# VIRTUAL ASSETS

*Evolution of the Digital Era in the Virgin Islands: A Virtual Asset Perspective*

22nd December 2025

**Reproduction is NOT authorised**
**22nd December 2025**

# CONTRIBUTORS

**Jelifa Robinson-Garrin**
**Jheanique Guishard**
**Perla Vanterpool**
**Princess London**
**Heather Mardenborough**
**Angeles Ramirez Payano**

# Table of Contents

# Table of Contents

# Table of Contents

# Table of Contents

# Diagrams & Tables

# PREFACE

The Financial Investigation Agency ("the Agency") is a key component of the Anti-Money Laundering/Countering Terrorism Financing/Countering Proliferation Financing (AML/CTF/CPF) machinery within the Virgin Islands ("VI"). One of the most significant ways in which it fulfils its function is by serving as the Financial Intelligence Unit ("FIU") of the VI in accordance with Recommendation 29 of the FATF Recommendations. Recommendation 29 requires FIUs to conduct analysis, which includes strategic analysis. The unit within the Agency which conducts these functions is called the Analysis and Investigation Unit ("AIU"). According to the Financial Investigation Agency Act, 2003, as amended, strategic analysis *"uses available and obtainable information, including data that may be provided by domestic competent authorities and foreign financial investigation agencies, to identify money laundering, terrorist financing and proliferation financing and related trends and patterns"*. Such data provided by domestic competent authorities and foreign investigation agencies, assists the Agency in identifying money laundering ("ML"), terrorist financing ("TF") and proliferation financing ("PF") typologies.

Strategic analysis achieves the following objectives:

1. Educating stakeholders and reporting entities, about ML/TF/PF-related trends and patterns, as well as related issues.
2. Recommending policies and procedures to fill identified gaps and enhance the future work of the Agency.
3. Informing the development of long-term strategies to combat ML/TF/PF-related threats and vulnerabilities within the VI which sometimes necessitates legislative intervention; and
4. Helping to inform the public about ML, TF, PF and other related issues.

This is the 2025 advanced strategic analysis report that has been compiled and produced by the Agency. The Agency takes this opportunity to renew its commitment to prepare and disseminate, when necessary, strategic intelligence. Doing so undoubtedly enhances the ability of the Agency to contribute in a meaningful way to the AML/CFT/CPF machinery of the Territory of the VI and the global AML/CFT/CPF community.

# GLOSSARY

AIU - Analysis and Investigation Unit

AML/CFT/CPF - Anti-money Laundering/Countering Financing of Terrorism/Countering Proliferation Financing

CSAM – Child Sexual Abuse Material

De-Fi – Decentralised Finance

FATF - Financial Action Task Force

FIU – Financial Intelligence Unit

FSC – Financial Services Commission

LEAs -Law Enforcement Agencies

ML – Money Laundering

TF – Terrorist Financing

PF – Proliferation Financing

STRs / SARs - Suspicious Transaction Reports/ Suspicious Activity Reports

VA - Virtual Assets

VASPs - Virtual Asset Service Providers

VI - The Territory of the Virgin Islands

VI Exchanges - Cryptocurrency exchanges operating in or from within the VI

# EXECUTIVE SUMMARY

The rapid growth of the virtual assets industry has transformed global financial ecosystems, offering new opportunities for innovation while simultaneously creating emerging risks for financial integrity and security. This evolving sector presents unique challenges for regulators, law enforcement and/or FIUs, particularly in relation to money laundering, terrorist financing, and other forms of financial crime. Some of the global common challenges highlighted include:

- Inconsistent adoption of the FATF Travel Rule, which hampers data-sharing across jurisdictions;
- Limited talent pool with specialised technical expertise for blockchain analysis and transaction tracing; and
- Difficulties in regulating unhosted wallets and monitoring cross-border peer-to-peer transactions.

One of the challenges faced by the VI, similar to jurisdictions like Gibraltar and Anguilla, is it has a limited talent pool with the specialised technical expertise for blockchain analysis and transaction tracing.

This strategic analysis report also highlights some of the risks posed by the virtual assets industry in the VI and other jurisdictions due to virtual assets' technological features such as rapid cross-border transfers, pseudonymity and privacy-enhancing tools. Additionally, this report highlights and analyses money laundering and terrorist financing trends and typologies identified from Virtual Asset-related SARs ("VA SARs") filed by VI Exchanges. The report also highlights money laundering and terrorist financing trends and typologies identified by FIUs, regionally and globally, in relation to the virtual assets industry. Some of the emerging typologies and trends include cross-border transfers to evade sanctions, layering through virtual assets and use of unhosted wallets and sanctioned exchanges. One of the key findings is that over the four-year period from 2022 to 2025, the VI observed a distinct increase in financial crime involving virtual assets. This trend aligns with the global evolution of financial technology and the increased use of virtual assets across borders. Understanding the risks and challenges posed by virtual assets is therefore crucial for the VI to develop effective regulatory measures, legislation and guidance to safeguard virtual assets and mitigate the risks posed by the virtual asset ecosystem.

# INTRODUCTION

The evolution of virtual assets began with the introduction of Bitcoin in 2009, the first cryptocurrency developed by Satoshi Nakamoto. The Bitcoin Whitepaper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' outlined the foundational protocol for decentralised digital currency.[1] This innovation marked a pivotal shift in the global financial landscape, demonstrating how blockchain technology could enable secure, peer-to-peer transactions without reliance on traditional financial intermediaries. Its success catalysed the development of numerous alternative cryptocurrencies, each seeking to enhance functionality, address perceived limitations, and introduce innovative mechanisms to improve Bitcoin's model.

Against this backdrop, the evolution of virtual assets has influenced financial systems and regulatory landscapes within jurisdictions such as the VI. A jurisdiction known for its robust financial services industry, the rise of virtual assets presents both opportunities and challenges. As the VI continues to position itself as a forward-thinking financial hub, understanding the implications of virtual assets becomes increasingly important.

# OBJECTIVES & STRUCTURE

This strategic analysis report seeks to explore the risks posed by the virtual assets industry and to provide strategic intelligence to the public, Competent Authorities and Law Enforcement Agencies to effectively identify, assess, and mitigate those risks.

By analysing current trends, typologies, and vulnerabilities within the virtual asset ecosystem, the report aims to enhance national understanding of how illicit actors may exploit these technologies. It also supports the development of informed policy responses and risk-based supervisory strategies aligned with international standards, including the FATF Recommendations on Virtual Assets and Virtual Asset Service Providers.

Ultimately, this report contributes to strengthening the VI's overall AML/CFT/CPF framework by promoting collaboration between government agencies, industry stakeholders, and the public, and ensuring that innovation in the virtual asset space evolves within a secure and compliant environment.



[1] Satoshi, N. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

# SCOPE

Information was gathered from suspicious activity/transaction reports (SARs/STRs), court judgements, legislation, domestic and international Competent Authorities and applicable records in the VI during the period of January 2022 to June 2025.

# METHODOLOGY

This strategic analysis report was put together with information from a variety of sources. Information was first retrieved from the Agency's internal database, which then prompted information gathering from domestic and international Competent Authorities, academia, news article, VI Exchanges, and LEAs. This information was turned into intelligence which then allowed for further collection, collation, and analysis. This allowed the creation of a detailed picture of virtual assets in the VI.

## LEGAL DEFINITION OF VIRTUAL ASSETS IN THE VI

According to section 2(1) of Virtual Assets Service Provider Act, 2022, Virtual Assets and Virtual Assets Service Providers are defined as follows:

*"Section 2(1): -*

Virtual Assets

*...a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, but does not include:*

*(a) digital representations of fiat currencies and other assets or matters specified in the Guidelines[2]; or*

*(b) a digital record of a credit against a financial institution of fiat currency, securities or other financial assets that can be transferred digitally*

Virtual Assets Exchange

*...a trading platform that it is operated for the purpose of allowing an offer or invitation to be made to buy or sell any virtual asset in exchange for money or any virtual asset and which comes into custody, control, power or possession of, or over, any money or any virtual asset at any point in time during its course of business.*

[2]Section 2(5) of the Virtual Assets Service Provider Act provides that references to Guidelines refers to the Guidelines issued by the Financial Services Commission under section 41A of the Financial Services Commission Act, Revised Edition 2020 which provides guidance on what constitutes providing or participating in financial services for purposes of the definition of virtual assets and VASP.

Virtual Assets Service Provider

*...a virtual asset service provider who provides, as a business, a virtual assets service and is registered under the Virtual Assets Service Provider Act to conduct one or more of the following activities or operations for or on behalf of another person:*

a. *exchange between virtual assets and fiat currencies;*
b. *exchange between one or more forms of virtual assets;*
c. *transfer of virtual assets, where the transfer relates to conducting a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another;*
d. *safekeeping or administration of virtual assets or instruments enabling control over virtual assets;*
e. *participation in, and provision of, financial services related to an issuer's offer or sale of a virtual asset; or*
f. *perform such other activity or operation as may be specified in the Virtual Assets Service Provider Act or as may be prescribed by regulations...*"

# ENHANCED UNDERSTANDING OF THE VIRTUAL ASSET ECOSYSTEM

Within the broader category of virtual assets, the FATF also refers to virtual currency, which is a digital form of value that functions as a medium of exchange, unit of account, or store of value, yet does not hold legal tender status in most countries.[3] Virtual currency is not typically issued or guaranteed by governments, and its value depends entirely on user acceptance.

A further distinction is required with cryptocurrency, particularly because this subset of virtual assets forms the basis of most VA SAR filings submitted to the Agency.

A cryptocurrency is a form of digital money that is created and managed using mathematics and cryptography rather than a central authority. Instead, it relies on a distributed network most commonly a blockchain to maintain security, verify transactions, and record the transfer of value.[4]

This structure allows value to be sent directly between individuals without the need for a bank or intermediary. For example, Person A can transfer value to Person B in Singapore on a Saturday within minutes, provided both parties have compatible wallet addresses.

However, cryptocurrencies remain largely unregulated in many jurisdictions and carry significant risks, including the potential to become worthless, as well as exposure to cyber attacks, fraud, and scams (Virtual Assets, n.d.)[5]

**DIAGRAM.1**

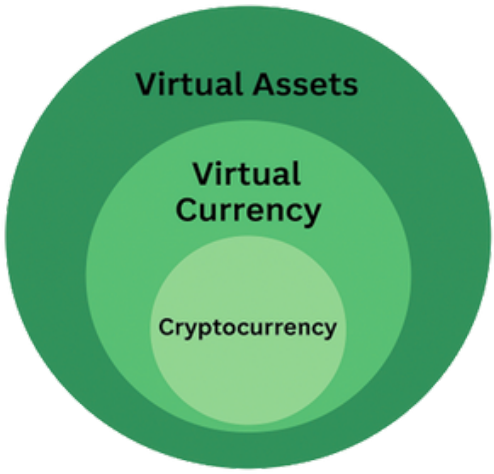



**Diagram.1** illustrates that all cryptocurrencies fall under virtual assets, but many virtual assets are not cryptocurrencies.

[3] Virtual Currencies Key Definitions and Potential AML/CFT Risks. (2014). Financial Action Task Force. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[4] Virtual Currencies Key Definitions and Potential AML/CFT Risks. (2014). Financial Action Task Force. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[5] Virtual Assets. (n.d.). Financial Action Task Force. https://www.fatf-gafi.org/en/topics/virtual-assets.html

# CRYPTOCURRENCY

While there are thousands of different cryptocurrencies in circulation; the cryptocurrencies listed below are the ones common in SARs submitted to the Agency.

**Table.1**

| | | |
|---|---|---|
| **Bitcoin (BTC):** | Bitcoin is the first successful cryptocurrency launched in 2009. Bitcoin is a decentralised and open-source payment system that operates without intermediaries or banks (Bitcoin – Open-Source P2P Money, n.d.).[6] |  |
| **Ethereum (ETH):** | Ethereum is a decentralised blockchain platform launched in 2015. Unlike Bitcoin, which mainly enables digital payments. Ethereum allows anyone to create and operate digital assets, DeFi apps, NFTs, games, and other web3 tools that run 24/7 without intermediaries. Today, it powers a vast ecosystem spanning finance, art, gaming, and decentralised social media, making it a core foundation of the web3 economy (ethereum.org & ethereum.org, 2025).[7] |  |
| **Ripple (XRP)** | Ripple is a payment network designed to make cross-border money transfers faster, cheaper, and more efficient launched in 2012. Its native currency, XRP, is used as a bridge currency that allows financial institutions to instantly convert one currency into another during international transactions. (Ripple, n.d.)[8] |  |
| **Litecoin (LTC):** | Created in 2011, Litecoin is a peer-to-peer cryptocurrency designed for fast, low-cost transactions. It is considered a proven medium of commerce complementary to Bitcoin, it provides quicker confirmation times and lower fees, making it suitable for everyday and frequent payments (Litecoin – Open-Source P2P Digital Currency, n.d.).[9] |  |

[6]Bitcoin - open source P2P money. (n.d.). Bitcoin.org.
[7]ethereum.org & ethereum.org. (2025, October 23). What is Ethereum? ethereum.org.
[8]Ripple. (n.d.). XRP Digital Asset for Global Crypto Utility. https://ripple.com/xrp/
[9]Litecoin - Open source P2P digital currency. (n.d.). Litecoin. https://litecoin.org/

| | | |
|---|---|---|
| **Tether (USDT)** | Launched in 2014, Tether is a stablecoin, meaning its value is pegged to the U.S. dollar (1 USDT ≈ 1 USD). Its purpose is to modernise traditional finance by allowing users to transact with familiar currencies on a blockchain without the volatility usually associated with cryptocurrencies. By enabling the digital use of stable, fiat-backed units of value, Tether became the first platform to simplify cross-border blockchain transactions and broaden access to stable digital payments[10] |  |
| **Solana (SOL):** | Solana is a high-performance global blockchain network that processes transactions in under a second while maintaining extremely low fees. It enables fast, secure, and affordable digital transactions and supports thousands of applications across payments, gaming, digital art, and financial services (What Is Solana? \| Solana, n.d.).[11] |  |
| **Monero (XMR)** | Introduced in 2014, Monero differs from partially transparent privacy-focused cryptocurrencies, such as Zcash, by providing mandatory anonymity for all users. Each transaction automatically obscures the sender, recipient, and transaction amount through technologies such as Stealth Addresses, Ring Signatures, and RingCT. As a result of this default privacy design, Monero transactions cannot be traced on the blockchain, which enhances its fungibility and prevents identification of coins associated with illicit activity or prior misuse (What Is Monero (XMR)?, n.d.).[12] |  |

[10] Tether. (n.d.). What is Tether? https://tether.to/en/

[11] What is Solana? | Solana. (n.d.). Solana. https://solana.com/learn/what-is-solana

[12] What is Monero (XMR)? (n.d.). getmonero.org, the Monero Project. https://www.getmonero.org/get-started/what-is-monero/

# A REGULATORY PERSPECTIVE IN THE VI

The rapid global expansion of virtual assets has prompted standard-setting bodies such as the Financial Action Task Force to strengthen international standards for regulating new technologies. FATF Recommendation 15 specifically requires jurisdictions to identify, assess, and mitigate the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks associated with VA/VASPs and New Technologies. Given that access to cryptocurrency markets is typically facilitated through VASPs, the absence of appropriate oversight can create significant vulnerabilities within a jurisdiction's AML/CFT/CPF framework.

The VIs' ML Risk Assessment 2022 confirmed that new technologies including virtual assets presented a high ML risk, particularly due to the decentralised, anonymity, and cross-border nature of VA activity. VA business models often involve the rapid movement of large values across multiple jurisdictions and the servicing of clients located in high-risk countries. Additionally, the TF Risk Assessment 2025 highlighted that VASPs are one of the sectors that poses the highest vulnerability to terrorist financing in the VI.[1] VA and VASPs are attractive to terrorists because they afford a high level of anonymity that terrorists can exploit to move funds without detection. Prior to regulation, the lack of legislative and supervisory controls over these activities represented a material weakness in the VIs' overall AML/CFT/CPF system, especially given the volume of VA-related business being conducted from within the Territory.[14]

In response, the VI enacted the Virtual Asset Service Providers Act, 2022 ("VASP Act"), which came into force with a transitional period ending on 31 July 2023 and is applicable to all entities operating in or from within the Virgin Islands that qualify and are registered as VASPs under the VASP Act. During this period, all existing businesses conducting virtual asset activities in or from within the Territory were required to apply for registration as VASPs. The VASP Act, together with the Anti-Money Laundering Regulations ("AML Regulations") and Anti-Money Laundering & Terrorist Finance Code of Practice ("AML Code"), established a comprehensive framework governing licensing, customer due diligence, ongoing monitoring, and reporting obligations to the Agency.

This regulatory framework enhances the jurisdiction's ability to detect, prevent, and mitigate the inherent risks associated with VA and VASPs, aligning the VI with FATF standards and strengthening its overall AML/CFT/CPF posture. Specifically, section 4(1) of the VASP Act permits the Agency to have and exercise any of its powers under the Financial Investigation Agency Act, 2003 (as amended) and any other powers under an enactment dealing with money laundering, terrorist financing and proliferation financing in relation to virtual assets and VASPs in so far as those powers are exercisable with respect to an entity.

[14] The BVI Financial Services Commission & Financial Investigation Agency. (2022). Money Laundering Risk Assessment Report - 2022. Financial Services Commission. https://www.bvifsc.vg/sites/default/files/virgin_islands_2022_ml_risk_assessmentam.pdf

Complementing the Act are three key guidance documents issued by the VI Financial Services Commission (FSC):

- ***Virtual Assets Service Providers Guide to the Prevention of Money Laundering, Terrorist Financing & Proliferation Financing***
- ***Virtual Assets Service Providers' AML Guidelines: A Tool for Demonstrating Compliance***
- ***VASP Travel Rule Guidance***

These documents provide practical tools and standards to help VASPs align with AML/CFT/CPF obligations. In addition to the VASP Act, all entities registered in the Virgin Islands including financial institutions and designated non-financial businesses and professions in the VI must comply with the following legislation:

- ***Proceeds of Criminal Conduct Act, 1997 (as amended)***
- ***Anti-Money Laundering and Terrorist Financing Code of Practice, 2008 (as amended)***
- ***Anti-Money Laundering Regulations, 2008 (as amended)***

## REPORTING OBLIGATIONS

Under section 20 of the VASP Act, registered VASPs are subject to ongoing supervisory reporting obligations, including the requirement to submit an annual report to the FSC. This report must provide accurate and current information on the VASP, including but not limited to its financial position, risks encountered or resolved, operational activities, client base, and any significant customer complaints, along with the steps taken to address them. These reporting requirements ensure that FSC maintains effective oversight of registered VASPs and can assess emerging risks within the sector.[15]

## AML/CFT/CPF COMPLIANCE

Under section 25 of the VASP Act, every VASP must maintain robust systems and controls to ensure compliance with all laws related to ML, TF and PF. In addition to the standard customer due diligence obligations under the AML Regulations and AML Code, VASPs are required to maintain records for a period of at least 5 years from the date of termination of a business relationship to which the records relate, and collect and retain key technical data such as Internet Protocol (IP) addresses, timestamps, geographic indicators, device identifiers, wallet addresses, and transaction hashes.

[15] The British Virgin Islands Financial Services Commission. (2022). VIRGIN ISLANDS VIRTUAL ASSETS SERVICE PROVIDERS ACT, 2022. In bvifsc.vg. https://www.bvifsc.vg/sites/default/files/virtual_assets_service_providers_act_2022.pdf

# COOPERATION WITH THE FINANCIAL SERVICES COMMISSION

VASPs must cooperate with the FSC and other Competent Authorities at all times to ensure ongoing compliance. This includes providing any documents or information the FSC requires in connection with its supervisory role.[16]

VASPs must promptly notify the FSC of any material changes to their business, including:

- Any enforcement or criminal proceedings taken against them locally or internationally;
- The acquisition of a controlling interest in another virtual asset business; or
- No longer meeting any of the registration requirements of the VASP Act

Additionally, VASPs must request approval from the FSC prior to registering or licensing in another jurisdiction or opening any new offices or physical locations abroad

# THE GLOBAL REGULATORY LANDSCAPE

## REGULATORY FRAMEWORKS

Effective global oversight of VA requires harmonised and risk-based regulatory frameworks that promote transparency, financial integrity, and market stability. Across the globe, about 99 jurisdictions have now passed legislation implementing the Travel Rule, thereby advancing their regulatory frameworks for VA and VASPs.[17] These frameworks are guided primarily by international standards established by FATF, which introduced its revised Recommendations in 2019 to explicitly cover VA and VASPs.

Countries with advanced regulatory infrastructures such as the United States, the United Kingdom, Singapore, and members of the European Union have taken leading roles by embedding these standards within domestic law and establishing licensing, monitoring, and enforcement mechanisms. Meanwhile, developing jurisdictions continue to enhance institutional capacity, strengthen inter-agency coordination, and build the technical expertise required to effectively regulate virtual assets activities.

[16] The British Virgin Islands Financial Services Commission. (2023). Virtual Assets Service Providers Guide to the prevention of money laundering, terrorist financing and proliferation financing. In bvifsc.vg. https://www.bvifsc.vg/sites/default/files/vasp_aml_cft_guidance.pdf

[17] FATF, Best Practices on Travel Rule Supervision (Paris: Financial Action Task Force, 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-RuleSupervision.pdf

# GLOBAL CHALLENGES & TYPOLOGIES

Despite the existence of regulatory frameworks globally, and drawing on insights from jurisdictions such as Gibraltar, Singapore, and others with established VA/VASP oversight regimes, countries continue to face similar challenges in the practical implementation of these frameworks. The report will now highlight some of the common challenges and typologies related to four jurisdictions that have adopted VA namely Guyana, Anguilla, Gibraltar and Singapore.

## GUYANA

Guyana's 2023 Virtual Assets and VASPs Risk Assessment marked the country's first comprehensive evaluation of how virtual assets could be exploited for money laundering and terrorist financing. Although Guyana remains largely cash-based, the rise of crypto trading, cross-border remittances, and informal peer-to-peer transactions have created new vulnerabilities.

Key challenges include the absence of a licensing framework for VASPs, limited blockchain tracing capabilities, and weak inter-agency coordination. The FIU stresses the need for updated legislation, regulatory training, and cross-border cooperation to effectively manage virtual asset risks.

The Risk Assessment also identified typologies such as the conversion of illicit fiat currency into virtual assets, transfers through offshore or unhosted VASPs, and the use of chain-hopping and mixers to disguise fund origins. The mining and oil sectors, along with limited financial inclusion in rural areas, increase exposure to informal crypto activity.[18]

## ANGUILLA

Anguilla's National Risk Assessment identifies several key challenges contributing to its very high money laundering risk in the virtual asset sector. The complex and evolving nature of virtual asset products poses challenges, as they differ from traditional financial services and require tailored AML/CFT controls. Strengthening beneficial ownership transparency is another priority, with improvements needed in the national database to enhance oversight. The broad client base of VASPs including members of the public, PEPs, and high-net-worth individuals—further increases exposure to misuse. Additionally, limited human resource capacity and technical expertise constrain the jurisdiction's ability to effectively implement legislative and supervisory improvements.

[18] AML/CFT/PF National Coordination Committee. (2023). Money Laundering/Terrorist Financing Risk Assessment Of Virtual Assets And Virtual Asset Service Providers. In Financial Intelligence Unit of Guyana. Retrieved October 24, 2025, from https://fiu.gov.gy/wp-content/uploads/2024/01/Risk-Assessment-Virtual-Assets-and-VASPs.pdf

[19] Information provided by Financial Intelligence Unit, Anguilla

Typologies identified in the Anguilla National Risk Assessment highlight the misuse of Anguilla-registered entities to facilitate virtual asset–related money laundering. In several cases, Anguilla-registered companies were used as fronts to receive fiat funds and convert them into virtual assets. Investigations also revealed the purchase of virtual asset products via Binance and Bifinity in European jurisdictions using UK online banking, with links to serious criminal conduct, including conspiracy to murder and organised crime activity. Additionally, there was an attempted purchase of virtual assets through an Anguilla-based VASP by a subject seeking to launder proceeds from a foreign fraud scheme. The transaction was ultimately refused due to insufficient KYC information, demonstrating the effectiveness of compliance controls within the regulated sector.[19]

## GIBRALTAR

Gibraltar introduced its Distributed Ledger Technology (DLT) Regulatory Framework in 2018, making it one of the first jurisdictions to formally regulate virtual asset activities. The framework requires registered VASPs to use blockchain analytics for monitoring and implemented the FATF Travel Rule in 2021 to enhance transaction traceability. In alignment with this, the Gibraltar Supervisory Authority has implemented its own use of blockchain analytics to assess risks at both the firm and sectoral levels, which allows the Supervisory Authority to monitor shifts in VASPs' on-chain exposure and to incorporate these insights into supervisory decision-making, including during the licensing process for new applicants.

As a small jurisdiction, Gibraltar faces challenges in attracting qualified professionals for key regulated roles. The higher-risk nature of virtual assets requires personnel with specialised technical and compliance knowledge, which is less common than in traditional financial sectors. While the Gibraltar Supervisory Authority acknowledges these challenges, it maintains strict fitness and propriety standards and does not grant exemptions or relax requirements for regulated positions. In recent years however, the Gibraltar Supervisory Authority has observed a notable improvement in the availability of qualified professionals within Gibraltar's DLT sector.

In line with global standards, the Gibraltar Supervisory Authority is preparing to fully enforce the FATF Travel Rule within Gibraltar's virtual asset sector. Although the requirement was introduced into local legislation in 2021, practical enforcement was delayed by the "Sunrise Issue" where other jurisdictions had not yet adopted equivalent measures. This created an informal grace period during which VASPs were aware of their obligations but not yet required to comply in full.[20]

[19] Information provided by Financial Intelligence Unit, Anguilla
[20] Information provided by Gibraltar Financial Intelligence Unit (GFIU)

## SINGAPORE

In Singapore, the main challenges lie in tracing and recovering illicit funds due to technological characteristic of VA, and foreign-based or unregulated exchanges that fall outside of Singapore's regulatory reach. Regulators face a constant race to keep pace with technological change while maintaining proportionate supervision. Singapore's 2024 Virtual Assets Risk Assessment highlights the need for stronger cross-border collaboration with LEAs and Regulatory bodies.

Additionally, Singapore's 2024 Virtual Assets Risk Assessment found that the primary typologies of misuse involve cyber-enabled fraud, ransomware, and theft of digital wallet funds. Criminals often convert illicit fiat proceeds into digital payment tokens, conceal them through mixing or chain-hopping, and move them across borders. Also, emerging typologies include the use of decentralised finance protocols, unhosted wallets, and NFTs.[21]

The Appendix attached to this Report entitled "*Additional Information on a Global Perspective of Virtual Assets*" highlights additional challenges, trends and typologies for other jurisdictions within the global landscape of virtual asset adoption.

# COMMON CHALLENGES FOR VI

Similarly, whilst the VI has implemented regulatory frameworks to govern virtual assets, it is not exempt from challenges. Some of the common challenges are as follows:

- Limited talent pool with specialised technical expertise for blockchain analysis and transaction tracing.
- Since VASP clients are overseas, obtaining intelligence or customer information from foreign counterparts can be slow or, in some cases, unsuccessful. This can delay or prevent access to key data needed to substantiate suspicious transactions.
- The volume of VA SARs increases operational pressure on the Agency, reinforcing the need to continually strengthen and refine existing policies and procedures to effectively manage and prioritise cases.

[21]Monetary Authority of Singapore. (2024). Virtual Assets Risk Assessment (30 October 2024). https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/virtual-assets-risk-assessment.pdf

- Cryptocurrency investigations require immediate action; however, the time gap between when the activity occurs, when the SAR is received, and when the case can be assessed and disseminated can limit opportunities to intervene. Given the rapid movement of cryptocurrency, this overall processing timeline can reduce the likelihood of timely disruption or recovery of funds once they have been withdrawn.

- Prosecution may be challenging due to the suspect residing in a foreign jurisdiction, which complicates efforts to secure a conviction or proceed with legal action.

These challenges contribute to inconsistent enforcement and create regulatory gaps that may be exploited for illicit activities, including ML, TF and PF.

## RISKS ASSOCIATED WITH VIRTUAL ASSETS

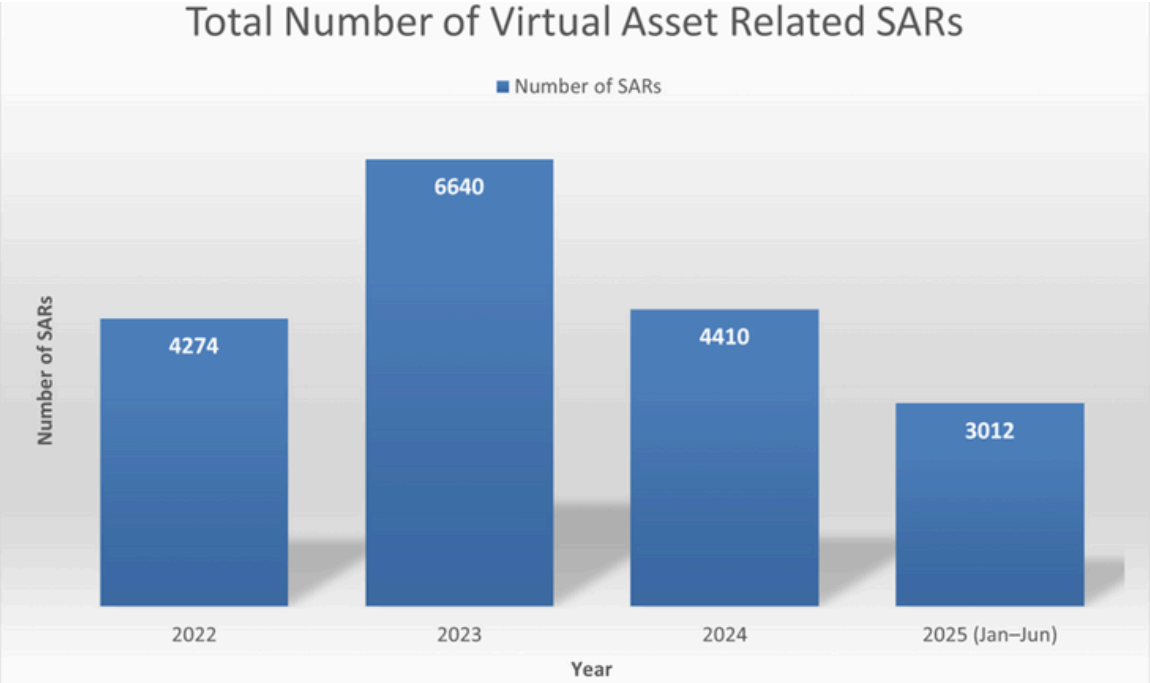
Virtual assets pose significant risks due to their technological features such as rapid cross-border transfers, pseudonymity, and privacy-enhancing tools. Although transactions are transparent on the blockchain, wallet owners are identified only by alphanumeric strings, making it easier to conceal beneficial ownership. Also, criminals exploit privacy coins such as Monero and Zcash, mixers/tumblers that obscure transaction trails, and transfer funds through unregulated decentralised exchanges. These heightens the risks of VA being used for ML, sanctions evasion, TF and PF. The instantaneous, borderless nature of VA, along with inconsistent AML/CFT/CPF regulations across jurisdictions, creates regulatory gaps and challenges in tracing or recovering illicit funds.

## SUSPICIOUS ACTIVITY OF VIRTUAL ASSETS WITHIN THE VI: OFFENCES & TRENDS

This section provides an analysis of the VA SARs received in the VI. Approximately 99% of the subjects identified in these reports are located in foreign jurisdictions, indicating that persons using VI Exchanges, are typically not residents of the VI. Diagram 2 below indicates the number of VA SARs the Agency received between January 2022 and June 2025.

During 2023, there was a notable increase in VA SARs. This upward trend can be attributed to several factors such as the VASP Act that was enacted in December 2022, which provided a transitionary period until 31 July 2023, during which all existing virtual asset businesses operating in or from within the VI were required to apply for registration as a Virtual Asset Service Provider.

**DIAGRAM.2**




Additionally, all VI entities carrying out virtual asset services business were obligated to comply with existing AML/CFT/CPF legislative requirements. This increased regulatory scrutiny, combined with mandatory filings to the relevant competent authorities as part of the registration process, likely contributed to the surge in SAR submissions. This trend was reflected in the growing number of VA SAR filers, which increased from 15 in 2022 to 29 by 2024.

Another factor that may have contributed to the rise in VA SARs can be as a result of FATF's "*Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (VASPs) 2022*". The report urged jurisdictions to accelerate adoption of FATF's standards particularly Recommendation 15 and Interpretive Note 15, which require countries to regulate, license, and supervise VASPs for AML/CFT/CPF compliance and implement the "Travel Rule" for originator and beneficiary information.[22]

As international conflicts intensified including the Russia–Ukraine war and the Israel–Hamas conflict, the United States and United Kingdom ("UK") significantly expanded their sanctions regimes including crypto mixers and other high-risk entities.

[22] FATF (2022) Targeted update on implementation of the FATF Standards on virtual assets and virtual asset service providers (VASPs) (Paris: FATF/OECD, 2022), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

These developments prompted financial institutions to enhance their compliance frameworks, and strengthen transaction monitoring, which in turn contributed to an overall increase in VA SARs. According to the Office of Financial Sanctions Implementation ("OFSI") Annual Review 2023–24, this escalation in global tensions directly influenced UK sanctions activity, with OFSI adding 564 designated persons to the consolidated list.[23]

Lastly, advances in detection technology have strengthened transaction monitoring, supported by the growing adoption of blockchain tracing tools such as Chainalysis and TRM Labs. As a result, the number of VA SARs filed by reporting entities climbed, reflecting improved detection capabilities and a stronger compliance culture across the sector.

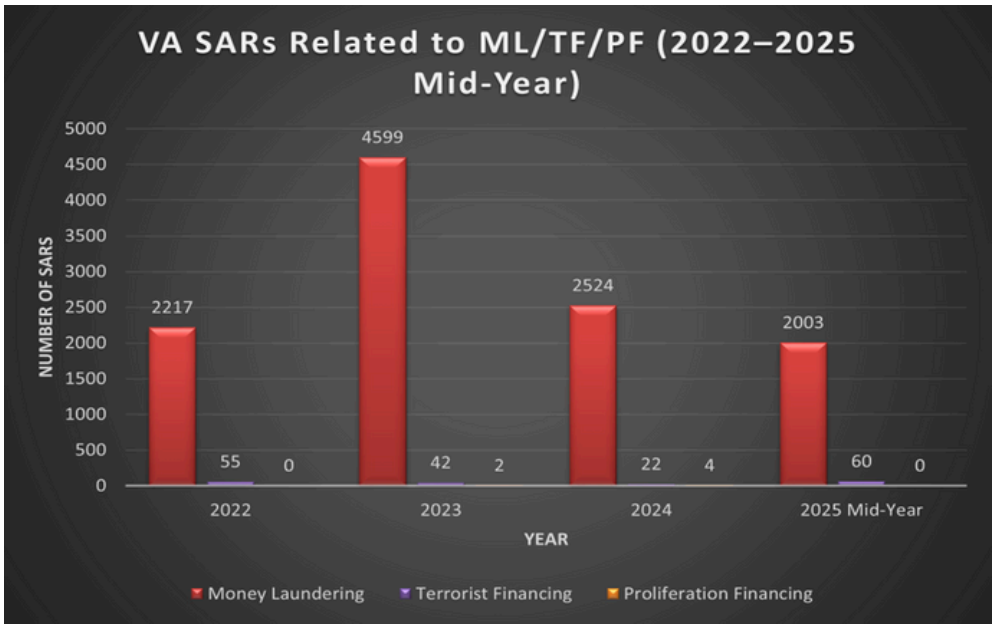
Collectively, these worldwide changes increased both the awareness and reporting obligations of institutions within the VI, that helped drive a sharp increase in VA-related SARs.

## OFFENCES AND TRENDS IN THE VI

Over the four-year period from 2022 to 2025, the VI observed a distinct increase in financial crime involving virtual assets.This trend aligns with the global evolution of financial technology and the increased use of virtual assets across borders. The VA SARs received are categorised within the broad categories of money laundering, terrorist financing and proliferation financing. This is demonstrated in Diagram 3 below.

As shown in Diagram 3, money laundering remains the most frequently reported offence in VA SARs, mirroring the trend observed in traditional financial crime cases.

**DIAGRAM.3**




[23]Office Of Financial Sanctions Implementation. (2025, March 21). OFSI Annual Review 2023 to 2024: Engage, Enhance, Enforce. GOV.UK. https://www.gov.uk/government/publications/ofsi-annual-review-2023-24-engage-enhance-enforce

## ML/TF/PF

Money laundering has been the most notable offence identified in the VA SARs received by the Agency between 2022 - 2025. Money laundering materialises more frequently because VA offer features that are attractive to criminals seeking to obscure the origin or movement of illicit funds. These include pseudonymity, rapid cross-border transfers, the use of privacy-enhancing technologies, and accessibility to unregulated or lightly regulated exchanges. As a result, typical ML behaviours such as layering, obfuscation, chain-hopping, and the use of mixers or decentralised protocol surface more readily in VA SAR reporting.

In contrast to money laundering, virtual asset transactions may provide only limited indicators of proliferation financing, as PF activity is more commonly associated with the procurement, shipment, and payment for physical goods and components. The Department of the Treasury's De-risking Strategy highlights that proliferation networks' use of opaque corporate entities to engage with the U.S. financial system for what appears to be legitimate commercial activities could enable indirect operation through correspondent banking networks (U.S. Department of the Treasury, 2023). Similar patterns have been observed across earlier National Proliferation Financing Risk Assessments, indicating a continued reliance on traditional financial channels.[24] As a result, PF risk may be less readily observable within VA SARs when compared to other illicit finance typologies.

With respect to terrorist financing, TF observed in VA SARs most often arises from the identification of virtual asset wallet addresses linked to sanctioned individuals or entities, where value is transferred to or received from such addresses, either directly or through indirect exposure. This typology may be more readily identifiable than proliferation financing, as relevant wallet addresses are often publicly designated as specially designated nationals and blocked persons through sanctions lists such as those maintained by the Office of Foreign Assets Control of the US Department of the Treasury ("O FAC").

Overall, this imbalance reflects the greater visibility and detectability of money laundering and terrorist financing activities within the virtual asset ecosystem, while proliferation financing activities are less commonly associated with the retail-level transactions and behavioural patterns that typically trigger VA SAR filings.

## HIGHEST ML OFFENCE - FRAUD

Given the landscape outlined above, it is evident that money laundering comprises the highest proportion of cases reported. Within this category, the analysis now turns to fraud, which represents the dominant predicate offence. Its substantial prevalence drives overall ML reporting volumes, and accordingly, the Agency seeks to specifically highlight this offence category.

[24]U.S Department of Treasury. (2023). 2023 De-Risking Strategy. Retrieved November 14, 2025, from https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf

The following section therefore examines fraud-related trends and typologies in greater detail, recognising its outsized impact on VA SARs and its central role in shaping the current money laundering risk profile.

Fraud involves the intentional use of deception to obtain money or assets and, in the virtual asset space, often features submission of misleading information, false identities, or fake investment opportunities to access or move cryptocurrency. Fraudsters exploit the speed, global reach, and pseudonymity of crypto to quickly convert and conceal illicit funds.

For example, during onboarding with a VI Exchange, individuals may attempt to circumvent verification controls by submitting passport images in place of a live selfie or by using AI-generated documents. Such attempts are typically flagged as suspicious and result in account rejection. Another example is VI Exchange clients receiving of funds linked to wallet addresses associated with “pig-butchering” and other investment scams. These schemes demonstrate how virtual assets are used to layer and rapidly move fraud proceeds across jurisdictions.

Lastly, fraudsters use of credit cards to purchase cryptocurrencies with the VI Exchange, followed by client-initiated chargeback requests to issuing banks after the purchased assets have been withdrawn from the exchange, leaving VI Exchanges exposed to negative account balances and financial loss.

**DIAGRAM.4**

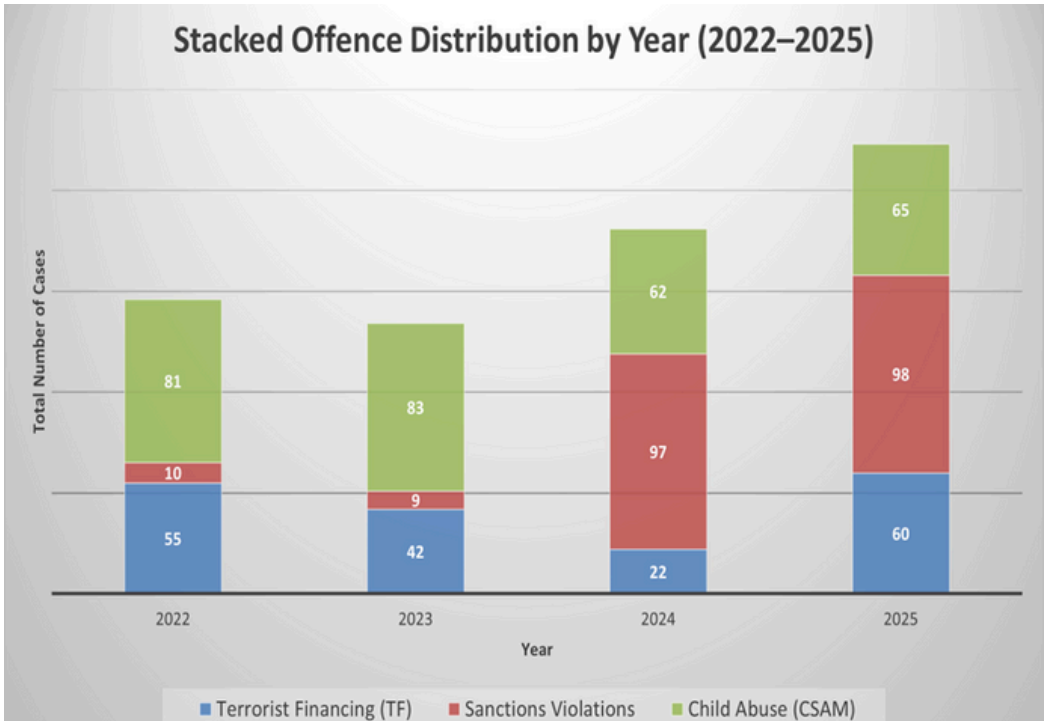

Although fraud continues to dominate reported offences, trends have fluctuated over the period reviewed. Diagram 4 above however indicates that fraud is likely to surpass 2024 levels by year-end as the 2025 statistics reflect only mid-year data.This renewed activity may be influenced by the evolving political and regulatory environment surrounding virtual assets, as well as the rapid advancement of AI. These developments have stimulated greater market participation and, consequently, created opportunities for both legitimate innovation and exploitation by fraudulent actors.

## HIGH-RISK OFFENCES

High-risk offences are predicate crimes that pose significant threats to national security, public safety, and the integrity of the financial system. These offences typically involve substantial ML/TF/PF exposure, cross-border elements, and serious harm to vulnerable populations. Within the virtual asset environment, high-risk offences include activities such as terrorist financing, sanctions breaches, and the dissemination or purchase of Child Sexual Abuse Material ("CSAM") all of which are recognised by global standard setters as priority risk areas requiring enhanced detection and reporting.

Although the number of VA SARs directly linked to these offences remains relatively low, the Agency continues to receive several high-risk VA-related cases. Diagram.5 below illustrates the number of commonly identified high-risk offences reported.

### DIAGRAM.5




Sanctions-related SARs peaked in 2024, largely due to the expansion of international sanctions regimes and intensified enforcement efforts. As previously mentioned, during this period, the UK significantly broadened its sanctions framework, with OFSI adding 564 designated persons to the consolidated list. These developments created heightened compliance scrutiny and increased attempts to use virtual assets to circumvent sanctions, ultimately leading to a rise in sanctions-related suspicious activity reports.[25]

[25]Office Of Financial Sanctions Implementation. (2025, March 21). OFSI Annual Review 2023 to 2024: Engage, Enhance, Enforce. GOV.UK. https://www.gov.uk/government/publications/ofsi-annual-review-2023-24-engage-enhance-enforce

Child sexual abuse material (CSAM) remains a significant category each year, as illicit actors exploit the perceived anonymity of wallet addresses to purchase explicit content using virtual assets. These transactions are often identified through blockchain monitoring tools or red-flag indicators and are subsequently reported by the VI Exchange. As the Agency continues to treat these cases with the highest priority, it is encouraging to note that the number of CSAM-related SARs have been decreasing.

## TYPOLOGIES OF COMMON OFFENCES

The analysis of VA SARs further revealed several recurring typologies linked to the misuse of virtual assets in the VI:

## LAYERING THROUGH VIRTUAL ASSETS

Clients were observed transferring large amounts of fiat currency (USD) from their bank accounts to regulated exchanges in the VI via bank transfers. The funds were then converted into Tether (USDT) and assets were subsequently transferred from regulated platforms to unregulated exchanges. This activity pattern aligns with the layering stage of money laundering, intended to obscure the origin of illicit funds through rapid conversion and movement across platforms.

## CROSS-BORDER TRANSFERS TO EVADE SANCTIONS

There has been a notable increase in money laundering cases involving Kazakhstan, rising from 13 cases in 2022 to 134 in 2024. Reported transaction values reached approximately USD 6 million in 2023. The transactions typically involved the rapid movement of funds across multiple exchanges, including VI Exchanges, suggesting deliberate attempts to circumvent Russian-related sanctions as the suspects were Russian and Kazakhstan nationals with Kazakhstan addresses.

## USE OF UN-HOSTED WALLETS AND SANCTIONED EXCHANGES

Several investigations identified the use of personal unhosted wallets to transfer funds to unregulated exchanges, sanctioned entities or jurisdictions associated with illicit activity. This typology highlights ongoing challenges in monitoring peer-to-peer transactions and enforcing compliance across decentralized ecosystems.

## TERRORISM FINANCING INDICATORS

VA SARs revealed transfers from multiple nationalities to wallet addresses linked to Hamas and other groups associated with terrorist financing.

## CARD-PAYMENT FRAUD

Fraudsters on-ramp fiat currency to VI Exchange using debit or credit cards. The funds are immediately converted into cryptocurrency and subsequently withdrawn to external wallets.

Following the outflow of funds from the exchange, the individuals initiated chargeback requests with their issuing banks, falsely claiming the transactions were unauthorised. As the cryptocurrency had already been transferred off-platform, the exchange was unable to recover the funds from the clients' accounts causing financial loss to the exchange.

## AGE-BASED RISK PATTERNS IN VA SARS

An analysis of VA SARs received by the Agency reveals clear age-based behavioural patterns in virtual asset engagement. Differences in digital familiarity and exposure to risk inform whether individuals within these demographics are more commonly identified as perpetrators or victims in VA SARs. Analysing these demographic dynamics provides valuable insight into the evolving risk landscape and supports the development of more targeted mitigation strategies.

## GENERATION Z (1997-2012)

Reports involving Generation Z increased from 2.6 % of VA SARs in 2022 to 7.1% in 2023 rising sharply to 19.1% in 2024 then, by mid-2025, 20.9%. Within the VA SARs reviewed, Generation Z accounted for 15% of suspects in terrorism financing, 47% in money laundering, and 14% in sanctions breach matters. Regarding analysis of 482 fraud-related SARs, it was revealed that Generation Z accounted for 30.5% of fraud perpetrators. This pattern reflects the growing engagement of younger demographics in virtual asset activity. At the same time, their lower financial capacity may limit their overall involvement in higher value or more complex criminal schemes.

## GENERATION Y MILLENNIALS (1981-1996)

Millennials remain the dominant generation across all reporting periods accounting for the largest share of SARs linked to virtual asset activity. Reports increased from 4.8% in 2022 to 19% in 2023, before surging to 45.3% in 2024 and continuing upward to 49.3% by mid-2025. They constitute the largest portion of suspects across typologies, including 60% in terrorism financing, more than 100% in money laundering due to multiple suspects per case, and 82% in sanctions breaches. Regarding analysis of 482 fraud-related SARs, it was revealed that Millennials accounted for the largest share of fraud perpetrators at 53.2%, emerging as the dominant offender group involved in fraud typologies. This sustained growth underscores Millennials' strong adoption of virtual assets and their greater financial capability, which collectively positions them as the primary risk cohort in VA-related criminal activity.

## GENERATION X (1965 - 1980)

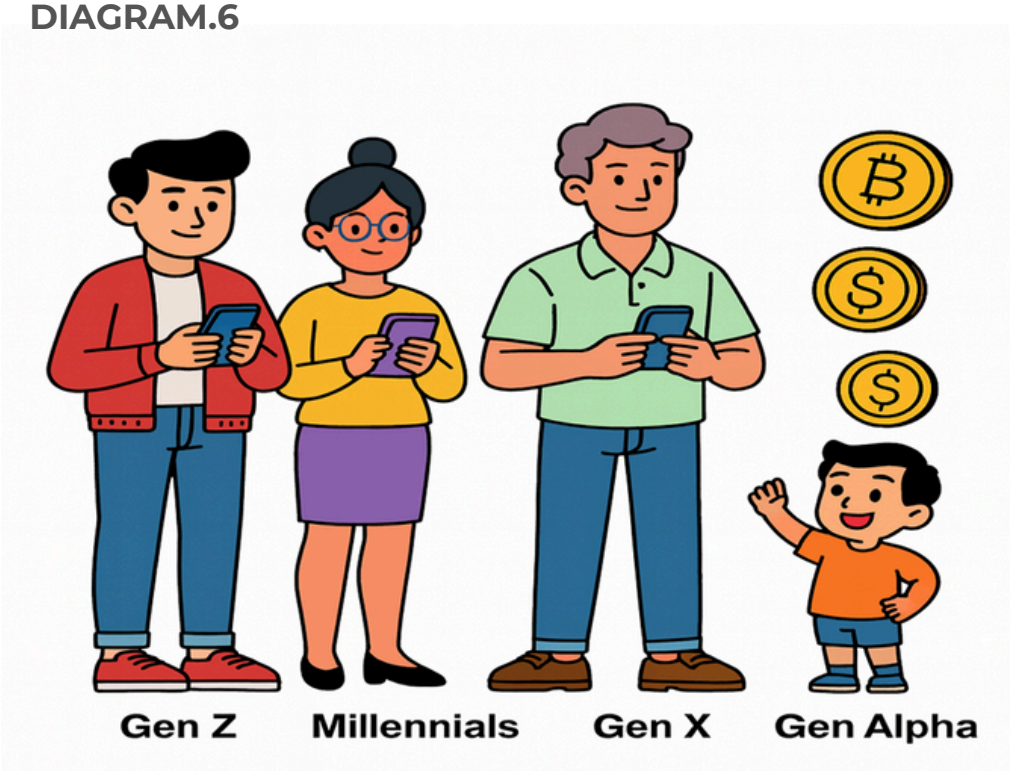
VA SARs involving Generation X increased from 1.68% in 2022 to 6.7% in 2023, 16.44% in 2024, and 15.17% in 2025. Generation X comprised 25% of terrorism-financing suspects, 26% in money laundering, and 22% in sanctions breaches. Regarding analysis of 482 fraud-related SARs, it was revealed that Generation X accounted for 16.3% of fraud perpetrators.

## BABY BOOMERS (1946 – 1964)

Reports involving individuals over 60 years old were absent from 2022 to 2024, with only four (4) cases recorded in 2025. This low representation highlights limited adoption of VA among older adults yet raises potential red flags for investment or romance scams that specifically target retirees.

The data therefore highlights generational trends in SARs involving virtual assets, showing greater crypto engagement among younger demographics. Generation Z and Millennials appear as the most active users, reflected in the sharp rise in VA SAR submissions tied to their digital fluency. Generation X shows deliberate participation, often linked to transactional behaviour and attempts to obscure fund origins. Whilst Baby Boomers appear as the least active users.

**DIAGRAM.6**

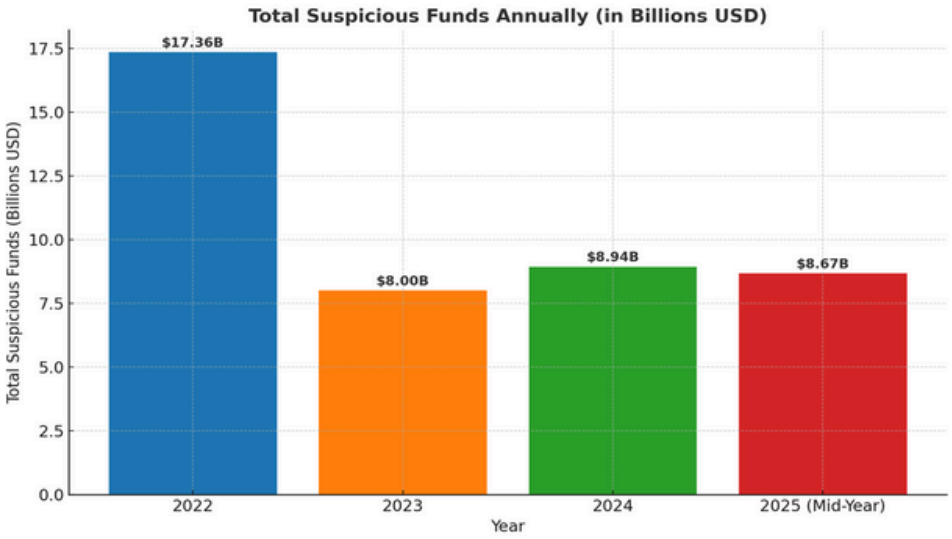



The illustration depicts Gen Alpha (2013 – 2025) as the next emerging wave of adopters, as digital assets become further normalized.

## VALUE REPORTED THROUGH VA SARS

Annually, the total suspicious values reported through VA SARs to the Agency are illustrated below:

**DIAGRAM.7**




## VALUE ANALYSIS

The data indicates a substantial decline in reported suspicious funds from 2022 ($17.36 billion) to 2023 ($8 billion), a decrease of approximately 54%. This sharp drop may be attributed to China's unique spike in suspicious amounts reported in 2022 with one case being valued at 1 billion, while $8 billion represents a more typical annual average for VA related SARs reported to the Agency. In 2024, reported amounts increased modestly to $8.94 billion, suggesting a stabilisation in VA-related reporting trends.

By mid-2025, the total already stands at $8.67 billion, suggesting that the full-year figure is on track to surpass 2024's total, which is in line with the increase in SARs received in 2025. This spike may be due to political and policy changes within the United States, which remains the most active global issuer of financial sanctions.

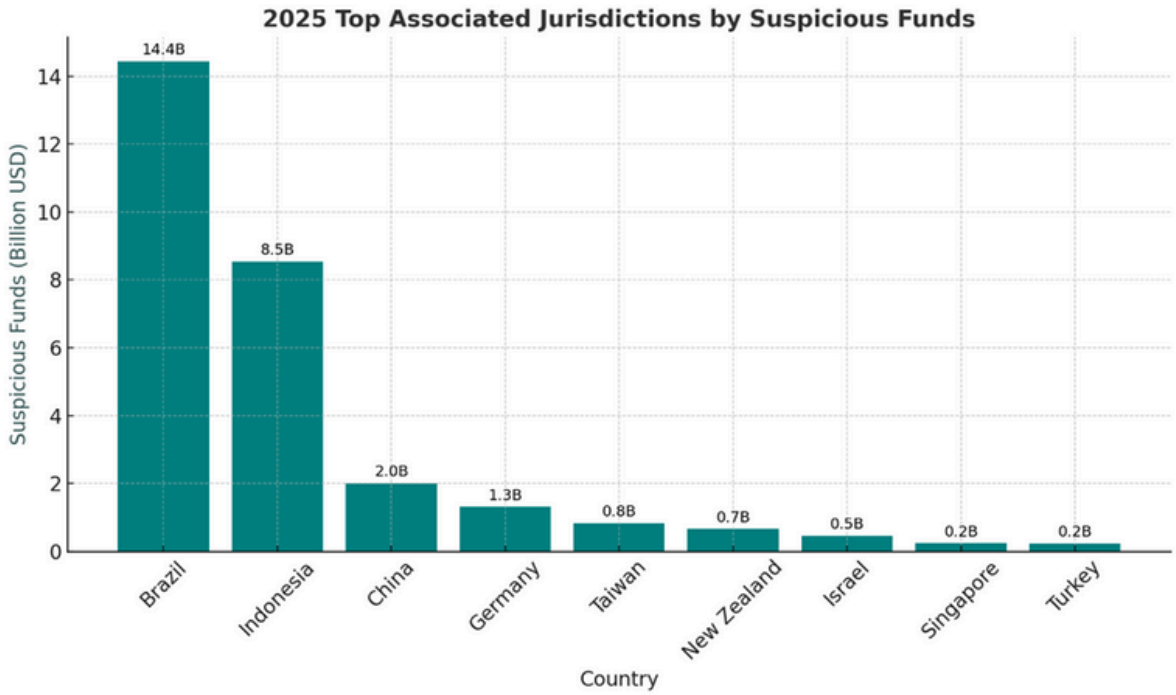
## GEOGRAPHICAL ANALYSIS

As previously mentioned, the majority of the VA SARs received by the Agency concern activities on the virtual platform where clients are residents of other countries. Diagrams 8 - 11 below outline the top countries associated with VA SARs by corresponding suspicious values, starting from 2025 (mid-year) and ending with 2022.

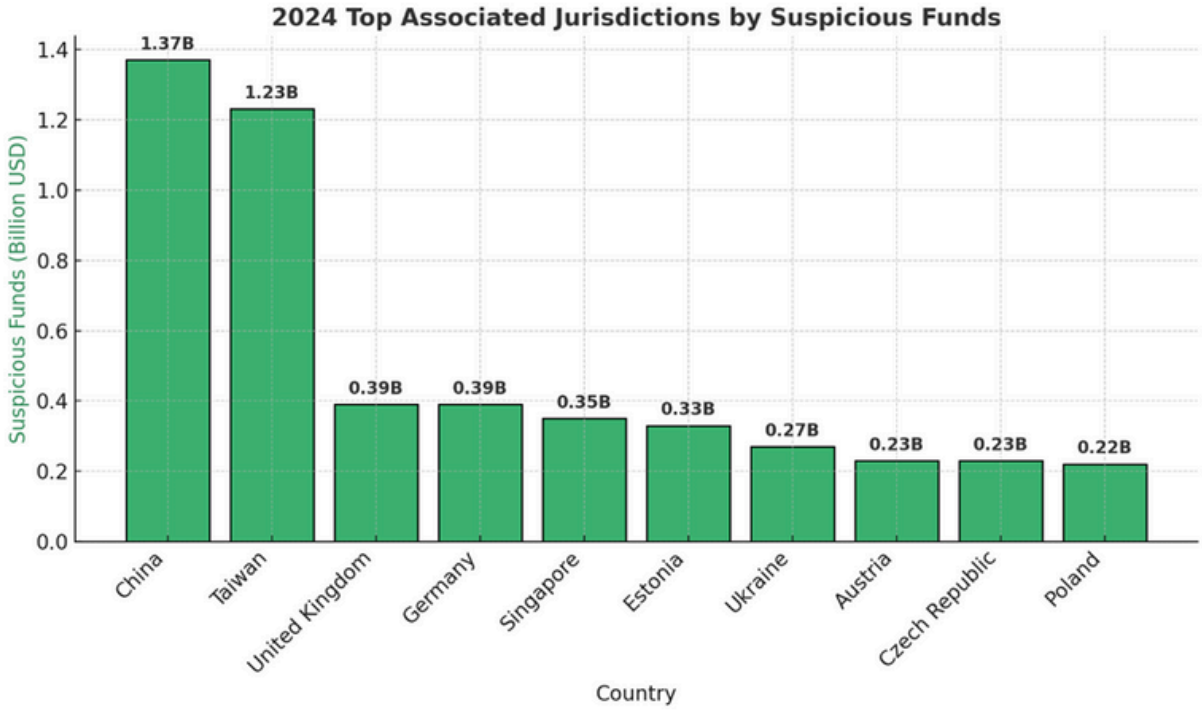
Additionally, diagrams 8 - 11 represent where the suspect committing the potential illicit activity is understood to originate, based on information provided on nationality or residency. It should therefore be interpreted as indicating the geographic origin of the subject.

The purpose of this information is to highlight which jurisdictions are linked to the highest value of suspicious activity reported by VI Exchanges. This helps the Agency understand where larger exposures may be coming from, identify emerging regional patterns, and focus supervision and intelligence efforts more effectively.

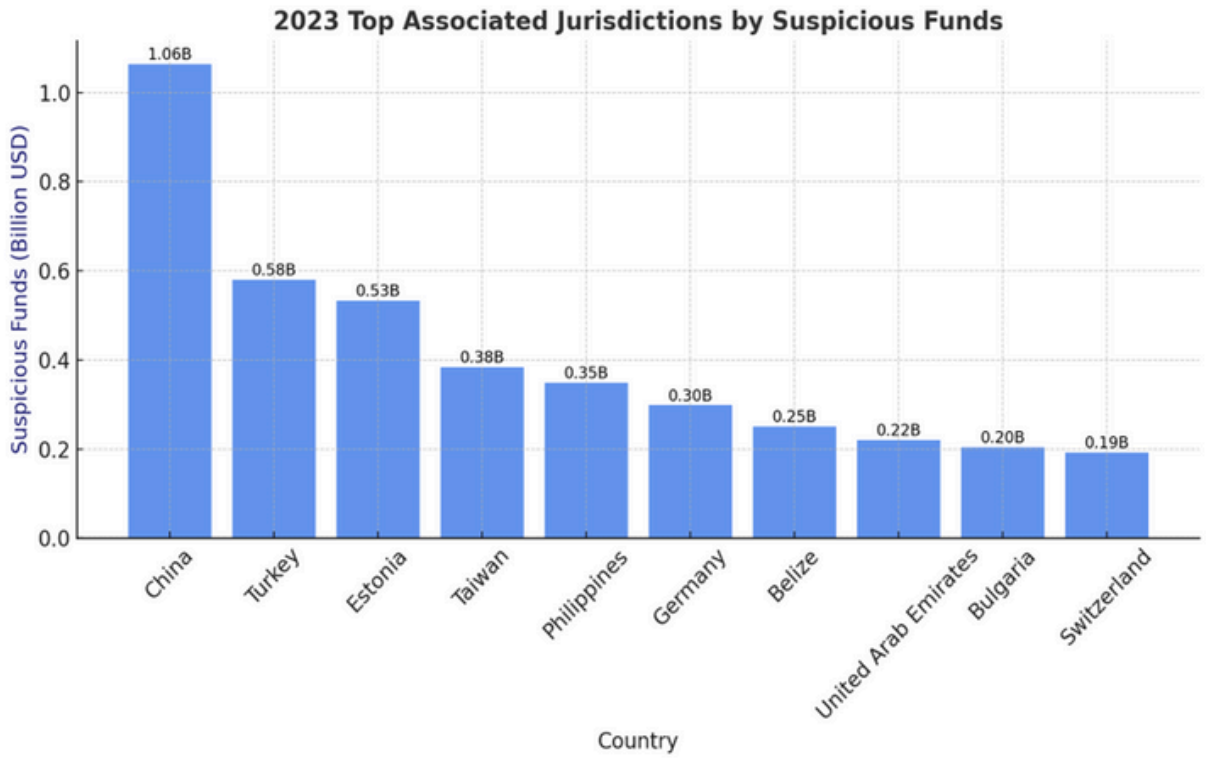
## DIAGRAM.8



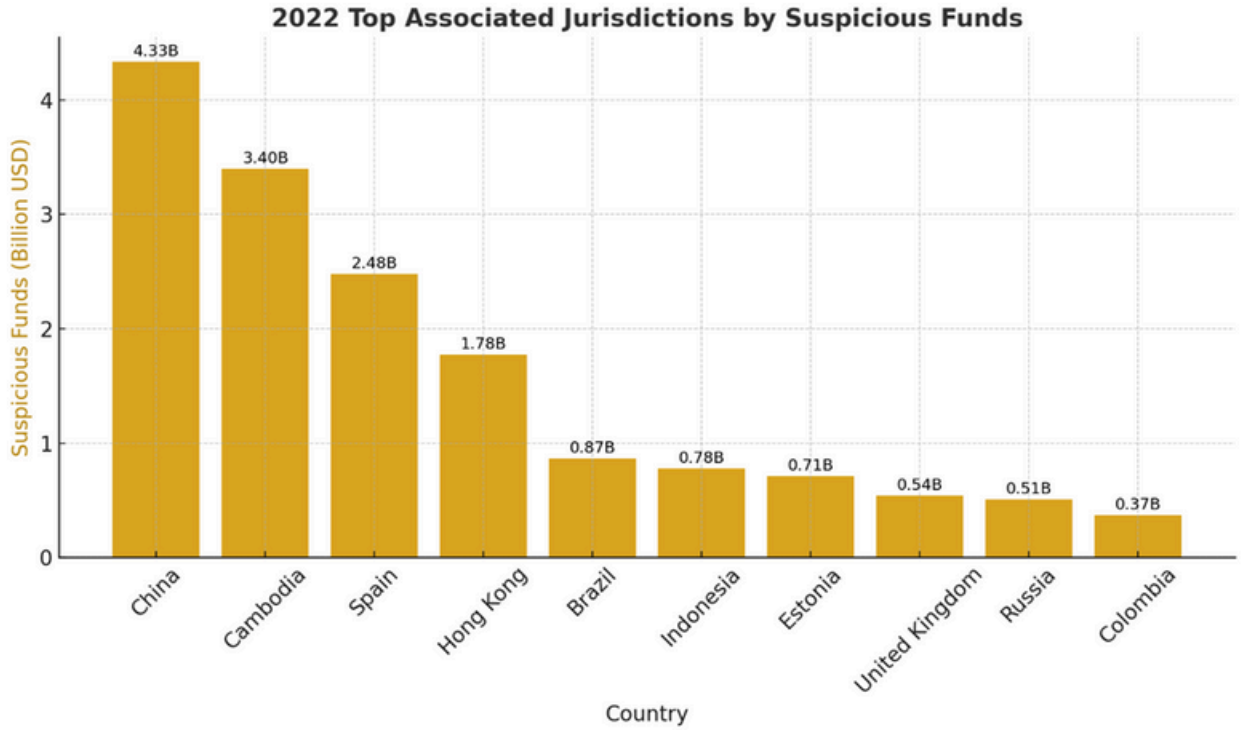

## DIAGRAM.9



## DIAGRAM.10




## DIAGRAM.11



Fluctuations in the top countries over the four-year period are expected. The countries associated with the highest VA SAR values may change from year to year due to the dynamic nature of virtual asset activity and related risks, including shifts in criminal typologies.

- China dominated suspicious activity amounts in 2022, accounting for over USD 4.3 billion in reported transactions. This can be due to a unique case where one of the VA SARs involved over 1 billion in value. However, though this figure declined to USD 1 billion by 2023, reports rebounded to approximately USD 2 billion by mid-2025, indicating that China remains a consistently significant source of suspicious activity within the virtual asset ecosystem.

- European countries appear repeatedly, though at varying levels. Their recurring presence can be attributed to robust banking and payment infrastructures and high levels of retail participation. These factors make such jurisdictions common targets for typologies including investment scams, pig-butchering schemes, and impersonation fraud. As highlighted by Europol, online fraudsters target millions of victims across the EU, with the scale of these crimes continuing to increase, resulting in recurring but generally moderate-value suspicious exposures.[26]

- The United Kingdom dropped from USD 541 million in 2022 to USD 32 million in 2023, before rebounding to USD 392 million in 2024.

- Cambodia, which was previously considered high-risk in 2022, experienced significant declines by 2024, consistent with the implementation of tighter AML/CFT/CPF measures and strengthened supervision following their removal from the FATF Grey List (*Jurisdictions Under Increased Monitoring - June 2022, 2022*).[27]

Since VI Exchanges operate globally, VA SAR values are influenced by a wide range of typologies and the mix of individuals and entities they serve. As a result, fluctuations in suspicious amounts reflect this diverse customer base and risk exposure.

[26] Europol (2023), Online fraud schemes: a web of deceit, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg. Europol chrome-

[27] Jurisdictions under Increased Monitoring - June 2022. (2022, June 17). FATF. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2022.html

## MITIGATING VIRTUAL ASSET RISKS

In May 2022, the Eastern Caribbean Supreme Court (Commercial Court Division) of the Territory of the Virgin Islands issued its first freezing injunction against unidentified individuals in the case Chainswap Limited v Persons Unknown,[28] which involved crypto asset theft.

Chainswap Limited, a VI-incorporated blockchain services provider, was the victim of two sophisticated cyberattacks in July 2021. Hackers exploited vulnerabilities in Chainswap's smart contracts used to facilitate cross-chain token transfers and diverted tokens to private wallets.

The case is an example of the mechanisms that the VI has in place to handle matters involving potential illicit activities conducted within the virtual asset ecosystem and can take action through the legislative regimes and/or the judicial process, as required, which is a necessary component in mitigating virtual asset risks. More specifically, the legal and regulatory framework, and cases highlight:

- A robust framework involving regulatory compliance and legislation involving VA.
- Effective applications of legislation surrounding Virtual Assets involving VI entities.
- Extra jurisdictional reach and international cooperation.
- Capabilities in tracing and freezing illicitly- obtained VA.
- Prevention of financial crime and adherence to AML/CFT/CPF guidelines.

## DETECTION AND MITIGATION

Regulators and financial institutions use advanced tools and collaborative mechanisms to address these risks. Blockchain analytics software helps trace the movement of funds and detect wallets linked to criminal activity. In addition, Know Your Customer and Enhanced Due Diligence requirements help verify user identities and apply additional scrutiny to high-risk individuals and entities. Information sharing between financial intelligence units, law enforcement, and regulators is also critical in detecting and responding to threats quickly. For example, the Beacon Network is a real-time intelligence-sharing platform by TRM Labs that connects law enforcement, crypto exchanges, DeFi services, and stablecoin issuers to combat crypto-related financial crime. Verified investigators can flag wallet addresses linked to illicit activity, triggering immediate alerts and risk-based actions such as freezing assets. By enabling rapid information exchange and collaboration, the Beacon Network helps prevent the movement of illicit funds and strengthen global defence against financial crime.

[28] Claim No. BVIHC (COM) 2022/0031

## FIU AND/OR LAW ENFORCEMENT ROLE IN DETECTION AND MITIGATION

Notably, majority of reported offences involve foreign subjects, however the Agency remains committed to supporting global efforts in combating financial crimes. All information received is thoroughly analysed and, when applicable, disseminated to other relevant jurisdictions and competent authorities. Investigative capabilities utilised by the Agency include Blockchain analytical tools such as Chainalysis and TRM Labs, in addition to OSINT and relevant databases. Information acquired enables the tracing of cryptocurrency transaction movements and the assessment of associated risks - including suspicious transactions and alleged illicit activities.

In high-risks cases involving breach of sanctions or indicators of terrorist financing, findings are disclosed to foreign FIUs.

These measures ensure that the Agency actively contributes to the global fight against **Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF)**. Therefore, in fostering international cooperation and leveraging cutting-edge technology, the Agency plays a vital role in safeguarding the integrity of the global financial system.

A real-world example of this in action is the Colonial Pipeline ransomware attack in May 2021. Hackers demanded payment in Bitcoin after disrupting a major U.S. fuel pipeline. Although they initially received over USD 4 million in payment, law enforcement agencies used blockchain analytics to trace the transactions, identify the hackers' wallets, and recover about USD 2.3 million worth of Bitcoin.[1] This case shows how technology, careful monitoring, financial intelligence and international cooperation can help track and recover illicit funds, even when criminals attempt to hide behind the anonymity of virtual assets.

Addressing the financial integrity risks related to VA requires a solid, multi-pronged approach.

[29] Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to. (2025, February 6). https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

# RECOMMENDATIONS

To mitigate the risks and challenges posed by the virtual assets industry, it is crucial that the VI considers risk mitigation measures that would include domestic, regional and international collaboration, a continued enhancement of legal and regulatory infrastructure and raising awareness through outreach and awareness campaigns.

Some recommendations of risk mitigating measures are highlighted as follows:

1. **Enhance legal and regulatory infrastructure:**

- The VI should continue to enhance its legal and regulatory infrastructure that governs the virtual assets industry to ensure that it is in a strong position to handle issues arising within the virtual asset ecosystem.

- The VI should ensure that its legal and regulatory infrastructure evolves with technological change and market development. Regular reviews, policy updates and engagement with global standard setters will ensure continued relevance and proportionality.

- The VI should continue to harmonise its legal and regulatory infrastructure with the FATF Recommendations and other international benchmarks. Consistent adoption of definitions, licensing requirements and Travel Rule implementation will assist in closing regulatory gaps and enhance supervisory coherence.

2. **Strengthen collaboration between regional and international counterparts:**

- The VI should be proactive in sharing information and intelligence with regional and international counterparts to combat financial crimes. Strengthened intelligence sharing through structured cooperation such as the Egmont Group will improve the jurisdictions' ability to detect and respond to cross-border risks. For example, the exchanging of typologies and key challenges can enhance detection of VA risks and foster collaboration.

- The VI should strengthen partnerships with regional and international counterparts that are engaged in the virtual assets business in an effort to share best practices and learn from other jurisdictions' experiences in handling issues and challenges posed by the virtual asset ecosystem.

3. **Utilisation of the Judicial Process:**

- The VI should use its judicial machinery to assist in mitigating risks and handling issues that arise within the virtual assets industry.

4. **Enhance Public Awareness and Engagement:**

- Public awareness campaigns should be launched on a continuous basis by FSC and the Agency to educate residents, nationals and visitors about virtual assets, the risks and challenges posed by virtual assets, the red flags, trends and typologies they should be aware of and what constitutes quality reports on VA-related matters filed with the Agency.

- Strengthening dialogue with industry participants through initiatives such as a VASP Advisory Committee led by FSC, can improve compliance culture and encourage responsible innovation. Collaboration with private sector analytics firms can also enhance monitoring capabilities.

5. **Enhance Training and Capacity Building for Law Enforcement Agencies:**

- Specialised training should be provided to law enforcement agencies on identifying and handling cases involving virtual assets.

6. **Provide Resources for Technology and Crypto-Analytics:**

- Adequate tools and resources should be provided to facilitate the analysis and investigation of cases involving virtual assets, such as Chainalysis etc., which is crucial in tracing assets on the block chain.

7. **Conduct Regular Inspections:**

- The FSC as the Regulator of VASPs should conduct regular inspections and collect additional data, as necessary, to ensure VASPs are complying with their AML/CFT/CPF obligations.

8. **Conduct Risk Assessments:**

- The VI should on a continuous basis assess the risks and vulnerabilities related to virtual assets to identify emerging trends and implement strategies, as necessary.

9. **Private Stakeholders:**

- Individuals with a stake in virtual asset activity and related products should possess adequate knowledge to identify the risks deriving from the virtual asset ecosystem. Individuals should:
    - understand the jurisdiction's laws involving virtual assets;
    - employ technological mechanisms such as anti-malware software and cybersecurity measures; and
    - safe keep private keys and passwords and other credentials used to access or control virtual assets.

10. **Improve Timeliness of VA SAR filings**

- VASPs should maintain clear internal escalation procedures, and adequately resourced compliance functions to support the timely identification and reporting of suspicious activity. VASPs should seek to file timely VA SARs, i.e. SARs should be filed as soon as is reasonably practicable after it comes to its attention according to section 30A of the Proceeds of Criminal Conduct Act, 1997 (as amended).

- Timely filings improve the quality and usefulness of the VA SAR, enhances law enforcement's opportunities to take action and enables the FIA and law enforcement to identify systemic risks and emerging trends.

# CONCLUSION

In conclusion, as shown, VA pose risks and challenges for the VI. Further, VA will continue to evolve. It is therefore imperative that the VI endeavours to stay ahead of the curb by continuing to strengthen its mechanisms to detect and mitigate the current and emerging virtual asset risks that will inevitably arise from the virtual asset ecosystem.

# REFERENCES


AML/CFT/PF National Coordination Committee. (2023). Money Laundering/Terrorist Financing Risk Assessment Of Virtual Assets And Virtual Asset Service Providers. Financial Intelligence Unit of Guyana. Retrieved October 24, 2025, from https://fiu.gov.gy/wp-content/uploads/2024/01/Risk-Assessment-Virtual-Assets-and-VASPs.pdf

Bitcoin - open source P2P money. (n.d.). Bitcoin.org. https://bitcoin.org/en/bitcoin-paper

Chamber. (2023, March 22). The different types of digital assets. The Digital Chamber. https://digitalchamber.org/the-different-types-of-digital-assets/

Coinbase. (n.d.). Utility tokens vs. security tokens: What are the differences? https://www.coinbase.com/learn/crypto-basics/utility-tokens-vs-security-tokens-what-are-the-differences#What-are-Utility-Tokens

Coinbase. (n.d.-b). What is a governance token? https://www.coinbase.com/learn/crypto-basics/what-is-a-governance-token

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to. (2025, February 6). https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Ethereum (2025, October 23). What is Ethereum? ethereum.org. https://ethereum.org/what-is-ethereum/

Europol (2023), Online fraud schemes: a web of deceit, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

FATF (2025), Best Practices on Travel Rule Supervision, FATF, Paris, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-RuleSupervision.pdf

FATF (2022), Targeted update on implementation of the FATF Standards on virtual assets and virtual asset service providers (VASPs). Paris: FATF/OECD. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

Financial Services Commission & Financial Investigation Agency. (2025). Terrorist Financing Risk Assessment 2025. https://www.bvifsc.vg/sites/default/files/vi_tf_risk_assessment_report_2025.pdf

Jurisdictions under Increased Monitoring - June 2022. (2022, June 17). FATF. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2022.html

# REFERENCES


Kraken Learn Team. (2024, December 2). What is an NFT? Non-fungible tokens explained. https://www.kraken.com/learn/what-are-non-fungible-tokensnft#:~:text=NFTs%2C%20or%20non%2Dfungible%20tokens%2C%20are%20unique%20digital,ownership%20and%20authenticity%20in%20the%20digital%20world.

Litecoin - Open source P2P digital currency. (n.d.). Litecoin. https://litecoin.org/

Monetary Authority of Singapore. (2024). Virtual Assets Risk Assessment Report (30 October 2024). https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/virtual-assets-risk-assessment.pdf

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Office Of Financial Sanctions Implementation. (2025, March 21). OFSI Annual Review 2023 to 2024: Engage, Enhance, Enforce. GOV.UK. https://www.gov.uk/government/publications/ofsi-annual-review-2023-24-engage-enhance-enforce

Ripple. (n.d.). XRP Digital Asset for Global Crypto Utility. https://ripple.com/xrp/

Tether. (n.d.). What is Tether? https://tether.to/en/

The British Virgin Islands Financial Services Commission. (2022). Virgin Islands Virtual Assets Service Providers Act, 2022. In bvifsc.vg. https://www.bvifsc.vg/sites/default/files/virtual_assets_service_providers_act_2022.pdf

The British Virgin Islands Financial Services Commission. (2023). Virtual Assets Service Providers Guide to the prevention of money laundering, terrorist financing and proliferation financing. In bvifsc.vg. https://www.bvifsc.vg/sites/default/files/vasp_aml_cft_guidance.pdf

The BVI Financial Services Commission & Financial Investigation Agency. (2022). Money Laundering Risk Assessment Report - 2022. In bvifsc.vg. Financial Services Commission. https://www.bvifsc.vg/sites/default/files/virgin_islands_2022_ml_risk_assessmentam.pdf

The Virtual Assets and Virtual Assets Service Providers Bill, 2025. (2025). In Parliament of the Republic of Trinidad and Tobago. Retrieved December 2, 2025, from https://www.ttparliament.org/wp-content/uploads/2025/11/hs20251126u.pdf

Two defendants charged in NFT Fraud and Money Laundering Scheme. (2022, March 24). U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0

# REFERENCES

U.S Department of Treasury. (2023). 2023 De-Risking Strategy. Retrieved November 14, 2025, from https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf

Virgin Islands. (1997). Proceeds of Criminal Conduct Act, No. 5 of 1997 (Revised Edition 2020). Retrieved from https://www.bvifsc.vg/sites/default/files/proceeds_of_criminal_conduct_act.pdf

Virtual Currencies Key Definitions and Potential AML/CFT Risks. (2014). In Financial Action Task Force. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

What is Monero (XMR)? (n.d.). getmonero.org, the Monero Project. https://www.getmonero.org/get-started/what-is-monero/

What is Solana? | Solana. (n.d.). Solana. https://solana.com/learn/what-is-solana

# APPENDIX

## ADDITIONAL INFORMATION ON A GLOBAL PERSPECTIVE ON VIRTUAL ASSETS

This section highlights challenges, trends and typologies for other jurisdictions within the global landscape of virtual assets adoption.

## TRINIDAD AND TOBAGO

Trinidad and Tobago has imposed a temporary prohibition on all virtual-asset activities until December 2027. According to official statements from the Parliament of the Republic of Trinidad and Tobago, the moratorium aims to provide authorities with sufficient time to establish a comprehensive regulatory and supervisory framework for Virtual Assets, while safeguarding the country's standing in the upcoming CFATF 5th Round Mutual Evaluation and the scheduled on-site visit in March 2026.

A key focus of this initiative is the proper implementation of FATF Recommendation 15, which addresses the regulation and supervision of VASPs. With the 5th Round Mutual Evaluation imminent, the government recognises that rushing implementation risks technical and operational deficiencies that could undermine compliance with all 40 FATF Recommendations.

As failure to demonstrate effective adherence could increase the risk of Trinidad and Tobago being grey-listed, which would have significant reputational and economic consequences. The moratorium therefore seeks to ensure that regulatory measures are robust and fully aligned with international standards.

The suspension enables the government to conduct a full national risk assessment while creating the space to establish clear regulatory requirements, strengthen institutional capacity, and implement robust consumer-protection measures. Collectively, these efforts are intended to mitigate money-laundering and terrorist-financing risks before allowing market expansion.[30]

[30]The Virtual Assets and Virtual Assets Service Providers Bill, 2025. (2025). In Parliament of the Republic of Trinidad and Tobago. Retrieved December 2, 2025, from https://www.ttparliament.org/wp-content/uploads/2025/11/hs20251126u.pdf

## AUSTRALIA

Australia treats digital currency as a regulated sector under AUSTRAC's AML/CTF framework. Digital currency exchanges are required to register and comply with reporting obligations. AUSTRAC has issued specific Indicators of Suspicious Activity for the Digital Currency Sector, integrating virtual asset risks into its National Risk Assessment (2024). The assessment highlights digital currency exchanges and related activities as increasing vulnerabilities for money laundering and terrorist financing.

## KEY CHALLENGES AND TRENDS

*Exploitation of Money Mules*

Criminals increasingly exploit money mules, particularly international students and migrants, to move or convert illicit virtual asset funds. These individuals are often unaware their accounts are being used to facilitate money laundering.

*Misuse of Crypto ATMs*

Crypto ATMs are being used as cash on/off ramps, commonly linked to scam proceeds and layering. Offenders deposit cash and convert it into crypto to obscure fund origins before transferring it abroad.

*Expansion of Fintech and Digital Payments*

The growing fintech and digital payments sector introduces new actors—such as payment facilitators or app-based intermediaries—who may lack mature AML controls. This expansion increases exposure to VA-related risks and regulatory blind spots.

*Oversight Gaps in Secondary Service Providers*

There remain gaps in oversight for secondary service providers such as wallet custodians, aggregators, and infrastructure firms. Coordination between AUSTRAC, Treasury, and other agencies is still evolving to ensure a unified supervisory approach.

## TYPOLOGIES AND RED FLAG INDICATORS

- Frequent inbound transfers from multiple addresses, followed by rapid outbound transfers to a single wallet.
- Transactions inconsistent with the customer's known profile or without clear source of funds.
- Use of foreign-based VASPs in jurisdictions with weak AML/CFT regulation.
- Large or repeated cash-to-crypto conversions through ATMs.
- Activity involving intermediaries, mixers, or layered wallets to obscure origins.
- Common IP addresses or shared infrastructure between unrelated wallet holders.[31]

## UNITED KINGDOM

The UK's 2025 National Risk Assessment (NRA) provides a comprehensive assessment of money laundering and terrorist financing risks across all financial sectors, including cryptoassets and VASPs. It introduces a dedicated typologies chapter and sectoral risk breakdowns, underscoring the enhanced understanding of crypto-related threats.

The assessment elevates the risk rating for fintech, Electronic Money Institutions (EMIs), Payment Service Providers (PSPs), and cryptoasset firms, reflecting the government's increased focus on convergence risks and regulatory scrutiny in digital finance.

## KEY CHALLENGES AND TRENDS

*Convergence of Sectors*

The UK is witnessing a growing integration between EMIs, PSPs, and cryptoasset providers, creating a "crypto-EMI nexus." This convergence blurs traditional sector boundaries and introduces complex new risk pathways.

*Unregistered or Underground Operators*

Authorities continue to identify unregistered money service businesses (MSBs) and unregulated crypto platforms operating outside the supervisory perimeter. These channels enable illicit fund transfers beyond AML oversight.

[31]Australian Government. (2024). Money laundering in Australia National Risk Assessment 2024. In Austrac.gov.au. Retrieved October 14, 2025, from https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf

*Rising Use of Stablecoins*

*The use of stablecoins such as Tether (USDT) in laundering and illicit flows has grown rapidly, surpassing Bitcoin in identified risk exposure. Stablecoins' liquidity and price stability make them preferred tools for layering activities.*

*Outsourced AML/CFT Compliance*

*An emerging issue is the outsourcing of AML compliance to third-party service providers who may lack crypto-specific expertise. This creates vulnerabilities in customer due diligence, transaction monitoring, and ongoing risk assessment.*

*Financial Crime and Sanctions Nexus*

*The UK's financial crime landscape increasingly intersects with sanctions evasion, kleptocracy, and geopolitical risk, especially following the Russia–Ukraine conflict. Crypto assets have been highlighted as potential tools for circumventing restrictions.*[32]

[32]UK HM Treasury. (2025). National Risk Assessment of Money Laundering and Terrorist Financing 2025. www.gov.uk. Retrieved October 15, 2025, from https://assets.publishing.service.gov.uk/media/6877be59760bf6cedaf5bd4f/National_Risk_Assessment_of_Money_Laundering_and_Terrorist_Financing_2025_FINAL.pdf


Financial Investigation Agency