequate supervision and regulation of the VA and VASP regime. This can be found by section 72 of the Guyana Compliance Commission Act No 14 of 2023.

12.REGIONAL LEGISLATIVE FRAMEWORKS

Among the CFATF member jurisdictions, The Bahamas, Bermuda and the Cayman Islands were the first countries to regulate VASPs. Bermuda passed the DAB Act in 2018, and created one of the first FinTech-specific regulatory regimes. [34]

The Cayman Islands, with its Virtual Asset Service Providers Act, and The Bahamas with its DARE Act, followed later on. The Bahamas, Bermuda and the Cayman Islands have each built a legal and regulatory architecture to bring balance between encouraging innovators, while demonstrating soundness, safety, and the protection of customers' interests and the VAs ecosystem.

The DAB Act in Bermuda, VASP Act in the Cayman Islands and DARE Act in The Bahamas essentially emphasize the need for service providers to, among other things:

• Exercise due care, skill and diligence.

• Establish and maintain effective security systems.

• Establish and maintain effective corporate governance and robust resilience of their systems.

[34] CFATF (2023) Money Laundering & Terrorism Financing Risks Through the use of Virtual Assets and Virtual Asset Service Providers - Implications In The Caribbean Region

• Have appropriate systems, policies, processes and procedures for the prevention, detection and disclosure of financial crime and to ensure compliance with AML/CFT laws.

• Establish and maintain adequate and effective systems for the protection and segregation of customer assets and data.

Cayman Islands

The VASP Act, which took effect October 31, 2020, empowers the Cayman Islands Monetary Authority to supervise all VASPs, including issuers, custodians, trading platforms and dealers. A full licensing regime was launched in July 2021 and the law implements the FATF's guidance on a riskbased approach for VASPs and its recommended AML/CFT standards.

The next phase of regulation will require VASPs to obtain and hold originator and beneficial ownership information on all transfers of virtual assets under Part XA of the Anti-Money Laundering (Amendment) Regulations of the Cayman Islands. The "Travel Rule", took effect on July 1, 2022 and its successful implementation was critical to investor confidence and security. It demonstrated the Cayman Islands' ability to effectively supervise VAs and those who provide certain services in relation to them.

The Bahamas

The DARE Act, which came into force December 14, 2020, regulates Bahamas-based entities involved in the issuance, sale and trade of digital assets, defined as "any digital representation of value distributed through a distributed ledger technology platform where value is embedded or in which there is a contractual right of use, including a contractual token."

Digital asset businesses within the scope of DARE include token issuers or exchanges, or digital assets payment service providers, as well as those who provide financial services to them. The DARE Act requires the Securities Commission of The Bahamas to regulate and maintain a register of digital asset businesses and initial token offerings.

Bermuda

The scope of Bermuda's DAB Act is similar. Having made clear its intentions to attract and grow a FinTech industry, Bermuda has built a regulatory framework using a risk-based approach.

The DAB regime, overseen by the Bermuda Monetary Authority, caters to Digital Asset Businesses at differing stages of development, offering the F (Full) license; the M (Modified) license, for those planning to expand operations for a limited period; and the T (Test) license for those seeking to test their proof of concept.

Mindful of deterring bad actors and reducing reputational risk to the country, Bermuda incorporates prudential rules into its regime, with requirements including cybersecurity audits and customer due diligence.

Regulators in all three (3) jurisdictions above run efficient registration and licensing regimes. When delays occur, they are often a result of incomplete applications. Compliance is a new challenge for many in a hitherto unregulated sector.

OECS Countries

Dominica, Antigua and Barbuda, St Kitts and Nevis and Saint Vincent and the Grenadines have all passed legislation relating to the regulation and supervision of VASPs and VAs between 2020 and 2023.

Overseas Countries and Territories (OCTs) in the Caribbean region

Anguilla and the British Virgin Islands also have legislation in relation to VAs and VASPs.

13.BEST PRACTICE LEGAL FRAMEWORK – FATF

In June 2019, the FATF released clarification to its guidance to member nations regarding the regulation of VASPs and other crypto entities. In response to the money laundering and terrorist financing risks posed by the virtual assets sector, the updated guidance included a 'Travel Rule'.

This rule requires VASPs to share sender (originator) and receiver (beneficiary) information for cryptocurrency transactions above USD/EUR 1000[35] globally and is a key AML/CFT measure, which mandates that VASPs obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers (as per paragraph 7 of FATF's Interpretative Note to 15). This is similar to so-called Travel Rules that have for years required financial institutions to share this information when executing bank wire transfers and SWIFT electronic funds transfers.

The FATF guidelines require both sending and receiving VASPs to exchange and store originator and beneficiary identification information in addition to the cryptocurrency addresses and transaction identifications for each transaction. Regulators require the latter, since cryptocurrency addresses can be used by multiple beneficiary customers.

For example, some exchanges use a single address to send all transactions. Also, cryptocurrency addresses can be recycled and consequently may be used by multiple customers at a VASP.

Specifically, INR. 16, paragraph 6 prescribes the originator and beneficiary information or equivalent in a virtual asset context on virtual asset transfers to be collected by the originating VASP, shared with the beneficiary VASP or FI and retained for sharing with appropriate authorities if required. This information includes the following:

a) The name of the originator;

b) The originator account number where such an account is used to process the transaction;

c) The originator's physical (geographical) address, or national identity number, or customer identification number, or date and place of birth;

d) the name of the beneficiary;

e) the beneficiary account number where such an account is used to process the transaction; and

[35] Countries may choose to adopt a de minimis threshold for VA transfers of USD/EUR 1 000 in line with the FATF Standards, having regard to the risks associated with various VAs and covered VA activities. If countries choose to implement such a threshold, there are comparatively fewer requirements for VA transfers below the threshold compared to VA transfers above the threshold. For VA transfers under the threshold, countries should require that VASPs collect: (a) the name of the originator and the beneficiary; and (b) the VA wallet address for each or a unique transaction reference number. Such information does not need to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to the customer should be verified.

f) the beneficiary's physical (geographical) address, or national identity number, or customer identification number, or date and place of birth.

14.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: 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	High	High	High
VIRTUAL ASSET EXCHANGES	**Transfer Services**	P2P	High	High	High	High
		P2B	High	High	High	High
	Conversion Services	Fiat-to-Virtual	High	High	High	High
		Virtual-to-Fiat	High	High	High	High
		Virtual-to-Virtual	High	High	High	High
VIRTUAL ASSET BROKING	**Payment Gateway**	Merchants	High	High	High	High
VIRTUAL ASSET MANAGEMENT PROVIDERS	**Fund Management**		High	High	High	High
	Compliance, Audit & Risk Management		High	High	High	High
VIRTUAL ASSET INVESTMENT PROVIDERS	**Trading Platforms**	Platform Operators	High	High	High	High
		Investment into VA-related commercial activities	High	High	High	High

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

15.CONCLUSION AND WAY FORWARD

The findings and ratings in this report are based on the prevailing conditions and the regulatory landscape as at July 2023 when the risk assessment was completed, and now updated in August 2023.

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.

In order to determine whether VASPs are operating in Guyana, it would be important to examine VASP travel rule requires VASPs along with their financial institutions to share relevant originator and beneficiary information from VA transactions, with the aim of preventing Money Laundering, terrorist financing, other fraud activity.

Further, Virtual assets are not available for purchase via any local exchanges. Therefore, it is unlikely that the Guyanese currency would be used to purchase or received virtual assets locally.

However, Virtual assets remain available for purchase in Guyana through the use of an international exchange. It is therefore possible to identify these transactions through close monitoring by banks and/ or MVTAs where the senders or beneficiaries of international money transfers may be entities that facilitate transactions for the trading of VAs.

This rule may assist jurisdictions in obtaining and identifying service providers which operate and provide services to Guyanese. However, this will only apply if VAs and VASPs are regulated by respective jurisdictions. Further, bilateral treaties and MOUs would also be required to facilitate as a secondary measure, information sharing.

These transactions and or activities can be identified with the use of analytical tools such as Block Explorers as well as resources which can pinpoint the location of the IP addresses of the virtual asset wallets. The transactions may also be tracked via the financial system (Banks/ MVTS) if/ when same to used to pay VASPs.

Guyana is limited in that its electricity and cybersecurity systems are lagging, like most Caribbean countries. This poses significant threats to the countries' financial system. Experts are required in these fields and significant investment in resources and software to protect the cyber system.

The Working Group agreed that VA activity should be prohibited in Guyana at this time. However, whilst there is prohibition some action should be taken in relation ML/TF/PF by all supervisory authorities and competent authorities. There will also be aneed for extensive dialogue, and cooperation with foreign counterparts. Active mitigation measures including outreach to private and public sectors, and necessary enforcement actions for the prohibition.

Further risks associated with cross-border VA activities must be mitigated by adopting various strategies, and cooperate with other jurisdictions as required. The FIU Guyana is authorized to share intelligence internationally in relation to VAs and or VASPs related activities in Guyana. However, there have not been any instances at this point in time.

This risk assessments of VAs and VASPs are the first step in mitigating such risks. The legal framework must support these mitigating measures which will allow Guyana to first identify any threat/risk and continue to push for its prohibition/Limitation.

Support will be given to prohibit VAs and VASPs at this time with continuous training of staff to detect VA related threats until Guyana is fully equipped and all supervisory authorities have the resources they need to regulate and supervise VAs/VASPs on a full or limited scale.

Universities should adopt and offer these courses to ensure that adequate (trained) staff will be available when full/limited regulation is adopted. It is important to engage with experienced parties who have a proven track record of VA related intelligence gathering and insights.

Further, these experts provide modern technological tools which greatly enhance and assist the process of blockchain intelligence and analytics. These tools should be utilized given their relative strengths, particularly in cross chain analytics and blockchain intelligence.

This VA/VASP risk assessment will lead 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.

The Guyana Compliance Commission has been tentatively identified as a possible supervisory and licensing authority for VAs and VASPs, with support from the BOG.

The AML/CFT (Amendment) Act 2023 lists all VA and VASP activities as AML/CFT/CPF related activities, and as a result, such activities are expressly under the AML/CFT framework.

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

- Advertisement of a Public Notice to ascertain operation of VASPs or use of VAs in Guyana by the AML/CFT/PF National Coordination Committee and the Guyana Compliance Commission, of which the template is provided at Appendix II;
- Supervised institutions should also implement risk management systems that allow them to detect VA and VASP related activities, conduct internal risk assessments, give staff training relevant to VA/VASP sector, and have the appropriate tools and processes to monitor transactions which may be related to VAs and VASPs and identify their originators and beneficiaries;
- As VAs are highly volatile and speculative assets, financial institutions 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
- Guyanese LEAs, supervisory authorities 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 and
- The design of a strategic plan for the implementation of recommendations will be provided.

APPENDIX I

WORKING GROUP MEMBERS

ORGANISATION	NAME	POSITION
Attorney General's Chambers and Ministry of Legal Affairs	Mr. Rommel St. Hill	Secretary of the AML/CFT/PF NCC and Coordinator for the VA Risk Assessment
Financial Intelligence Unit	Mr. Raphel Bascombe	Financial Analyst
Guyana Revenue Authority	Mrs. Carol Baldeo-Worrell Mr. Brian Wilson Ms. Tricia Jordan	Senior manager, Licence Revenue Office Manager, Law Enforcement Investigations Division Risk Officer/AML/CFT Team Member.
Guyana Securities Council	Ms. Tevera Franklin	Corporate Secretary
Gaming Authority	Mr. Victor Herbert	Compliance Officer
Special Organised Crime Unit	ACP Fazil Karimbaksh	Head
Office of the Director of Public Prosecutions	Ms. Natasha Backer	Assistant Director of Public Prosecutions
Bank of Guyana	Ms. Niranjanie Ramprashad	Assistant Director, Bank Supervision Department
Bank of Guyana	Mr. Imran Khan	Payment Service Provider Division

APPENDIX II

THE ANTI- MONEY LAUNDERING/COUNTERING THE FINANCING OF TERRORISM/PROLIFERATION FINANCING NATIONAL COORDINATION COMMITTEE

PUBLIC NOTICE

RESTRICTION ON VIRTUAL ASSET ACTIVITIES

THE PUBLIC IS HEREBY NOTIFIED OF THE FOLLOWING PROVISIONS OF THE **GUYANA COMPLIANCE COMMISSION ACT NO. 14 OF 2023 (THE ACT),** WHICH SPECIFIES AS FOLLOWS:

1. UNDER SECTION 72(1) - 'NO PERSON SHALL AS A BUSINESS, EXCEPT WHERE LICENSED UNDER THE AFOREMENTIONED ACT, CONDUCT IN OR FROM WITHIN GUYANA ON BEHALF OF ANY OTHER PERSON-

(a) negotiation, brokerage, or exchange, between virtual assets and fiat currencies whether such currency is the legal tender of Guyana or any other country;

(b) negotiation, brokerage, or exchange between one or more forms of virtual assets;

(c) transfer of virtual assets;

(d) loan, deposit, custody, safekeeping, management, or administration of–

(i) virtual assets; or

(ii) instruments enabling control over virtual assets; or

(e) participation in and provision of financial services related to the issuance or an issuer's offer or sale of a virtual asset.

2. UNDER SECTION 72 (3) - "NO LICENSES WILL BE ISSUED UNDER THE ACT FOR ANY ACTIVITY OR OPERATION REFERRED TO IN 1(A) TO (E) ABOVE, ON OR BEFORE THE 31ST DAY OF DECEMBER 2025".

Given the prohibitions at Section 72 (1) and 72(3) above, any person who prior to the commencement of THE ACT , was carrying on an activity or operation referred to in 1(a) to (e) above, must–

(a) within one month of the commencement of **THE ACT**, notify the Secretary of the AMLCFT/PF National Coordinating Committee in writing at asg.sthill@mola.gov.gy, that it has been/ is carrying on such activity or operation; and

(b) within three months of the commencement of the Act, cease such activity or operation.

ANY PERSON WHO HAS FAILED TO ADVISE AS PER THE REQUIREMENT IMMEDIATELY ABOVE IN THIS NOTICE, MUST DO SO WITHIN ONE MONTH OF THE DATE OF THIS NOTICE.

The public is hereby urged to be vigilant of and keep abreast of updates regarding virtual asset activities.

FAILURE TO COMPLY WITH PROVISIONS OF THE GUYANA COMPLIANCE COMMISSION ACT NO 14 OF 2023, SOME OF WHICH IS REINFORCED IN THIS NOTICE, COULD RESULT IN A PERSON BEING LIABLE TO CRIMINAL SANCTIONS IN ACCORDANCE WITH SECTION 72(5) AND (7) OF THE ACT.

CHAIRMAN
ANTI- MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING NATIONAL COORDINATION COMMITTEE
[DATE]

GLOSSARY

AG	Office of the Attorney General
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
BoG	Bank of Guyana
CA	Companies Act
CANU	Customs Anti -Narcotics Unit
CCDO	Chief Co-operative Development Officer
CFATF	Caribbean Financial Action Task Force
CFT	Counter Financing of Terrorism
DC&FS	Department of Co-operatives and Friendly Societies
DNFBPs	Designated Non-Financial Businesses and Professions
DPP	Director of Public Prosecutions
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FT	Financing of Terrorism
GA	Gaming Authority
GA	Gaming Authority
GGB	Guyana Gold Board
GGMC	Guyana Geology and Mines Commission
GoG	Government of Guyana
GPF	Guyana Police Force
GRA	Guyana Revenue Authority
GSC	Guyana Securities Council

IMF	International Monetary Fund
LEA	Law Enforcement Agency
ML	Money Laundering
MLA	Mutual legal assistance
MOF	Minister of Finance
MOHA	Ministry of Home Affairs
NCC	National Coordination Committee
NPOs	Non-profit organizations
PEPs	Politically Exposed Persons
PF	Proliferation Financing
Q1	January to March
Q2	April to June
Q3	July to September
Q4	October to December
RBAP	Risk Based Action Plan
SOCU	Special Organised Crime Unit
STRs	Suspicious Transaction Reports

REFERENCES

1. Chainalysis, “Making Cryptocurrency Part of The Solution to Human Trafficking”, 21 April 2020, at https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020

2. Chainalysis, “The Chainalysis 2020 Crypto Crime Report”, January 2020, https://go.chainalysis.com/2020-crypto-crime-report

3. Chainalysis, “The Chainalysis 2020 Crypto Crime Report” January 2020, https://go.chainalysis.com/2020-crypto-crime-report

4. CipherTrace “Cryptocurrency Intelligence - Cryptocurrency Anti-Money Laundering Report, 2019 Q3”, November 2019, https://ciphertrace.com/q3-2019-cryptocurrency-anti-moneylaundering-report/

5. CoinMarketCap, “Global Cryptocurrency Charts Total Cryptocurrency Market Cap”, https://coinmarketcap.com/charts/

6. 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.fatfgafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

7. 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-exchange110-million-facilitating-ransomware

8. 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

9. 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/indiacrypto-scam-websites-chainalysis-2712975

11. Internet Watch Foundation, “Annual Report 2019 – Zero Tolerance”, 2019, https://www.iwf.org.uk/report/iwf-2019- annual-report-zero-toleranceInternet

12. 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

13. News 18, “Online Sextortion Attacks Increased During Pandemic, Demanded Ransom in Cryptocurrencies”,19 February 2021, https://www.news18.com/news/buzz/online-sextortionattacks-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/

14. 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.

15. 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-OnlineChild-Sexual-Abuse-Material_03.17.21-publish-1.pdf 25. The Securities Act 2005

16. Trade Based Financial Crime News, “Virtual currencies increasingly feeding TBML operations says DEA”, 8 March 2021, https://amlnewsflow.coastlinesolutions.com/2021/03/08/virtualcurrencies-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-launderingand-terrorist-financing-2020

17. Wired, “The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster”, 3 March 2014, https://www.wired.com/2014/03/bitcoin-exchange/

18. Caribbean Financial Action Task Force (CFATF) Project Report on Virtual Assets and Virtual Asset Service Providers - Money Laundering & Terrorism Financing Risks Through the use of Virtual Assets and Virtual Asset Service Providers- Implications In The Caribbean Region (January 2023)