2025 ML/TF RISK ASSESSMENT OF VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, TRINIDAD AND TOBAGO

February 2026

TABLE OF CONTENTS

Disclaimer

This risk assessment is based on information, data and materials available at the time of concluding this report. The assessment reflects the quality, scope and completeness of data accessible during that period and is therefore, subject to data limitations and information gaps. Consequently, the findings, risk ratings and conclusions presented herein may change should additional, updated or more comprehensive information become available. This report should be read in conjunction with these constraints and does not preclude the need for periodic review and reassessment in accordance with a risk-based approach.

GLOSSARY OF TERMS

Term	Definition
Cryptocurrency	Cryptocurrency is a digital asset based on cryptography and distributed ledger technology that facilitates the electronic transfer of value through secure transactions. It generally does not constitute legal tender but may be accepted by natural or legal persons as a means of exchange.
Legal Person	A Legal Person is a company or business other than a natural person.
Money laundering	Money laundering is the process used by criminals to conceal the illegal origin and ownership of funds derived from criminal activities. If successfully undertaken, it allows them to maintain control over those proceeds, the funds lose its criminal identity and appear to be legitimately derived. The money laundering process involves three (3) main stages, namely, placement, layering and integration: a) Placement: refers to the entry of illicit proceeds into the virtual asset (VA) system. The illicit proceeds may have been received in the form of a VA (e.g. from selling drugs on darknet markets and paying in VAs) or in fiat currency. When the proceeds are in fiat, the criminal must first convert them to VAs, typically by transferring the funds to a VA exchange, over-the counter broker or VA ATM. Once converted, the VAs are transferred to a wallet, or a dedicated custodian or any VA safekeeping service. b) Layering: refers to the movement of the funds through a series of transactions designed to obscure their origin and disguise the criminal source by creating the appearance of legitimacy. These transactions often span multiple jurisdictions. VAs have unique technological properties that enable pseudo-anonymous and anonymous transactions, fast cross-border value transfer and non-face-to-face relationships that can be exploited by criminals. Anonymization tools such as mixers can further reduce traceability of illicit funds. c) Integration: refers to the process by which illicit funds re-enter the legitimate economy. This may occur through the withdrawal of funds in fiat to bank accounts, exchanging VAs for cash, or using VAs to invest in real estate, luxury assets and business ventures, or to purchase goods and services.
Non-Fungible Tokens	Non-fungible tokens are digital assets that are unique, rather than interchangeable. They are in practice used as collectibles rather than as payment instruments and can be referred to as crypto-collectibles. NFTs may be viewed as investments by persons purchasing them.
Person	Includes an individual, company, partnership, trust, association and any other organised group or body whether incorporated or unincorporated.
Proliferation Financing	Means the provision of funds or financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons, their means of delivery, and related materials.

Term	Definition
Pseudonymity / Pseudo-anonymous	System where participants are identified by cryptographic addresses or other identifiers rather than legal names, providing a layer of privacy and anonymity.
Remittances	Domestic or International transfers of fiat currency.
Smart Contract	A smart contract is a self-executing digital program that automates the actions required in a blockchain transaction, when specified terms are met, eliminating the need for intermediaries.
Stablecoins	According to the FATF, stablecoins are VAs whose value is kept "stable" through reference to fiat currencies that have legal tender. The entity issuing a stablecoin attempts to reduce its price volatility by pegging its value to some external asset or basket of assets like fiat money or exchange-traded commodities. For example, Tether18 is a privately issued stablecoin whose history points to the need for a clear regulatory framework for private digital currencies.
Terrorist Financing	Terrorist Financing is the process by which funds are provided to an individual or group to finance terrorist acts.
Trust and Company Service Providers	All persons and entities that on a professional basis, participate in the creation, administration and management of trusts and corporate vehicles.
Unhosted or Self-Custody Wallets	An Unhosted or Self-Custody wallet refers to a type of wallet in which the user, rather than a third party service provider, retains control of the private keys and therefore has direct control over the VAs therein.
Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, or used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets covered under any other written law.
Virtual Asset Service Provider	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: 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.

ACRONYMS

Acronym	Meaning
AML/CFT/ CPF	Anti-Money Laundering/ Countering the Financing of Terrorism/ Countering Proliferation Financing
CDD	Customer Due Diligence
CBTT	Central Bank of Trinidad and Tobago
DeFi	Decentralized Finance
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FI	Financial Institution
FIUTT	Financial Intelligence Unit of Trinidad and Tobago
ICO	Initial Coin Offering
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML	Money Laundering
P2P	Peer-to-Peer
P2B	Peer-to-Business
PF	Proliferation Financing
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
TTSEC	Trinidad and Tobago Securities and Exchange Commission
VA(s)	Virtual Asset(s)
VASP(s)	Virtual Asset Service Provider(s)

LIST OF TABLES, CHARTS AND FIGURES

FOREWORD

As Trinidad and Tobago continues to modernise its financial and regulatory architecture, it is imperative that we remain responsive to emerging risks and adaptive to global developments. The rapid adoption of virtual assets (VAs) and growth of virtual asset service providers (VASPs) represent one of the most significant shifts in the international financial system in recent decades. While these technologies offer opportunities for innovation, efficiency, and financial inclusion, equally they present new avenues for money laundering (ML), terrorist financing (TF), proliferation financing (PF) and other illicit activity, that must be effectively addressed.

This National Money Laundering and Terrorist Financing Risk Assessment of VAs and VASPs is the first for Trinidad and Tobago. It reflects the Government's ongoing commitment to fortifying our Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CFT/CPF) framework and ensuring alignment with the Financial Action Task Force (FATF) Standards, particularly Recommendation 15. The objective of the risk assessment is to aid the country in recognizing potential threats and vulnerabilities arising from the adoption of VAs and the activities of VASPs, and to formulate appropriate mitigating strategies to safeguard the integrity of the country's financial system, while fostering innovation, inclusion and consumer protection.

The assessment noted the growing domestic VA/VASP ecosystem promoting alternative investments and commercial activity among others. The growth is driven by factors such as our citizens' increasing interest in VAs, and the emergence of blockchain start-ups and Fintech. In parallel, there has been a proliferation of fraudulent investment schemes and scams seeking to exploit the vulnerable in our society. The findings set out in this report present the sector's exposure to ML/TF threats and, the inherent vulnerabilities in the VAs and VASPs and limitations in national mitigating measures that could be exploited by illicit actors.

Importantly, the assessment charts the course for the legislative, regulatory, and institutional reforms required to safeguard the financial system while enabling responsible technological advancement. This report is timely, with the introduction of the Virtual Assets and Virtual Assets Service Providers Act, 2025. The legislation represents one of several government initiatives for progressive digital and technological transformation in the financial system, and aims to introduce regulatory clarity while balancing innovation with financial stability and consumer protection. As Attorney General, I affirm this Government's unwavering commitment to addressing these matters with urgency, transparency, and strategic purpose.

I take this opportunity to acknowledge that this assessment was made possible through the collaboration of a dedicated Working Group of public and private sector partners, supported by the technical expertise of the EU AML/CFT Global Facility and guided by the World Bank's VA/VASP Risk Assessment Methodology.

Senator the Honourable John Jeremie SC
Attorney General
Office of the Attorney General
February 2026

EXECUTIVE SUMMARY

Virtual assets (VAs) have become increasingly mainstream as an innovative option for trade financing, cross border payments and settlement. The pseudonymous, decentralised nature of VAs which facilitate near instantaneous transmittal of value, also make VAs an attractive vehicle for criminal activities and laundering of illicit proceeds. Since October 2018, the Financial Action Task Force (FATF), the international standard setter for anti-money laundering and counter-financing of terrorism and proliferation (AML/CFT/CPF), updated its Standards[1] to include the regulation and supervision of VAs and virtual asset service providers (VASPs). The FATF expects *inter alia,* countries to *"identify and assess the money laundering, terrorist financing and proliferation financing risks emerging from virtual asset activities and the activities or operations of VASPs."*

Accordingly, this is Trinidad and Tobago's first risk assessment of VAs and VASPs. The assessment was conducted in 2025, with a review period of January 2021 to December 2025. The risk assessment was conducted by a working group comprising of both public and private sector stakeholders using the World Bank's Methodology and VA Risk Assessment Tool. Technical assistance was provided by the European Union AML/CFT Global Facility. This assessment is based on the premise that risk is a function of threats, vulnerabilities and mitigating controls.

Notably, at the commencement of the risk assessment process in January 2025, the assessment was being undertaken as part of a phased approach in preparation for the Caribbean Financial Action Task Force (CFATF) 5th Round Mutual Evaluation (MEV) of Trinidad and Tobago. The MEV formally commenced in March 2025 and will culminate with an on-site assessment in March 2026. As such, priority was placed on completing the risk assessment and concurrently, preparing draft legislation which sought to impose a time-bound prohibition on VASP activities, to allow the authorities sufficient time to develop an appropriate regulatory framework, guided by the outcomes of the risk assessment. The legislation was laid in Parliament in September 2025 prompting tremendous feedback and engagement from stakeholders including the VASP sector, which provided valuable insights that were absent during the risk assessment.

The Virtual Assets and Virtual Assets Services Providers Act 12 of 2025 (VA/VASP Act 2025) came into effect on December 23, 2025, establishing a time-bound prohibition on the conduct of specified VASP activities as a business, in and from within Trinidad and Tobago up until December 31, 2026. The prohibition takes effect within three (3) months of the commencement of the Act. The prohibition does not prevent private citizens from conducting personal VA transactions.

The Trinidad and Tobago Securities and Exchange Commission (TTSEC) is the regulatory authority for the sector, with the necessary monitoring and enforcement powers to ensure compliance with the prohibition. Notwithstanding the temporary prohibition, the VA/VASP Act 2025 also provides for a Regulatory Sandbox which seeks to preserve VASP businesses in existence at the time the legislation came into effect. The Sandbox will be administered by the

[1] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

TTSEC, within which VASPs authorised by the TTSEC will be able to continue to operate, under closely monitored parameters including AML/CFT/CPF controls during the one-year moratorium period.

The findings of this risk assessment and learnings from the observed activity in the Regulatory Sandbox will provide the foundation for the development of a comprehensive risk based regulatory framework for VAs and VASPs.

Due to the timing of the passage of the VA/VASP Act and the publication of this report, this assessment considers the VASP landscape and the associated threats, vulnerabilities and risks as at the conclusion of the assessment in September 2025. Therefore, a full view of the implementation of the VA/VASP Act 2025, the effectiveness of the prohibition and operations of the regulatory sandbox, and a subsequent residual risk estimation, is premature and out of scope for this report.

KEY FINDINGS

The assessment identified a growing domestic VA/VASP ecosystem promoting *inter alia* alternative investment and payment options and commercial activity. VAs and VASPs services are being promoted as an alternative to making/receiving cross-border payments.In parallel, there has been a proliferation of fraudulent investment schemes and scams seeking to exploit the vulnerable in the society. In the absence of a regulatory framework, there is a high likelihood that VAs can be misused to launder illicit funds or procure illicit products and services.

SUMMARY OF ASSESSMENT RATINGS

The following is a summary of the assessment ratings, reflecting the status quo before and after the passage of the VA/VASP Act 2025, adopting a conservative assessment of the impact given the nascent and unimplemented regulatory environment.

RISK ASSESSMENT SUMMARY	AS AT SEPTEMBER 2025	AS AT DECEMBER 2025
Overall ML/TF Threat Exposure	**High**	**High**
Overall ML/TF Vulnerability of Products & Services / Types of VA	**Very High**	**Very High**
ML/TF Risk Level ***before*** Mitigating Measures	**High**	**High**
Quality of ML/TF Mitigating Measures	**Low Mitigation**	**Medium Low Mitigation**
ML/TF Risk Level ***after*** Mitigating Measures	**High**	**Medium High**

The assessment identified four (4) VASPs offering the following services:

TYPE OF VASP	DESCRIPTION OF SERVICES
Virtual Assets Exchanges	1. Purchase and sale of stablecoins (USDC and USDT); the VASP also provides remittance services and is a Financial Technology company. 2. Purchase of USDT and on-ramp access to Binance and other major crypto exchanges. 3. Purchase VAs, Non Fungible Tokens (NFTs) and VA-related investment opportunities.
Virtual Asset Payment Processing	4. ATM and remittance services where customers can purchase Bitcoin via cash-in at the ATM (fiat-to-virtual), receive funds from local or foreign senders via cash-out at the ATM (virtual-to-fiat). Transactions are strictly in Bitcoin via Lightning-enabled wallets.

Market surveillance also suggested the existence VASPs offering Fund Management/ Fund Distribution activities, conversion services and the distribution of VA cards.

The primary VAs used domestically are: Bitcoin, Ethereum, Tether (USDT), Stablecoin (USDC) and NFTs. A high incidence of mining was also detected potentially due to the low rates for electricity use. Anecdotal information suggests that the activity is individual mining for personal use.

Traditional financial institutions demonstrate a low risk appetite to interact with VASPs or to offer VA products and services. There is evidence that bank cards have been utilized to purchase VAs but the value/volume is limited by the transaction thresholds placed by the banks.

The volume and value of Suspicious Transaction Reports (STRs) reported on VA-related activity have increased over the scope period, however the reported activity is predominantly comprised of personal bank-card related transactions which are investment related and do not meet the threshold of suspicion for ML or TF.

RECOMMENDATIONS

Given the sector's exposure to ML/TF threats, the inherent vulnerabilities in the VAs and VASPs, and limitations in mitigating measures that could be exploited by illicit actors, the following are the key recommendations:

a. Full Implementation of the VA/VASP Act 2025

At the time of the publication of this report, the Act is in effect and the TTSEC was considering applications received from existing market actors for entry into the Regulatory Sandbox. Measures have also been implemented to monitor for unauthorised VASP activity during the prohibition period.

b. Capacity Building Programmes for VASPs

Supervisory authorities to establish regulatory requirements and clear guidelines for the Regulatory Sandbox and the AML/CFT/CPF compliance requirements.

c. Capacity & Technical Building for Competent Authorities

Adequate resource allocation and capacity and technical building for regulatory bodies, LEAs and judiciary must be provided to facilitate supervision, monitoring, investigation, asset tracing, seizure, confiscation and recovery.

d. Traditional Financial Institutions and DNFBPs – Risk Assessments

Financial institutions and DNFBPs are to consider the ML/TF/PF risks posed by VAs and VASPs in conducting their enterprise risk assessments.

e. Public Awareness

Educational campaigns to be undertaken aimed at both consumers and businesses to increase public awareness about the risks and responsibilities associated with VAs. This will reduce the incidence of fraud and promote responsible usage of VAs.

f. Development and Implementation of a Comprehensive Regulatory framework

The findings of this risk assessment and learnings from the observed activity in the Regulatory Sandbox will provide the foundation for the development of a comprehensive risk based regulatory framework for VAs and VASPs to be implemented at the end of the prohibition period.

g. Advancement of proposed legislative reform of the National Payment System

While current data suggests that the activity is primarily of a securities nature, the Central Bank will consider including future-proof provisions for the Payments Systems and Services (PSS) Bill to cover payments activities involving VAs or conducted by VASPs, as this activity falls under the Central Bank's regulatory remit.

h. Promote innovation in the digital asset space for economic growth and financial inclusion

The Government of the Republic of Trinidad and Tobago (GoRTT) reaffirms its commitment to digital innovation and citizen-centred services. In respect of moving towards a cashless society and the digitilisation of government payments and services, and to address the evolving Artificial Intelligence (AI) space, the GoRTT will continue to advance key initiatives, including the development of a National Interoperability Framework to ensure systems and agencies operate collaboratively rather than in silos; the launch of Trinidad and Tobago's first National Intelligence Assistant; and the development of a unified citizen services portal to bring all public and legal services into one accessible space. Additionally, the GoRTT, in collaboration with the International Telecommunications Union, has become one of only five countries globally to participate in a landmark AI Governance Assessment, positioning Trinidad and Tobago as a forward-thinking nation in the responsible adoption of AI.

1.0 INTRODUCTION

1.1 BACKGROUND

In recent years, VAs have become increasingly mainstream. The distinct technological features of VAs can foster financial innovation for more efficient trade financing, cross border payments and settlement. These features also make VAs vulnerable to significant ML/TF/PF risk due to its borderless nature and the ease and speed of transferring funds to different countries coupled with the absence of homogeneous controls and prevention measures globally. Illicit actors use VA systems to transfer value or purchase goods anonymously and rapidly.

Globally, several jurisdictions and international bodies have recognised the increasing ML/ TF threat posed by VAs and VASPs. The FATF updated its Standards[2] in October 2018, to clarify the application of the FATF Standards to VA activities and VASPs in order to, among other things, assist jurisdictions in mitigating the ML/TF/PF risks associated with VA activities and in protecting the integrity of the global financial system. In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 (INR. 15) to further clarify how the FATF requirements should apply in relation to VAs and VASPs, including *inter alia*, the application of a risk based approach to VA activities or operations and VASPs.

The FATF also issued Guidance for a Risk-Based Approach on Virtual Assets and Virtual Asset Service Providers in October 2021[3] (FATF VA/VASP Guidance), and in June 2025, published its "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers". The report outlines the status of adherence to the FATF Standards with greater implementation of licensing or registration requirements, and varying approaches adopted including *inter alia* some jurisdictions opting for partial prohibitions.

1.2 GLOBAL VIRTUAL ASSETS LANDSCAPE

The use of VAs, also referred to as cryptocurrencies or digital assets, has grown exponentially since the introduction of Bitcoin in 2009. In 2013, the global VA market was still considered to be in its infancy with a modest 66 VAs in existence[4]. The 2017-2019 years are considered to be the initial boom period fuelled by increased public awareness and growing investor/speculative interest, with an estimated 2,817 VAs in existence by 2019. By 2020, the COVID-19 pandemic, financial uncertainty, and the growing appeal of decentralised finance (DeFi) resulted in significant growth with over 4,000 VAs in existence, and by 2021, to over 7,000 VAs. The unprecedented growth was attributed to the mainstream acceptance of VAs, institutional investments, and the broader adoption of blockchain technology. The subsequent years witnessed a slower growth trend due to *inter alia*, increased regulatory scrutiny and a more mature investor focus on quality over quantity.

[2] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
[3] *Financial Action Task Force (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers". https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html*
[4] CoinJournal, January 5, 2024 The explosive growth of cryptocurrencies over the past decade

As at November 2025, it is estimated that there are over 9,000 active VAs with an approximate market capitalization[5] value of US$ 3 trillion. However, most VAs are not considered significant, with Bitcoin and Ethereum accounting for over 70% of the entire market capitalization[6].

The number of VA users has also grown exponentially with the highest forecast for the global user base of cryptocurrencies projected to reach 900 million[7] by the end of 2025. In 2025[8], the global VA space has a projected revenue of US$ 100.2 billion with the Caribbean accounting for US$ 78.6 million[9] or approximately 0.08% of global VA revenue, and projected to be US$75.4 million in 2026. The number of VA users in the region is estimated at approximately 1.54 million in 2025 and is expected to reach 1.75 million by 2026.[10]

1.3 DOMESTIC LANDSCAPE

According to Chainalysis' crypto adoption index[11], Trinidad and Tobago ranked 137th out of 151 countries and 112th out of 130 countries in 2024 and 2025, respectively. Trinidad and Tobago is estimated to have received US$1.6 billion worth of VAs over the period January 2024 to January 2025. This placed the country 4th in the Latin America region behind the Dominican Republic (US$ 4.4B), Puerto Rico (US$ 4.3B) and Jamaica (US$ 2.3B).

Based on the Chainalysis reports, the majority of on-chain activity was conducted via centralized exchanges[12], ranging from 56.07% in 2022; 88.9% in the 2023; and 93% in 2025, of total activity. Further, 3.8% of the VA activity was attributed to mining in Trinidad and Tobago which exceeds the global average of 0.2%. This could be as a result of the low electricity rates in Trinidad and Tobago when compared to the Caribbean region, as noted in a 2023 article entitled "*The High Cost of Subsidized Electricity*" (Caribbean Investigative Journalism Network, 2023).[13]

The VA industry in Trinidad and Tobago includes, *inter alia,* industry associations and consultancy firms that promote the development of the VA sector e.g. the Fintech Association of Trinidad and Tobago. At the time of the assessment, VAs were not recognized as legal tender in Trinidad and Tobago, and VASPs were not regulated or supervised under existing laws. Following searches with the Companies Registry and the Tax Authority, there are no official record of the number and type of VASPs operating in Trinidad and Tobago. Notwithstanding, information on VASPs operating domestically was gathered through various sources including open source searches and surveys.

[5] The price of the virtual currencies times the number of coins in the market.
[6] CoinMarketCap as at December 3, 2025: https://coinmarketcap.com/charts/
[7] Crypto users worldwide 2016-2025| Statista
[8] *Statista, "Digital Assets – Worldwide." https://www.statista.com/outlook/fmo/digital-assets/worldwide?currency=USD*
[9] *Statista, "Digital Assets – Caribbean." https://www.statista.com/outlook/fmo/digital-assets/caribbean?currency=USD*
[10] *Statista, "Cryptocurrencies – Caribbean." https://www.statista.com/outlook/fmo/digital-assets/cryptocurrencies/caribbean#revenue*
[11] *Chainalysis: "The 2024 Geography of Crypto Report". https://www.chainalysis.com/wp-content/uploads/2024/10/the-2024-geography-of-crypto-report-release.pdf and "The 2025 Geography of Crypto Report: https://go.chainalysis.com/2025-geography-of-cryptocurrency-report.html*
[12] In the Chainalysis 2025 report, mining accounts for 3.8%; DeFi accounts for 2.6% and 'Other' accounts for 0.1% of total VA activity.
[13] *Caribbean Investigative Journalism Network (2023), "The High Cost of Subsidized Electricity". https://www.cijn.org/high-cost-of-subsidised-electricity/*

1.4 LEGAL FRAMEWORK

Trinidad and Tobago's legislative landscape surrounding technology and financial innovation is evolving. At the time of the assessment the existing legal framework did not address VA/VASP activity. However, through the passage of the VA/VASP Act 2025 in December 2025, Trinidad and Tobago adopted the FATF definitions of VAs and VASPs:

> '*Virtual asset*' means a digital representation of value which may be digitally traded, transferred or used for payment or investment purposes, but does not include the digital representation of fiat currencies, securities or other financial assets that are covered under any other written law.
>
> A '*Virtual Asset Service Provider*' means a person who conducts one or more of the following activities as a business, for or on behalf of another person:
> a) the exchange between virtual assets and fiat currencies;
> b) the exchange between one or more forms of virtual assets;
> c) the transfer of virtual assets;
> d) the safekeeping or administration of virtual assets or instruments enabling control over virtual assets;
> e) the participation in and provision of financial services related to an offer of an issuer or sale of a virtual asset**;** and
> f) such other activity as may be prescribed.

The VA/VASP Act 2025 introduced a 1-year prohibition of the conduct of the above listed VASP activities as a business, in and from within Trinidad and Tobago. The Act grants the TTSEC the regulatory remit to monitor VA activity and emerging risks with the necessary enforcement powers to ensure that the prohibition is effectively imposed. Notwithstanding the temporary prohibition, the Act seeks to preserve existing VASP businesses/activities listed above, with the exception of VASPs providing safekeeping or administration of VAs or instruments enabling control over VAs (category (d)), through the provision of a Regulatory Sandbox, administered by the TTSEC, within which VASPs authorised by the TTSEC will be able to continue to operate during the prohibition period, under closely monitored parameters including AML/CFT/CPF controls. The VA/VASP Act empowers the TTSEC to ensure that VASPs within the Regulatory Sandbox effectively implement these obligations and to take proportionate action where breaches are identified.

Through consequential amendments made to the existing AML/CFT/CPF legislative regime, VASPs will be subject to the same AML/CFT/CPF obligations as traditional financial institutions, with enhancements made to the law to accommodate nuances in VA transactions, such as the travel rule. Notably, the Proceeds of Crime Act, Chap. 11:27 (POCA) was amended to include a definition of a VA allowing it to be considered as "property or funds" for the purpose of the POCA. This amendment came into force on August 15, 2025 and provides a legal basis for seizure/freezing/confiscation of VAs.

During the prohibition period, the findings of this risk assessment and learnings from the observed activity in the Regulatory Sandbox will provide the foundation for the development of a comprehensive risk based regulatory framework for VAs and VASPs by late 2026.

2.0 CHRONOLOGY OF ACTIONS UNDERTAKEN TO DATE

Trinidad and Tobago remains steadfast in its commitment to the global fight against ML, TF and PF. This commitment is demonstrated through the development and maintenance of a robust AML/CFT/CPF framework. Pending the implementation of a regulatory framework for VAs and VASPs, the authorities took the following steps in response to the emerging risks:

1. In 2019, the Central Bank of Trinidad and Tobago (Central Bank/ CBTT), the Trinidad and Tobago Securities Exchange Commission (TTSEC) and the Financial Intelligence Unit of Trinidad and Tobago (FIUTT) issued a Joint Public Advisory[14] cautioning the public of the potential risks associated with VAs and of schemes promising high returns[15]. The advisory highlighted concerns such as anonymity, fraud, and the potential for misuse in money laundering and terrorist financing schemes.

2. In August 2020, CBTT, FIUTT, and TTSEC issued a joint advisory cautioning the public on Pyramid or Ponzi Type schemes[16].

3. In November 2022, the TTSEC published notification on its website advising of the prohibition of Ponzi Type schemes[17].

4. In addition to the SWG of the NAMLC, the Central Bank, FIUTT and TTSEC established a Joint Fintech Steering Committee (JFSC) in March 2022 to ensure effective collaboration among the domestic Supervisory Authorities on Fintech related matters.

5. In September 2023, there was a public private engagement on crypto asset regulation in Trinidad and Tobago. The Central Bank and the TTSEC hosted a high-level panel discussion on "*Considerations in Crypto Asset Regulation"*[18]. The objectives of this discussion were to advance public education and gather perspectives on an appropriate domestic regulatory framework for crypto assets. The Governor of the Central Bank made a case for urgent legislative/regulatory reforms since, crypto asset activities have:
    a) internationally grown in usage over the last decade with heightened significant risk;
    b) grown in interest and involvement in Trinidad and Tobago; and
    c) created legal and regulatory uncertainty which may be limiting the development of business models connected to crypto assets (*According to the 2023 International Monetary Fund (IMF) Report from the Technical Assistance on Fintech Regulation and Legislation).*

    Further, the Deputy Chief Executive Officer (DCEO) of the TTSEC, outlined the reforms needed to allow for investor protection where crypto assets were considered as securities. The DCEO indicated that regulators should:

[14] *https://fiu.gov.tt/wp-content/uploads/Joint-Public-Statement-on-Virtual-Currency-by-Regulatory-Authorities.pdf*
[15] https://www.central-bank.org.tt/cbtt_storage/pdf/Joint_Public_Statement_Virtual_Currency_Jan_2019.pdf
[16] https://www.ttsec.org.tt/joint-media-release-financial-sector-regulators-on-pyramid-schemes/
[17] https://www.ttsec.org.tt/ponzi-type-schemes-now-prohibited/
[18] Video of the Webinar.
Governor Dr. Alvin Hilaire's (CBTT) Power Point presentation.
Ms. Lystra Lucillio's (TTSEC) Power Point presentation.
Mr. Mark Pereira's Power Point presentation.

a) understand the ML/TF risks the sector faces [Crypto Assets];
b) license or register VASPs;
c) supervise the sector, in the same way it supervises other financial institutions; and
d) implement the Travel Rule.

The private sector representative, a local Fintech company, emphasised the importance of a regulatory environment that was supportive of innovation in Fintech in order to assure Trinidad and Tobago's competitiveness in the global ecosystem. He posited that the impact of the lack of regulation of crypto assets in Trinidad and Tobago included but was not limited to, the loss of talent and loss of foreign exchange and taxes.

6. Subsequently, on September 07, 2023, the IMF published its report from the Technical Assistance on Fintech Regulation and Legislation, which was held at the Central Bank in April 2023 ("IMF Report")[19]. This IMF Report noted several options for the design of a strategy to support the development of crypto asset activities under a proper regulatory environment and include the following:
    a) comprehensive legal reform;
    b) targeted legal amendments followed by regulation;
    c) regulations issued without legal changes; or
    d) the use of exemptions.

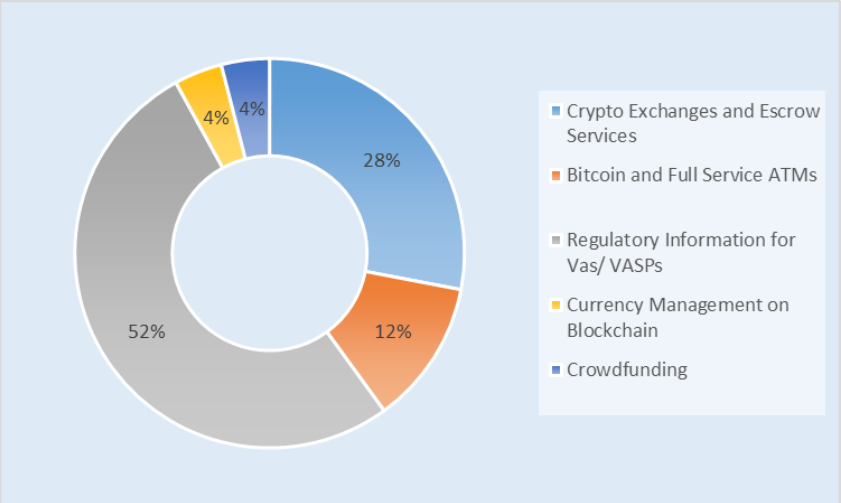
7. In November 2024, the JFSC produced a policy proposal document (PPD) for the treatment of VAs/VASPs and their related activities in Trinidad and Tobago. The PPD proposed the following:
    a) **Mandatory (short term or immediate)**
    - Conduct a NRA to determine the scope of the activities, players and accompanying risks posed by VAs and VASPs in Trinidad and Tobago. This NRA may be further supplemented by an impact assessment to measure the cost and benefits of regulating VAs and VASPs, as recommended by the IMF.
    - Upon the results of the NRA on VAs and VASPs and any other risk assessment conducted, the next phase may focus on targeted legal amendments to the existing AML legislation to comply with and adhere to the requirements of FATF Recommendation 15. These legislation include but are not limited to the POCA and the Financial Obligations Regulation 2010 as amended (FORs).

    b) **Long Term**
    - Post 2026 and following a consultative process on a clearly articulated policy approach, develop bespoke legislation with a regulatory regime that comprehensively deals with all prudential requirements and address risk mitigation measures including consumer protection, AML/CFT/CPF, technology, cyber security and safeguarding of customer funds.

[19] According to the IMF, this report reflects the main findings and recommendations from the April 2023 mission to Port of Spain. This report focuses narrowly on the request of authorities in relation to the licensing and supervision of e-money by CBTT, the operation of the Innovation Hub and Regulatory Sandbox at both authorities, and a review of existing securities legislation by TTSEC.

8. The regulators continued to utilise existing regulatory and supervisory tools such as the Joint Regulatory Innovation Hub (Innovation Hub) to facilitate the efforts of the Supervisory Authorities in treating with VAs, VASPs and their related activities (see Figure 1).

Figure 1: Expressions of Interest received via the Innovation Hub



9. In September 2025, following completion of the VA/VASP risk assessment, a VA/VASP Bill was laid in Parliament introducing a time bound (two (2) year) prohibition on the VASP activities, following the experience of Guyana and Belize, given limited technical capacity and resources to implement Recommendation 15. The prohibition did not prevent private citizens from conducting personal VA transactions. The Bill, *inter alia,* established the TTSEC as supervisory authority to monitor and enforce the prohibition. The moratorium established by the prohibition would allow the country sufficient time to establish an appropriate framework based on the findings of the risk assessment.

10. Subsequently in October 2025, following stakeholder feedback and consultations among the private sector and the Attorney General, the Ministry of Finance, the TTSEC, the Central Bank, and the FIUTT, the authorities agreed to revise the prohibition regime by introducing a Regulatory Sandbox framework to allow limited, supervised activity in the VA sector while comprehensive regulation is developed. In November 2025, the VA/VASP Bill was amended which sought to *inter alia:*
    a) Reduce the prohibition period on VA business activities from two (2) years to one (1) year, ending December 31, 2026.
    b) Grant the TTSEC the power to establish a VASP Regulatory Sandbox to allow existing entities to operate, subject to specific regulatory requirements, under TTSEC supervision and enforcement during the prohibition period.

3.0 OBJECTIVE OF THE RISK ASSESSMENT

This VA/VASP risk assessment covers the scope period 2021 to 2025 and seeks to satisfy criterion 15.3(a) of the FATF Recommendation 15, which requires countries to *"identify and assess the money laundering, terrorist financing and proliferation financing risks emerging from virtual asset activities and the activities or operations of VASPs."*

4.0 METHODOLOGY

The risk assessment of VAs and VASPs was coordinated through the National AML/CFT/CPF Committee (NAMLC) and conducted by the Supervisory Working Group (SWG) of NAMLC. The SWG is comprised of the three (3) AML/CFT/CFT supervisory authorities, those being the Central Bank, TTSEC and FIUTT.

The risk assessment working group comprised of the SWG and other relevant public and private sector stakeholders including, *inter alia*, the Ministry of Finance (MOF), the Trinidad and Tobago Police Service (TTPS), traditional reporting entities, technology firms and consultants, the Fintech Association of Trinidad and Tobago and the Trinidad and Tobago International Financial Centre (TTIFC). The World Bank's (WB) VA/VASP's 2022 methodology and risk assessment tool were utilized to conduct the risk assessment. The assessment process was supported with technical assistance from the European Union AML/CFT Global Facility.

Data was collected from open-source intelligence, and from survey responses received from the public, reporting entities, regulators, law enforcement agencies, and VASPs. Notably, there was a low survey response rate from VA users, and no responses were received from the sector itself, until after completion of the first draft risk assessment report in September 2025. Where possible, these challenges were mitigated through the use of qualitative analysis with reliance placed on, *inter alia*, information derived from market surveillance on locally operating VA users and VASPs, open-source information primarily from academic articles and research, guidance and reports from international agencies such as the FATF, typology reports from blockchain analytics providers like Chainalysis, and reports from other public and private sector agencies.

4.1 THREAT ASSESSMENT

The goal of the threat assessment was to identify the nature of the predicate offences VAs/ VASPs are most exposed to e.g. fraud, tax evasion and ML. The WB tool uses various threats from a domestic and international perspective. These pose inherent ML/TF risks, as applicable to the profile of VASPs operating in the country, before any controls or mitigation measures are put in place. The threat assessment considered the findings of the 3rd NRA, including feedback on the STR data from the FIUTT, criminal matters from the Financial Investigations Branch (FIB) of the TTPS and regional and global typologies.

4.2 VULNERABILITY ASSESSMENT

The inherent vulnerability assessment considered the nature of the VASP and the nature of the products/services that could be exploited by criminals, as well as traditional reporting entities' interaction with VASPs.

4.3 MITIGATING MEASURES

Mitigating measures pertain to AML/CFT measures and controls that exist at a national level and are implemented by both VASPs and traditional reporting entities, and where these exist, the effectiveness of such measures. While limited information was obtained on mitigating measures employed by VASPs, there was an adequate response rate from the traditional reporting entities.

4.4 OVERALL ML/TF RISK EXPOSURE

Risk was quantified using the WB's VA/VASP risk assessment module tool. It measured the threats and the inherent vulnerabilities of each selected VASP category against mitigating measures and generated residual risk scores.

5.0 THREAT ASSESSMENT

ML/TF/PF threats stem from predicate offences and the illicit actors that perpetrate them. This report examines the threats most relevant to the domestic VASP sector based on the nature and type of VA/VASP activity, considering the overall threat level of predicate offences identified in the 3rd NRA, the prevalent threats highlighted by the FATF in its 2025 '*Targeted Update on Implementation of the FATF Standards on VAs and VASPs' (FATF 2025 Update)*, and the typologies identified by Chainalysis and domestic and regional agencies.

The FATF 2025 Update has indicated that illicit actors have, *inter alia*:

- breached VASPs cybersecurity measures albeit at a decreasing rate, for large scale VA thefts, with the largest single theft of VAs by the Democratic People's Republic Korea (DPRK);
- used unregistered VASPs to facilitate money laundering;
- utilised international laundering networks across jurisdictions to swap VAs for cash or to purchase illicit products without moving physical money across borders; and
- increasingly used existing and new types of VA fraud and scams, and the growth of 'scam-as-a-service' activity in the VA ecosystem.

FATF's 2025 Update highlighted the continued prevalence of investment and romance scams and particularly, 'pig butchering'. Ransomware attacks have continued with hundreds of millions in illicit revenue but multilateral law enforcement disruption and a decreased appetite to pay amongst victims, have resulted in lower revenues compared to previous years. FATF also noted that there continues to be a link between VAs and gambling. Artificial intelligence

(AI) tools are also being used to perpetuate scams. Chainalysis' 2025 Crypto Crime report[20] also highlighted the increasing use of AI in the fraud and scams space, consistent with an emerging trend of services using AI to bypass know-your-customer (KYC) requirements.

Additionally, FATF flagged the increased use of stablecoins by illicit actors including the DPRK, terrorist financiers and drug traffickers, with estimates suggesting that the majority of on-chain illicit activity is being transacted in stablecoins. Sanctioned entities, including individuals operating in sanctioned jurisdictions, are turning more to stablecoins due to challenges with accessing the U.S. dollar through traditional means.

The FATF also noted that terrorist groups continue to utilise VAs, particularly to raise and move funds, but the exact scale is difficult to measure. Identifying individuals or entities exercising control or influence over DeFi arrangements also continues to be challenging.

Chainalysis reported in its 2025 Crypto Crime report "*a steady diversification away from BTC, with stablecoins now occupying the majority of all illicit transaction volume (63% of all illicit transactions)*". This aligns with the upward trend in global stablecoin adoption which represents a sizable percentage of all crypto activity, with year-on-year growth of 77% in stablecoin activity to total crypto activity which could accelerate illicit finance risks, given the uneven implementation of the FATF Standards globally.

Notably, in its 2025 Crypto Crime report, Chainalysis highlighted that stablecoin issuers often freeze funds once they become aware of illicit use, which can make stablecoins a poor tool for the transfer of value by illicit actors. Tether was given as an example of taking action to freeze addresses of concern linked to scams, terrorist financing, and sanctions evasion. Some forms of crypto crime, such as ransomware and darknet market sales of illicit goods, remain BTC-dominated.

The Chainalysis reports on VA activity in Trinidad and Tobago for the period 2022 to 2025 highlight scams, transactions along the blockchain from sanctioned entities, interactions with darknet marketplaces and gambling as main forms of illicit activity in the country.

The inherent global/borderless nature of VAs and VASPs pose a threat which can be exploited by criminals to conduct illicit activities as VA systems can be accessed via the internet (including via mobile phones) for cross-border payments and funds transfers. Transactions can involve several entities, often spread across several countries, to transfer funds or execute payments with customer and transaction records held by different entities across different jurisdictions. This poses challenges for AML/CFT/CPF compliance and supervision/enforcement, and to law enforcement efforts, which are relevant in the Trinidad and Tobago context.

In this regard, the amendment made to the POCA[21] to include a definition of a virtual asset and to provide that a virtual asset should be considered "property or funds" provides a legal basis for seizure/freezing/confiscation of VAs.

[20] Chainalysis: The 2025 Crypto Crime Report
[21] Amendment made via the Miscellaneous Provisions (FATF Compliance) Act 2024

5.1 KEY PREDICATE OFFENCES INVOLVING VAS AND VASPS

5.1.1 DRUG, HUMAN AND ARMS TRAFFICKING, AND THE DARKNET

The 3rd NRA highlighted fraud, corruption, drug trafficking, illicit arms trafficking, human trafficking, and related offences as "High" risk predicate offences. These traditional predicate offences have evolved in tandem with technological advancements. A 2023 article by The Commonwealth entitled "Funding Crime Online: Cybercrime and its Links to Organised Crime in the Caribbean" highlights the nexus between traditional organized crime groups and the dark web (Brain, 2023).[22] Further, a 2022 paper on the '*Dynamics of Dark Web Financial Marketplaces*' by the Center for Cybercrime Investigation and Cybersecurity highlights VAs as the preferred payment medium on the darknet due to the pseudo-anonymous nature of VAs (Jung, 2022)[23].

In Trinidad and Tobago, access to darknet marketplaces accounted for a small but increasing portion of the observed illicit activity across in the Chainalysis reports (0.3% in the 2022 report, 1.8% in the 2023 report and 6.7% in the 2025 report). Further, no drug trafficking, illicit arms trafficking or human trafficking cases involving the use of VAs were identified and/or investigated for the period under review. However, the Chainlaysis 2025 Crypto Crime Report emphasized that its values *"…exclude revenue from non-crypto-native crime, such as traditional drug trafficking…"* as *"…Such transactions are virtually indistinguishable from licit transactions in on-chain data…"* (Chainalysis, 2025, p. 3).[24] As such, it is likely that the true extent to which VAs are misused for organized crime is unknown, both locally and internationally.

5.1.2 SCAMS AND FRAUDULENT ACTIVITY

Fraud was identified as a "High" risk predicate offence in the 3rd NRA and represents the most common category of suspected criminal conduct in the STRs/SARs received by the FIUTT. It was also the most prevalent predicate offence identified in the Intelligence Reports received for investigation by the FIB from the FIUTT. In this review period, the FIUTT has identified several types of fraud and other typologies[25], including *inter alia*, identity fraud, fraudulent loan documents, romance and investment scams and email phishing. Also, according to the FATF 2025 update, *"…Participants at the April VACG…noted the significant increase in the use of VAs in fraud and scams. One industry participant estimated that there was approximately $51 billion in illicit on-chain activity relating to fraud and scams in 2024..."* (Financial Action Task Force, 2025, p. 20).

Notably, scams have featured prominently in all Chainalysis reports on on-chain activity in Trinidad and Tobago. In the 2022 Chainalysis report, scams accounted for 49.33% of illicit activity. Both of the latter Chainalysis reports highlighted that multiple scams had significant web traffic in Trinidad and Tobago; 92.6% of illicit activity observed was attributed to scams in

[22] *Commonwealth (2023),"Funding Crime Online: Cybercrime and its Links to Organised Crime in the Caribbean". https://thecommonwealth.org/publications/commonwealth-cybercrime-journal-volume-1/funding-crime-online-cybercrime-and-its-links-organised-crime-caribbean*

[23] *The Center for Cybercrime Investigation & Cybersecurity (2022), "Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business". https://vc.bridgew.edu/ijcic/vol5/iss2/2/*

[24] *Chainalysis (2025), "The Chainalysis 2025 Crypto Crime Report". https://go.chainalysis.com/2025-Crypto-Crime-Report.html*

[25] https://fiu.gov.tt/about-us/publications/analysis-products/

the 2023 report while a much lower percent (16%) was linked to scams in the 2025 report. The scams referenced by these reports were all perpetrated by foreign entities, some of which have had regulatory warnings issued against them as highlighted below.

Victims involved in a pyramid scheme, which marketed lucrative returns from trading Forex underpinned by VAs

This case involves a VASP (Company A) perpetuating foreign currency trades underpinned by bitcoin ("BTC"). This company marketed itself as a multi-level marketing ("MLM") company where persons paid to have access to a trading program provided by the company. The trade contracts were funded by BTC and facilitated via VA wallets/exchanges. The trades were carried out by Company A's partner brokers, which were all authorized and regulated by the relevant regulatory authorities in the countries in which they were licensed.

Amidst the lucrative returns touted by the company and its promoters, allegations/claims were made concerning the credibility of the company's founders and promoters, and the involvement of these persons with previous alleged scams. Further, one (1) regulatory advisory was issued against the company warning persons that the entity was not regulated. The scam proliferated within close knit groups, notably churches and community groups, where persons recruited close friends to join their network and invest monies. Several of these persons invested significant sums of monies without having a proper understanding of foreign currency trading and/or cryptocurrency, and the increased risks.

By 2023, persons began experiencing difficulty to cash out. As at the time of the report, there is no evidence that any of the investors were able to cash out funds or recoup their initial investments.

This assessment also highlighted instances where scams have been perpetrated by local entities/ persons.

Victims potentially scammed by a local entity purporting to be VASP

This case involves a company purporting to be a VASP (Company B) carrying out VA trading services. Company B either sent trade signals to customers to initiate trades or purportedly traded on behalf of customers. According to a report into the company by an investigative journalist, approximately 3,000 investors have not been able to receive payouts following the investments they made into the fund.

Notably, Company B's footprint increased in 2023 with lucrative claims by the company's director to provide significant returns on persons' investments. Since then, thousands of persons made investments. Notably, one (1) person invested TT$14 million (US$ 2.06 million) with the company.

Initially, persons were able to withdraw monies shortly after investing. For instance, one (1) person, noted to have deposited TT$ 4,000 (US$ 588) in early 2024, was able to withdraw TT$ 16,000 (US$ 2,353) by mid-2024 and so invested an additional TT$ 90,000 (US$ 13,235) between September and October 2024. However, in 2025, investors started to experience difficulties when requesting payouts/ withdrawals.

In August 2025 the TTSEC announced that it had initiated a probe into the company. At the time of the report, the matter was ongoing.

The foregoing cases correlate with FIUTT's Advisory to the Public on Online Investment Scams (ADV/002/2024) where the FIUTT highlighted the rise in suspected online investment scams with a recurrent theme being *"…purporting to receive a high return from their investment portfolio…"*. References to VAs featured heavily in the Advisory. Scammers were noted to *"…take advantage of the evolving world of crypto assets to offer fraudulent investment opportunities …"; and "…ask Victims to deposit money into their (or third parties) accounts for online trading in virtual asset…"* (Financial Intelligence Unit of Trinidad and Tobago, 2024, p. 2)[26]. Victims of VA scams have limited opportunities for recourse given the absence of regulatory framework and consumer protection mechanisms for VA activity in the country.

For the period under review, there was one (1) case concerning a scam purporting investments in VAs that was being investigated by the FIB (see below). There remains significant appetite for VAs due to the country's foreign exchange shortages and persons' inclination to 'get rich quick' schemes. Consequently, scammers taking advantage of the local demand for VAs will continue to pose a significant ML/TF threat domestically.

Local VA Case

In 2023, the FIB commenced investigations concerning investment fraud/Ponzi Scheme type activity. A Trinidad and Tobago national made use of cash, bank deposits and inter-bank transfers when carrying out the scheme. The value of the proceeds attributed to the activity was TT$ 602,384 (US $88,586). The matter was still ongoing as at the time of the report.

5.1.3 CORRUPTION

Corruption has been a prevalent predicate offence assessed as 'high' in the country's NRAs. Notably, a 2023 paper from the Transparency International and the Anti-Corruption Resource centre[27] indicated that *"…A study by the IMF using cross-country regression analysis indicates that more virtual asset use is empirically associated with higher levels of perceived corruption…".* The paper also indicated that *"There are numerous ways in which bribes can be channelled to public officials, including cash payments, inflated commissions, and expensive travel arrangements (UNODC 2022). With the advent of cryptocurrencies, a new avenue has been opened for corrupt transactions…"* (S, 2023, p. 6 and 7)

Consequently, while there have been no documented corruption/bribery cases involving VAs/ VASPs in Trinidad and Tobago, the risk for abuse is present due the pseudo-anonymous and borderless nature of VAs/ VASPs.

[26] *Financial Intelligence Unit of Trinidad and Tobago (2024), "Advisory to the Public on Online Investment Scams (ADV/002/2024)". https://fiu.gov.tt/about-us/publications/analysis-products/advisories/*

[27] *Transparency International and the Anti-Corruption Resource Centre (2023), "Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption". https://knowledgehub.transparency.org/helpdesk/cryptocurrencies-corruption-and-organised-crime-implications-of-the-growing-use-of-cryptocurrencies-in-enabling-illicit-finance-and-corruption*

5.1.4 TAX EVASION

Tax evasion was identified as a medium-risk predicate offence in the 3rd NRA. An August 2025 Working Paper entitled "Taxation of Crypto Assets in Latin American and Caribbean Countries" published by the Inter-American Center of Tax Administrators[28] stated that *"...The taxation of crypto-assets faces multiple difficulties and challenges due to their unique nature and technological characteristics. One of the main issues is the quasi-anonymity offered by many cryptocurrencies, which prevents clear identification of the individuals or legal entities involved in transactions. This lack of identification represents a significant obstacle to third-party reporting and tax enforcement..."* (Jimenez, 2025, p. 11).

Based on theoretical calculations in the report, total tax liability for the Latin American region for the period July 2023 to June 2024 amounted to US$ 4.15 billion or 0.06% of the region's GDP. As such, while there were no tax evasion cases involving VAs/VASPs for the period under review, VAs/VASPs remains a viable avenue for tax evasion in the country due to their inherent pseudonymity and borderless nature.

5.1.5 GAMBLING

According to a January 2024 Report by the United Nations Office on Drugs and Crime (UNODC) on Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia ("the UNODC report")[29], *"...Online gambling platforms, and especially those that are operating illegally, have emerged as among the most popular vehicles for virtual asset-based money launderers, particularly for those using Tether or USDT on the TRON blockchain..."* (United Nations Office on Drugs and Crime, 2024, p. 6).

Though specific to East and Southeast Asia, observed parallels between Eastern Asia and Latin America and the Caribbean warrant the consideration of the identified issues. Notably, as identified in the World Bank's Global Findex 2025 report, financial exclusion is higher in both regions (this indirectly drives crypto adoption). Also, there is comparable projected growth of the online gambling market (World Bank, 2025)[30]. Notably, gambling was assessed as medium-risk in the 3rd NRA. In this regard, the 2022 and 2023 Chainalysis reports highlighted the popularity of VA gambling sites in Trinidad and Tobago. The interconnectedness of online gambling and VA, and the popularity for online gambling with VAs in Trinidad and Tobago, presents additional avenues for illicit actors to launder their illegitimate gains.

5.1.6 CYBERCRIME

Domestically, cyber risk, which was an emerging risk during the COVID-19 pandemic, has increased significantly in tandem with the rapid digitalisation of financial services and government payments. Key risks include increased exposure to cybercrime, growing reliance

[28] *Inter-American Center of Tax Administrators (2025), "Taxation of Crypto Assets in Latin American and Caribbean Countries". https://www.ciat.org/wp-07-2025-taxation-of-crypto-assets-in-latin-american-and-caribbean-countries-english-soon/?lang=en*
[29] *United Nations Office on Drugs and Crime (2024), "Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia". https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html*
[30] *World Bank (2025), "The Global Findex 2025". https://www.worldbank.org/en/publication/globalfindex*

on a small number of third-party digital service providers and heightened threats of disinformation and fraud, through the use of social media and other like platforms.

According to the Cyber Security Incident Response Team (TT-CSIRT)[31], cybersecurity incidents in Trinidad and Tobago have more than doubled from 2023 to 2024[32] driven largely by a surge in phishing and business email compromise attacks. These cyber incidents were disruptive, but none had a systemic impact. This risk is particularly relevant considering the increase in phishing (fraudulent emails), smishing (deceptive SMS messages), and vishing (voice-based scams) incidents used to deceive stakeholders of financial institutions.

In its 2024 Financial Stability Report, the Central Bank considers that the cyber risk facing the financial sector remains **elevated** (Central Bank of Trinidad and Tobago, 2024). Strengthening cyber resilience is a top priority, which requires urgent, coordinated policy measures and close collaboration among regulators, financial institutions, and third-party digital service providers. While the exact number of local ransomware attacks is unknown, there have been more than ten (10) reported attacks targeting Trinidad and Tobago companies for the period under review (see below).

Ransomware attack via RaaS Model

In mid-2025, Company C was subject to a ransomware attack by an entity using the Qilin Ransomeware-as-a-Service (RaaS) model, which is believed to be operating out of Russia. According to a regional cybersecurity expert, Qilin had become more active in the Caribbean in 2025. While Company C was able to regain control of its operations, customers' personal information (e.g., national ID cards and utility bills) had been leaked on the dark web, thus leaving said clients susceptible to potential identity theft, phishing attacks and other cyber-attacks.

In the Chainalysis reports, ransomware attacks did not account for a significant sum of the observed illicit activity - *"…the total volume of ransom payments decreased year-over-year (YoY) by approximately 35%, driven by increased law enforcement actions, improved international collaboration, and a growing refusal by victims to pay…"*.

The Chainalysis 2025 Crime Report noted however that *"…Crypto hacking remains a persistent threat…"* with an estimated US$2.2 billion in value stolen in 2024. While the majority of funds were stolen due to private key compromises (43.8%), the method in which 25.5% of funds were stolen was unknown. The February 2025 DPRK hack of ByBit[33] underscores the significant threat that cybercrime poses to the industry (Rajic, 2025).

[31] The Cyber Security Incident Response Team (TT-CSIRT) operates under the Ministry of Homeland Security (previously known as the Ministry of National Security). In November 2015, the Government of Trinidad and Tobago, with support from the Organization of American States (OAS) and the International Telecommunications Union (ITU), established the Cyber Security Incident Response Team (TT-CSIRT). The establishment of the CSIRT aligns with the strategic goals set forth in Trinidad and Tobago's 2012 National Cyber Security Strategy. https://ttcsirt.gov.tt/about-us/

[32] From 52 incidents reported in 2023 to 118 in 2024. Source: TTCSIRT

[33] *Center for Strategic & International Studies. (2025). "The ByBit Heist and the Future of U.S. Crypto Regulation". https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation*

ByBit Crypto Hack

ByBit faced a significant cyber breach in February 2025 by the Lazarus Group. The hackers exploited a free storage software solution used by ByBit to move Ethereum to its cold storage solution. The exploit of this software coupled likely with phishing attacks, enabled the heist. When the CEO attempted to authorize a transaction for a recipient, the hackers intercepted the request, changed the code and rerouted the funds to their wallets. As such, the CEO inadvertently facilitated the hack.

5.1.7 TRANSACTIONS FROM SANCTIONED ENTITIES

The FATF 2025 Update noted that *"Since 2024, the use of stablecoins by illicit actors, including DPRK actors and terrorist financiers, has risen, with most on-chain illicit activity now involving stablecoins."* The report also states that *"… the DPRK continues to be particularly adept at stealing and laundering funds using VAs…"*.

While scams accounted for the majority of illicit activity observed in the Chainalysis 2023 report, transactions linked to blockchain addresses of sanctioned entities were the main form of illicit activity identified in the Chainalysis 2025 report on Trinidad and Tobago, accounting for US$9.17 million (i.e., approximately 50%). Notably, Chainalysis' 2025 Crypto Crime report[34] indicated that globally, "*Sanctioned jurisdictions and entities received $15.8 billion in cryptocurrency in 2024, accounting for about 39% of all illicit crypto transactions*", largely driven by Iran's growing use of cryptocurrency. This is due to Western imposed sanctions restrictions, leading sanctioned jurisdictions to seek out alternative systems to sustain trade and access capital.

Domestically, the 3rd NRA has risk rated TF as medium-low and PF was assessed as low. No significant terrorist financing activity was identified, and intelligence reports indicate that the main potential threats—such as lone actors, radicalised individuals, and foreign terrorist fighters—remain low and well-monitored. Trinidad and Tobago also has well established institutional coordination through agencies such as the NAMLC, the Anti-Terrorism Unit (ATU), the FIB, and the Strategic Services Agency.

[34] Chainalysis: *The 2025 Crypto Crime Report

Local VASP TF Related Case

In 2022 the FIB received an Intelligence Report (Report) (along with further supplemental reports) which involved a US-based cryptocurrency exchange platform having provided information to a country's Financial Intelligence Agency and indicated that the Subject withdrew the BTC equivalent of approximately $160.00 United States Dollars (USD) to an external bitcoin wallet which is associated with a cluster of addresses, which were also financed by a suspected terrorist group. As a result, the Subject was suspected of engaging in terrorist financing. The Report provided an analysis of Bitcoin transactions involving various blockchain addresses. The analysis was conducted using blockchain analysis tools and information was obtained from the cryptocurrency exchange platform. The primary focus of the information provided was to trace the flow of funds through specific Bitcoin addresses, identify their associations and highlight any connections to potentially illicit activities.

The Report also highlighted that there was some indirect connection between the Subject's address and a Bitcoin address associated with the said terrorist group. Most of the received Bitcoins were transferred to two (2) addresses, one of which was also funded by the Subject's address, but was also indirectly associated with the Bitcoin address associated with the said Terrorist Group. This finding suggested that a portion of the Bitcoin associated with the Subject's addresses may have been used to support terrorism-related activities. The Report was classified as high priority and immediately assigned for investigation. Enquiries were conducted which revealed that the Subject was not known to the FIUTT or any other FIUTT database. The Subject had not travelled for the period 2009 to 2024. There was no information, intelligence or evidence from local law enforcement to suggest that the Subject was involved in any terrorist related activities.

An address was obtained for the Subject and he was located and interviewed. Coming out of the investigation it was determined that the Subject had no knowledge of the suspected terrorist group which would have directly financed a wallet to which a portion of his funds may have also been directed. Further, the Subject had no knowledge of the third party wallet which ultimately received the funds he sent. There was no intelligence or evidence obtained by law enforcement to determine that he had knowingly done so. There was therefore no evidence to suggest that the Subject knowingly financed the wallet associated with the suspected terrorist group and terrorism-related activities.

5.2 OVERALL RATING OF THREAT ASSESSMENT VARIABLES

The overall threat exposure was assessed as **High.** See Table 1 below which defines the variables assessed and provides the rationale for the respective ratings.

Table 1: Overall Threat Risk Rating

#	Threat - Product Dimension	Threat Rating
1.	**VA Nature and Profile:** (*The threats posed by the underlying technology of VAs that may increase anonymity, the portability of VAs and its propensity for cross border transfers, the non-face-to-face nature of VAs, its traceability or lack thereof and the speed in which transfers can be undertaken*.) In the absence of a regulatory framework, domestic VASPs are not obligated to implement measures for KYC and the travel rule requirements. As such, the nature and profile of VAs are assessed as **'Very High'** risk due to their anonymity, ease of cross-border transactions, lack of physical interaction, traceability challenges and fast transaction speeds.	Very High
2.	**Accessibility to Criminals:** (*The threats posed by possible criminal involvement in VA mining operations, the ease with which funds can be collected and transferred for/ by illicit actors for illicit purposes, use of the darknet by criminals and the expenditure of illicit funds in new technologies as part of the VA ecosystem.*) Overall, 'Accessibility to Criminals' was assessed as **'High'**. There is a higher than average incidence of VA mining activity. This is due to the country's low rate of electricity, so the likelihood of illicit actors using stolen processing power to mine is low. Anecdotal information point to individual mining for personal use. However, wallets can be abused for ML/TF by illicit actors with mining operations, in the absence of regulatory controls. There is no evidence of funding via VAs or fundraising via crowdfunding. Products/services such as cold wallets, transfer and conversion services, cards and ATMs were identified domestically, and can facilitate cross border transfers to jurisdictions posing high TF risk near instantaneously and with no face-to-face contact. Absent regulatory controls allow for ease of transfer without travel rule requirements.	High
3.	**Source of funding VA** (*The threats posed by the bankcards, cash transfers, valuable in kind goods and other VAs being used as a sources of funding for VAs.*) STRs were based on private purchases made by individuals using domestic credit cards via online trading platforms not domiciled in Trinidad and Tobago - these VA purchases were funded by cash deposits into bank accounts via Automated Banking Machines, third party transfers, online transfers and ACH transfers by order of third parties. These financial services are via traditional reporting entities subject to AML/CFT regulations. The deposited funds were usually transferred to credit cards of third parties for the purpose of purchasing VAs for individuals and potentially layer illegitimate funds. It is noted that USDC and USDT were used domestically. Additionally, based on a July 2025 IMF working paper on Stablecoin flows[35], "*Analyzing 2024 stablecoin transactions totalling $2 trillion...Relative to GDP, they are most significant in Latin*	Medium

[35] IMF Working Paper WP/25/141 entitled *"Decrypting Crypto: How to Estimate International Stablecoin Flows"*, July 2025 - https://www.imf.org/-/media/files/publications/wp/2025/english/wpiea2025141-source-pdf.pdf

#	Threat - Product Dimension	Threat Rating
	America and the Caribbean (7.7%)...". Further, several scams in the Caribbean have been based on stablecoins, particularly USDT. As such, VA wallets can be abused to enable these scams. Overall, 'Source of Funding VA' was assessed to pose a **'Medium'** threat.	
4.	**Operational Features of VA** (*The threats posed by the environments in which VAs exist and VASPs operate in, that is, whether there is regulation or whether the environment is centralized or decentralized.*) The use of VAs are not regulated in Trinidad and Tobago. Chainalysis reports that the majority of VASP activity occurs on centralized exchanges. Unregulated and decentralized environments pose high risks due to vulnerabilities and lack of oversight and enforcement. Overall, the operational features of VA was assessed to pose a '**High'** threat.	High
5.	**Ease of Criminality** (*The threats posed by the ease with which VAs/VASPs can be used to facilitate tax evasion and ML/TF, how difficult it is to these VAs to traced and seized, and how these VAs/VASPs can be used to circumvent exchange control regulations.)* There is no evidence of the use of VA in criminal investigations at this time. However, reference is made to the findings of the 3rd NRA conducted in 2025. The key predicate offences include threats resulting from fraud, trafficking, scams, corruption, gambling and cybercrimes. The national TF risk from the 3rd NRA was found to be 'Medium-Low' and the threat of tax evasion was found to be 'Medium'. In the absence of a regulatory framework for VAs and VASPs, domestic actors are not subject to licensing/registration, exchange control requirements, AML/CFT or tax obligations, including on revenue earned or gains on investment in VAs. Overall, 'Ease of Criminality' was assessed as '**High'**.	High
6.	**Economic Impact** (*The threats posed by VAs/VASPs impact on the country's monetary policy through the informal economy, the integration of VAs/VASPs with the financial services market and the interactions between VASPs and traditional financial institutions, and corporate governance structures of VASPs.*) There is no evidence of widespread adoption of VAs having a material impact on the money supply or on the country's economic results, notwithstanding the limited use observed for the purchase of goods and services, and as an alternative to foreign exchange needs. Public consumption is primarily speculative in nature and is not materially significant at this time, but the potential exists for an underground economy for VAs in the absence of regulation. While the 3rd NRA indicated the existence of an informal economy, cash is the preferred means of payment at this time. Increasing adoption of digital payment options has be observed which warrants monitoring as this may include VAs in the future. Due to the lack of a regulatory framework, including absent corporate governance requirements for VASPs in T&T, there is a low level of accountability for VASPs. Overall the 'Economic Impact' threat was assessed as **'Medium High'**.	Medium High
	OVERALL THREAT RATING	**High**

5.3 THREAT ASSESSMENT OF VASP ACTORS

Traditional reporting entities do not provide VA services or products, and based on the sectors' responses to the risk assessment surveys, have a low risk appetite to doing business with VASPs. As such, the risk ratings outlined in Table 2 pertain to VASPs determined to be operating locally.

Table 2: Threat Risk Ratings per VASP Categories

VASP Category	Type of service	Sub-Type	Threat rating
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	Hot Wallet	High
	Non-Custodial Services	Cold Wallet	Very High
VIRTUAL ASSET EXCHANGES	Transfer Service	P2P	Very High
		P2B	Very High
	Conversion Services	Fiat-to-Virtual	High
		Virtual-to-Fiat	Very High
		Virtual-to-Virtual	High
VIRTUAL ASSET BROKING / PAYMENT PROCESSING	Payment Gateway	ATMs	High
		Cards	Medium High
VIRTUAL ASSET MANAGEMENT PROVIDERS	Fund Management		Medium High
	Fund Distribution		Medium High
INITIAL COIN OFFERING (ICO) PROVIDERS	Fund Raising	Fiat-to-Virtual	Medium High
		Virtual-to-Fiat	Medium High
	Investment	Development of Product & Services	High
VIRTUAL ASSET INVESTMENT PROVIDERS	Emerging Products	Crypto Escrow service	High
		Crypto-custodian Services	Medium-High
VALIDATORS / MINERS/ ADMINISTRATORS	Proof of Work	Fees	Medium High
		New Assets	Medium High

While no *Virtual Asset Wallet Providers* were identified to be operating domestically, users of VAs utilize hot wallets and cold wallets which are readily accessible online. Cold wallets were assessed as posing a **'Very High'** threat due to its high anonymity and lack of traceability. Cold wallets are easily accessed on traditional online marketplaces such as Amazon and possess a high accessibility to criminals.

The threat level posed by *P2P and P2B* type VASPs was rated 'Very High'. Several social media forums and groups were observed where persons routinely connect to buy and sell VAs. However, the extent of activity could not be quantified. Most of these transactions may occur through centralized exchanges, as implied by Chainalysis data. However, some of this activity occurs via decentralized exchanges. Further, several scams and fraudulent activity are

purported through these groups; the threat posed by such scams would only increase in a P2P environment. The virtual-to-fiat conversion services facilitated by VASPs, including the *VA ATM* can be exploited in the absence of regulatory requirements. As such, this service and ATMs were risk rated as **'Very High'** and **'High'** respectively.

Fiat-to-virtual and *virtual-to-virtual* conversion services were risk rated as **'High'**. Notably, the main form for converting fiat-to-virtual is via banking products offered by traditional reporting entities that are subject to AML/CFT obligations. However, there is one known BTC ATM operating domestically which facilitates BTC to fiat / fiat to BTC for users with lightening network enabled wallets.

The assigned threat rating for *hot wallets and Crypto Escrow type services* were **'High'** and and *Crypto-custodian type services* were **'Medium High'**. While statistics on wallets, escrow services and custodian services were not available, the value of VAs estimated to be coming into the country implies the use of these services by VA users within the country.

A **'High'** threat rating was assigned for *ICO activity* related to the Development of Products and Services. The absence of a regulatory framework and supervisory oversight of the sector makes it attractive as an avenue for the integration of criminal funds into products/ services that can be used to further the agendas of these illicit actors. The other ICO activities deemed relevant to the sector (*fiat-to-virtual fund raising and virtual-to-fiat fund raising*) were assigned a **'Medium-High'** threat rating. These activities pertain to the receipt of money for funding and as such, may be less attractive for the integration of illegitimate funds. However, they can be avenues for scams and other fraudulent activities. One (1) high profile ICO was attempted in the country in the past (BarterCoin), but failed to launch due to regulatory intervention.

Attempted ICO in Trinidad and Tobago: Bartercoin

BarterCoin Exchange Ltd and Zip Coin, through Rentier Company Limited, was carded to launch in Trinidad and Tobago in February 2018. Rentier Company Limited partnered with an international team to establish BarterCoin exchange which was head quartered in Trinidad and Tobago. While the company highlighted the advantages of the launch such as job creation locally and regionally, The Ministry of Finance issued a media release on February 23, 2018, cautioning the public on the associated risks, such as; heightened potential for fraud, cross-border distribution risks, information asymmetry and liquidity risks. The notice highlighted that the BaterCoin Exchange was not endorsed by the Ministry of Finance and no approval was obtained from the TTSEC or CBTT.

All other VASP categories (*Cards, Fund Management and Distribution, and Validators/Miners/Administrators*) were assigned a **'Medium-High'** threat rating. *VA Cards* can be easily transferred across the border, have been observed to have high transactional limits and there is evidence that cards were used to withdraw funds from traditional commercial bank ATMs. Further, given the country's low electricity rates and the aforementioned observation that mining activity in Trinidad and Tobago exceeded the regional and global average, it is likely that there is significant local mining activity in the country, however, anecdotal information point to individual mining for personal use.

6.0 INTERACTION BETWEEN VA ACTIVITIES AND TRADITIONAL REPORTING ENTITIES

Surveys were developed by the working group to determine the interaction between VA activities and traditional reporting entities namely; Commercial Banks; Non-Banks, Insurers, Credit Unions and Securities entities. Overall, there are little to no interaction by the sampled traditional obliged entities with VAs and VASPs. In summary:

- Banks reported **minimal interaction** with VAs primarily through the use of banking products to purchase VAs. The banks reported a low risk appetite to doing business with VASPs and do not intend to offer VA services/products. Further, the offering of new or materially changed products and services by any entity regulated by the Central Bank of Trinidad and Tobago (Central Bank) is subject to regulatory requirements and the approval of the Central Bank prior to launch.

- The banks scrutinize Source of Funds Declaration forms, payment messages, behavioural alerts and customer activity to determine any linkages to VAs/VASPs. Notably, STR data provided by the FIUTT revealed that 'crypto' related SARs were based on private purchases made by individuals utilising domestic credit cards via online trading platforms not domiciled in Trinidad and Tobago. The FIUTT's analysis of these STRs determined that predominantly the activity comprised of personal transactions which are investment related and do not meet the threshold of suspicion for ML or TF.

- Insurers, Non-banks, Credit unions and Securities entities reported no interaction with VAs/ VASPs. DNFBPs generally have no interaction with VAs and VASPs, but there may be attorneys-at-law who provide legal services to VASPs.

6.1 INTERACTION BETWEEN VA ACTIVITIES AND THE INFORMAL SECTOR

There are no official statistics on the Informal Sector. However, based on a 2017 study conducted by the Inter-American Development Bank (IADB)[36], the value of Trinidad and Tobago's informal sector can be estimated to range between 26% to 33% of GDP due to the significant use of cash in the country (Inter-American Development Bank, 2017). Following the 2019 demonetisation exercise conducted by the GoRTT, the Central Bank produced a working paper in 2020[37] which posited that economies with sizable informal sectors are typically associated with a significant use of cash (Hilaire, 2020).

In this regard, while the 3rd NRA indicated the existence of an informal economy, cash is the preferred means of payment at this time. Increasing adoption of digital payment options has been observed which warrants monitoring as this may include VAs in the future.

[36] *Inter-American Development Bank (2017), "Estimating the Size of the Informal Economy in Caribbean States"*
[37] *Central Bank of Trinidad and Tobago (2020), "The Great Exchange: Rapid Demonetization in Trinidad and Tobago". https://www.central-bank.org.tt/resources-category/publications-and-research/#working-papers-series*

7.0 VULNERABILITY ASSESSMENT

As noted previously, Trinidad and Tobago did not have a regulatory framework governing the VA/VASP sector for the period under review for the risk assessment. The working group obtained some limited information from entities on their business model and product offering to inform the vulnerability assessment. Reliance was also placed on public source information.

The overall inherent vulnerability of the sector was risk rated as 'Very High' (see Table 3 for the ratings for the individual variables).

Table 3: Ratings assigned to Inherent Vulnerability Variables

#	Inherent Vulnerability Variable	Rating
1)	**Licensed in the country or abroad** (*Considerations in light of the countries entry controls and the comprehensiveness of the legal and regulatory framework*)	Very High
2)	**Nature, size and complexity of business**	Very High
3)	**Products/services** (*The types of VA products and services offered by the VASPs*)	Very High
4)	**Methods of delivery of products/services**	Very High
5)	**Customer types** (*The risk profiles of the customers that VASPs are exposed to*)	Very High
6)	**Country risk** (VASPs' exposure to higher risk jurisdictions)	Very High
7)	**Institutions dealing with VASP** (Counterparty risks from a ML/TF/PF standpoint)	Very High
8)	**VA (Anonymity/pseudonymity)**	Very High
9)	**Rapid transaction settlement**	Very High
10)	**Dealing with unregistered VASP from overseas**	Very High
	OVERALL INHERENT VULNERABILITY RATING	**Very High**

On account of the high value of local on-chain activity (US$1.6 Billion) as reported by Chainalysis, the inherent borderless and pseudonymity nature of VAs, the absence of a VASP regulatory framework, the prominence of the informal sector and the limited information provided by VASPs, a **'Very High'** vulnerability rating has been applied (see Table 4 for the ratings per VASP type).

Table 4: Inherent Vulnerability Ratings by VASP Category / Type of VA Services

VASP Category	Type of service	Sub-Type	Inherent Vulnerability rating
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	Hot Wallet	Very High
	Non-Custodial Services	Cold Wallet	Very High
VIRTUAL ASSET EXCHANGES	Transfer Service	P2P	Very High
		P2B	Very High
	Conversion Services	Fiat-to-Virtual	Very High
		Virtual-to-Fiat	Very High
		Virtual-to-Virtual	Very High
VIRTUAL ASSET BROKING / PAYMENT PROCESSING	Payment Gateway	ATMs	Very High
		Cards	Very High
VIRTUAL ASSET MANAGEMENT PROVIDERS	Fund Management		Very High
	Fund Distribution		Very High
INITIAL COIN OFFERING (ICO) PROVIDERS	Fund Raising	Fiat-to-Virtual	Very High
	Fund Raising	Virtual-to-Fiat	Very High
	Investment	Development of Product & Services	Very High
VIRTUAL ASSET INVESTMENT PROVIDERS	Emerging Products	Crypto Escrow service	Very High
		Crypto-custodian Services	Very High
VALIDATORS / MINERS/ ADMINISTRATORS	Proof of Work	Fees	Medium High
		New Assets	Medium High

8.0 MITIGATING MEASURES

The assessed variables for the mitigating measures fell into three (3) main categories:

- Government Measures;
- VASP Measures; and
- Financial Institution (FI) Measures and Designated Non-Financial Businesses and Professions (DNFBPs) measures.

The mitigation level across these variables were assessed as **'Low'** given the absence of a regulatory framework at the time of the assessment and the limited data provided from VASPs. The ratings assigned per measure are listed out in Table 5 below.

Table 5: Overall Mitigating Measures Rating

#	Mitigating Measures	Threat Rating
1.	**Government Measures:** (The comprehensiveness of the AML/CFT Legal Framework, the availability and effectiveness of entry controls, the adequacy of the supervision and monitoring mechanisms, regulatory requirements for customer due diligence and source of funds and availability of a reliable identity infrastructure, the financial and human resource capacity of LEAs to investigate, trace, seize and secure VAs, the effectiveness of international cooperation and the quality of guidance issued to VASPs, and engagement with VASPs.)	Very Low Mitigation
2.	**VASP Measures:** (The transparency of VASPs' shareholder structure, the quality of VASPs' Governance structure and the level of accountability, the effectiveness of VASP's compliance function and internal control mechanisms and the AML/CFT knowledge of VASPs' staff.)	Close to Nothing
3.	**FI and DNFBP Measures** (The risk assessment and risk mitigation measures by FIs and DNFBPs, and the effectiveness of their compliance function and internal control mechanisms.)	High Mitigation
	OVERALL RATING FOR MITIGATION MEASURES	**Low Mitigation**

8.1 GOVERNMENT MEASURES

The seven (7) input variables under government measures attributing to the **'Very Low'** mitigation rating are assessed below:

1. **Comprehensiveness of the AML/CFT Legal Framework**
   At the time of the assessment, the AML/CFT/CPF framework in Trinidad and Tobago did not consider VAs and VASPs. The subsequent passage of the VA/VASP Act 2025 temporarily prohibits the operation of VASPs as a business until **December 31, 2026**, while at the same time, introduces a Regulatory Sandbox in which VASPs meeting the entry criteria will be permitted to operate under the supervision of the TTSEC. One of the criteria for entry is the capacity of a VASP applying for entry to the Sandbox to comply with existing AML/CFT/CPF laws. A conservative rating of 'Medium' has been adopted given that the legislation has not yet been tested at the time of this report.

2. **Availability and Effectiveness of Entry Controls**
   In the absence of a regulatory framework, market entry controls and fit and proper requirements for VASPs did not exist. The VA/VASP Act 2025 imposes entry requirements for VASPs seeking entry into the Regulatory Sandbox including, *inter alia*, local physical presence, incorporated in T&T, and fit and proper requirements. A conservative rating of 'Medium' has been adopted given that the legislation has not yet been tested at the time of this report.

3. **Adequacy of the Supervision and Monitoring Mechanisms**
   The powers conferred on the TTSEC at the time of the report was not yet in effect. In the absence of a regulatory framework, no authority was identified/empowered with supervisory oversight and monitoring and enforcement powers. Notwithstanding, some supervisory staff have received training on VAs. Further, there are free blockchain explorers that can be utilized for monitoring purposes. However, the technological sophistication of the sector warrants capacity building and the acquisition of specialized solutions for monitoring.

   The Regulators (CBTT, FIUTT, TTSEC) through the Joint Fintech Steering Committee have conducted market surveillance monitoring of VASPs and collected information on VASPs through interactions via the Innovation Hub.

4. **Regulatory requirements for customer due diligence and source of funds and availability of a reliable identity infrastructure**
   This mitigation measure does not exist as the current AML/CFT/CPF framework does not impose AML/CFT requirements on VASPs. Through the several consequential amendments recently made to the existing AML/CFT/CPF legislative regime, VASPs will be subject to the same AML/CFT/CPF obligations as traditional financial institutions, with enhancements made to the law to accommodate nuances in VA transactions, such as the travel rule. The Act further empowers the TTSEC to ensure that VASPs within the Regulatory Sandbox effectively implement these obligations and to take proportionate action where breaches are identified.

5. **Financial and human resource capacity of LEAs to investigate, trace, seize and secure VAs**
   The Miscellaneous Provisions (FATF Compliance) Act 2024 amended the POCA to include a definition of a VA and to provide that a VA should be considered "property or funds" for the purpose of the POCA. This amendment came into force on August 15, 2025 and now provides a legal basis for seizure/freezing/confiscation of VAs. Given the recent proclamation, the provision has not yet been tested.

6. **Effectiveness of international cooperation**
   Trinidad and Tobago has established a framework for facilitating MLAT requests either for seeking cooperation from or providing cooperation to LEAs in other jurisdictions with regard to VA cases. In addition to formal requests through the Central Authority Unit, Trinidad and Tobago also makes use of informal cooperation mechanisms through a number of agencies such as ARIN-Carib and Interpol. These channels have been useful in supporting cross-border investigations, especially in drug trafficking, money laundering, and organized crime as they facilitate the advance confirmation of information that may form part of a MLA request.

7. **Quality of guidance issued to VASPs, and engagement with VASPs**
   VASPs are not licensed or regulated in Trinidad and Tobago, as such, no formal guidance have been issued to VASPs. Notwithstanding, the regulators through the Joint Fintech Steering Committee have provided feedback and guidance to VASPs or persons wishing to conduct VASP activities through the Innovation Hub since 2022. This variable was rated as having very low mitigation.

8.2 VASP MEASURES

The VASPs who subsequently responded to the survey have limited controls in place given that the sector is not familiar with AML/CFT requirements. Notably, open source media revealed one (1) VASP advertising 'No KYC' requirements. Sufficient information was not available to make a determination on transparency or lack thereof of VASPs shareholder structures and the Companies Registry confirmed that none of the known VASPs were registered. Similarly, assessment of the quality of their corporate governance structures, the effectiveness of their compliance function and the internal control function, and the adequacy of the AML/CFT knowledge of their staff could not be undertaken. The absence of this information contributed to the **'Close to nothing'** mitigation rating.

8.3 FINANCIAL INSTITUTION (FI) MEASURES AND DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPS)

The traditional reporting entities have a low risk appetite to doing business with VASPs, offering VA products/services and investing in VAs. Additionally, the following provide a level of mitigating controls.

8.3.1 LIMITS TO CREDIT CARDS

Although the majority of banks have indicated that they do not allow their products/ services to be used to buy VAs, it is widely known that VAs are primarily purchased via credit cards. Based on STR data from the FIUTT and information received via survey responses, activities related to VAs and VASPs in Trinidad and Tobago appear to be mainly private purchases made by individuals utilising credit cards via online trading platforms not domiciled in Trinidad and Tobago. STRs related to VAs were minimal with the value of each transaction ranged between TT$85.00 to TT$15,000.00 (US$12.50 to US$2,205.88) with an average preferred amount of TT$5,000 (US$735) per transaction.

The deposited funds were usually transferred to credit cards of third parties for the purpose of purchasing VAs for individuals. These purchases and trades were observed to occur via a variety of online VA trading platforms, none of which appeared to be domiciled in Trinidad and Tobago.

Overall, the available data suggests that there are purchases of VAs occurring from within the country and a probability of VASPs operating within the country, at a minimum, conducting the purchase and trade of VAs on behalf of others. In this regard, the foreign exchange challenges facing the country in terms of the supply of USD has caused major banks to steadily reduce the US dollar limit on their credit cards. As such, while some persons can circumvent bank's credit card restrictions and use the cards to buy VAs, there is a limit to the amount of VAs that they can actually buy.

8.3.2 NEW PRODUCT/SERVICES REGULATORY APPROVALS

Financial institutions regulated by the Central Bank who intend to launch or utilize a VA product/services, must first obtain approval to do so from the Central Bank. Further verifications are conducted during onsite examinations. DNFBPs are also required to conduct a risk assessment of any new technology, product or service offered or used.

9.0 OVERALL ML/TF RISKS

Given the aforementioned assessment, VAs and VASPs pose a **'Medium High'** ML/TF risk in Trinidad and Tobago. See Table 6 for a summary of the assessment ratings, reflecting the status quo before (as at September 2025) and after the passage of the VA/VASP Act 2025 (as at December 2025), adopting a conservative assessment of the impact given the nascent and unimplemented regulatory environment.

Table 6: Summary of Risk Assessment Summary

RISK ASSESSMENT SUMMARY	AS AT SEPTEMBER 2025	AS AT DECEMBER 2025
Overall ML/TF Threat Exposure	**High**	**High**
Overall ML/TF Vulnerability of Products & Services / Types of VA	**Very High**	**Very High**
ML/TF Risk Level ***before*** Mitigating Measures	**High**	**High**
Quality of ML/TF Mitigating Measures	**Low Mitigation**	**Medium Low Mitigation**
ML/TF Risk Level ***after*** Mitigating Measures	**High**	**Medium High**

10.0 KEY FINDINGS AND RECOMMENDATIONS

10.1 KEY FINDINGS

- The assessment identified four (4) VASPs offering the following services:

TYPE OF VASP	DESCRIPTION OF SERVICES
VA Exchanges	1. Purchase and sale of stablecoins (USDC and USDT) locally. The VASP also provides remittance services and is a Financial Technology company. 2. Purchase of USDT and on-ramp access to Binance and other major crypto exchanges. 3. Purchase VAs, Non Fungible Tokens (NFTs) and participate in VA-related investment opportunities.
VA Broking/ Payment Processing	4. ATM and remittance services where customers can purchase Bitcoin via cash-in at the ATM (fiat-to-virtual), receive funds from local or foreign senders via cash-out at the ATM (virtual-to-fiat). Transactions are strictly in Bitcoin via Lightning-enabled wallets.

Market surveillance of social media forums also suggest the existence of VASPs offering Fund Management/ Fund Distribution activities, conversion services, the distribution of VA cards, validators and Initial Coin Offering Providers. The VASPs which responded to the assessment survey, demonstrate uneven application of mitigating AML/CFT controls.

- Based on Chainalysis reports, 93% of local VA activity is conducted on centralized exchanges. This VA activity appears to be mainly speculative in nature, with persons hoping to benefit from appreciation in value in a short space of time.

- The primary VAs used domestically are: Bitcoin, Ethereum, Tether (USDT), USD Coin (USDC) and NFTs.

- Based on Chainalysis reports, 3.8% of the VA activity was attributed to mining in Trinidad and Tobago which exceeds the global average of 0.2%. This could be as a result of the low electricity rates in Trinidad and Tobago and anecdotal information point to individual mining for personal use.

- Access to darknet marketplaces accounted for a small but increasing portion of the observed illicit activity across in the Chainalysis reports (0.3% in the 2022 report, 1.8% in the 2023 report and 6.7% in the 2025 report). However, no drug trafficking, illicit arms trafficking or human trafficking cases involving the use of VAs were identified and/or investigated for the period under review.

- Given the current challenges with the local foreign exchange market and access to USD, VASP services are being promoted as an alternative to making/receiving cross-border payments which can be exploited by criminals and for illicit activity. Chainalysis reports also highlighted the popularity of VA gambling sites in Trinidad and Tobago.

- High profile instances observed in the media concerning purported VA/VASP activity and ongoing investigations, coupled with statistics from Chainalysis and FATF, indicate that the domestic VA/VASP space is vulnerable to scams and fraudulent investment schemes. In the absence of a regulatory framework, there is a high likelihood that VASPs do not have appropriate AML/CFT risk mitigation measures in place, and that VAs can be misused to launder illicit funds or procure illicit products and services.

- The VA-related/VASP cases investigated by law enforcement for the period 2022 to 2024, did not evidence actual VA activity.

- Traditional reporting entities demonstrate a low risk appetite to interact with VASPs or to offer VA products and services. There is evidence that bank cards have been utilized to purchase VAs but the value/volume is limited based on transaction thresholds placed on cards by the banks. The volume and value of STRs reported on VA-related activity have increased over the scope period, however the FIUTT's analysis determined that the activity predominantly comprised of personal bank-card related transactions which are investment related and do not meet the threshold of suspicion for ML or TF.

- Key regulatory and law enforcement and other agencies, including the TTSEC, CBTT, FIUTT, TTPS, Customs & Excise, BIR and the Judiciary, will require appropriately trained human resources, and the requisite technological monitoring and investigative tools to aid the detection, monitoring, supervision and investigation of VASPs and VA matters.

10.2 RECOMMENDATIONS

The assessment identified a growing domestic VA/VASP ecosystem promoting alternative investments and commercial activity, among other things. In parallel, there has been a proliferation of fraudulent investment schemes and scams seeking to exploit the vulnerable in the society. Given the sector's exposure to ML/TF threats, the inherent vulnerabilities in the VAs and VASPs, and limitations in national mitigating measures that could be exploited by illicit actors, the following are the key recommendations:

1. **Full Implementation of the VA/VASP Act 2025**

At the time of the publication of this report, the Act is in effect and the TTSEC was considering applications received from existing market actors for entry into the Regulatory Sandbox. Measures have also been implemented to monitor for unauthorised VASP activity during the prohibition period.

2. **Capacity Building Programmes for VASPs**

Supervisory authorities to establish regulatory requirements and clear guidelines for the Regulatory Sandbox and the AML/CFT/CPF compliance requirements.

3. **Capacity & Technical Building for Competent Authorities**

Adequate resource allocation and capacity and technical building for regulatory bodies, LEAs and judiciary must be provided to facilitate supervision, monitoring, investigation, asset tracing, seizure, confiscation and recovery.

4. **Traditional Financial Institutions and DNFBPs – Risk Assessments**

Financial institutions and DNFBPs are to consider the ML/TF/PF risks posed by VAs and VASPs in conducting their enterprise risk assessments.

5. **Public Awareness**

Educational campaigns to be undertaken aimed at both consumers and businesses to increase public awareness about the risks and responsibilities associated with virtual assets. This will reduce the incidence of fraud and promote responsible usage of VAs.

6. **Development and Implementation of a Comprehensive Regulatory framework**

The findings of this risk assessment and learnings from the observed activity in the Regulatory Sandbox will provide the foundation for the development of a comprehensive risk based regulatory framework for VAs and VASPs to be implemented at the end of the prohibition period.

7. **Advancement of proposed legislative reform of the National Payment System**

While current data suggests that the activity is primarily of a securities nature, the Central Bank will consider including future-proof provisions for the Payments Systems and Services

(PSS) Bill to cover payments activities involving VAs or conducted by VASPs, as this activity falls under the Central Bank's regulatory remit.

8. Promote innovation in the digital asset space for economic growth and financial inclusion

The GoRTT reaffirms its commitment to digital innovation and citizen-centred services. In respect of moving towards a cashless society and the digitilisation of government payments and services, and to address the evolving Artificial Intelligence (AI) space, the GoRTT will continue to advance key initiatives, including the development of a National Interoperability Framework to ensure systems and agencies operate collaboratively rather than in silos; the launch of Trinidad and Tobago's first National Intelligence Assistant; and the development of a unified citizen services portal to bring all public and legal services into one accessible space. Additionally, the GoRTT, in collaboration with the International Telecommunications Union, has become one of only five countries globally to participate in a landmark AI Governance Assessment, positioning Trinidad and Tobago as a forward-thinking nation in the responsible adoption of AI.

APPENDIX – RED FLAG INDICATORS

The following Red Flag Indicators were taken from FATF's 2020 report on VA Red Flag indicators of ML/TF (Financial Action Task Force, 2020)[38].

1. Size and frequency of transactions

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

- Making multiple high-value transactions –
  - in short succession, such as within a 24-hour period;
  - in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or
  - to a newly created or to a previously inactive account.

- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –
  - there is no relation to where the customer lives or conducts business; or
  - there is non-existent or weak AML/CFT regulation.

- Depositing VAs at an exchange and then often immediately –
  - withdrawing the VAs without additional exchange activity to other VAs, which is an unnecessary step and incurs transaction fees;
  - converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
  - withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.

- Accepting funds suspected as stolen or fraudulent -
  - depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

2. Transactions concerning new users

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

- Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading.

[38] *Financial Action Task Force. (2020). FATF Report Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing.* https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

- A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.

3. Transactions concerning all users

- Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation.

- Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account –
    - by more than one person;
    - from the same IP address by one or more persons; or
    - concerning large amounts.

- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency.

- Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).

- Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.

4. Red Flag Indicators Related to Anonymity

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced virtual asset (AEC) or privacy coins.

- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin.

- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.

- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.

- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.

- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.

- Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.

- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.

- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.

- A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.

- Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.

- Receiving funds from or sending funds to VASPs whose CDD or know-your customer (KYC) processes are demonstrably weak or non-existent.

- Using VA ATMs/kiosks –
    - despite the higher transaction fees and including those commonly used by mules or scam victims; or
    - in high-risk locations where increased criminal activities occur.

- A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).

5. Irregularities observed during account creation

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

- Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.

- Trying to open an account frequently within the same VASP from the same IP address.

- Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.

6. Irregularities observed during CDD process

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

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

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

7. Profile

- A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account.

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

- A customer's VA address appears on public forums associated with illegal activity.

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

8. Profile of potential money mule or scam victims

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.

- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.

- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.

- Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

9. Other unusual behaviour

- A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.

- A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day.
- Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.

- A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure.

10. RED FLAG INDICATORS IN THE SOURCE OF FUNDS OR WEALTH

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

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

- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.

- Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.

- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.

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

- Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.

- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

11. RED FLAG INDICATORS RELATED TO GEOGRAPHICAL RISKS

- Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.

- Customer utilises a VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures.

- Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls.

- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

REFERENCES

Brain, S. a. (2023, March 31). Funding Crime Online: Cybercrime and its Links to Organised Crime in the Caribbean. *The Commonwealth Cybercrime Journal*, p. 94 and 95. Retrieved from https://thecommonwealth.org/publications/commonwealth-cybercrime-journal-volume-1/funding-crime-online-cybercrime-and-its-links-organised-crime-caribbean

Caribbean Investigative Journalism Network. (2023). The High Cost of Subsidized Electricity. Retrieved from https://www.cijn.org/high-cost-of-subsidised-electricity/

Central Bank of Trinidad and Tobago. (2024). *Financial Stability Report 2024.* Retrieved from https://www.central-bank.org.tt/core-functions/financial-stability/financial-stability-report/

Chainalysis. (2024). *The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption.* Retrieved from https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Chainalysis. (2025). *Cryptocurrency activity in Trinidad and Tobago, 2025 Update.*

Chainalysis. (2025). *The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption.* Retrieved from https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/

Chainalysis. (2025). *The Chainalysis 2025 Crypto Crime Report.* Retrieved from https://go.chainalysis.com/2025-Crypto-Crime-Report.html

Cryptocurrencies - Caribbean. (n.d.). Retrieved from Statista: https://www.statista.com/outlook/fmo/digital-assets/cryptocurrencies/caribbean#revenue

Digital Assets - Caribbean. (n.d.). Retrieved from Statista: https://www.statista.com/outlook/fmo/digital-assets/caribbean?currency=USD

Digital Assets - Worldwide. (n.d.). Retrieved from Statista: https://www.statista.com/outlook/fmo/digital-assets/worldwide?currency=USD

Financial Action Task Force. (2020). *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing.* Retrieved from https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

Financial Action Task Force. (2021, October). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Retrieved from https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Financial Action Task Force. (2023). *Crowdfunding for Terrorism Financing.* Retrieved from https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf

Financial Action Task Force. (2025). *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers.* Retrieved from https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

Financial Intelligence Unit of Trinidad and Tobago. (2024, May 29). Advisory to the public on Online Investment Scams (ADV/002/2024). Retrieved from https://fiu.gov.tt/about-us/publications/analysis-products/advisories/

Hilaire, A. a. (2020, June). The Great Exchange: Rapid Demonetization in Trinidad and Tobago. *Working Papers*. Retrieved from https://www.central-bank.org.tt/resources-category/publications-and-research/#working-papers-series

Inter-American Development Bank. (2017). *Estimating the Size of the Informal Economy in Caribbean States.*

Jimenez, J. P. (2025, August 7). Taxation of Crypto Assets in Latin American and Caribbean Countries. *Working Papers*, p. 11. Retrieved from https://www.ciat.org/wp-07-2025-taxation-of-crypto-assets-in-latin-american-and-caribbean-countries-english-soon/?lang=en

Jung, B. R.-S. (2022, August 22). Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. *International Journal of Cybersecurity Intelligence & Cybercrime*. Retrieved from https://vc.bridgew.edu/ijcic/vol5/iss2/2/

Rajic, T. a. (2025, March 18). The ByBit Heist and the Future of U.S. Crypto Regulation. *Critical Questions*. Retrieved from https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation

S, E. (2023, March 28). Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption. *Anti-Corruption Helpdesk*, p. 6 and 7. Retrieved from https://knowledgehub.transparency.org/helpdesk/cryptocurrencies-corruption-and-organised-crime-implications-of-the-growing-use-of-cryptocurrencies-in-enabling-illicit-finance-and-corruption

United Nations Office on Drugs and Crime. (2024). *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat.* Retrieved from https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html

World Bank. (2025). *The Global Findex 2025.* Retrieved from https://www.worldbank.org/en/publication/globalfindex