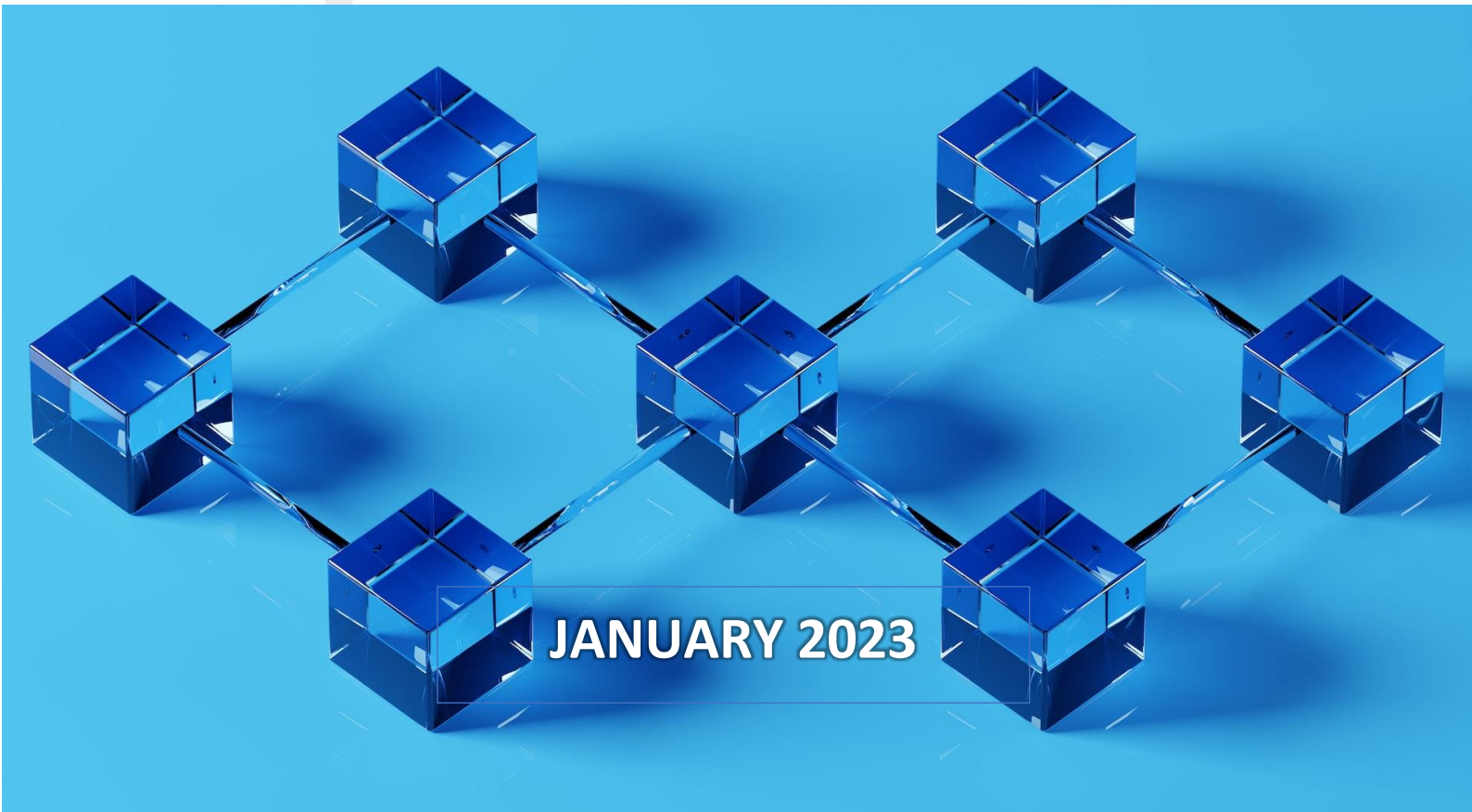
# Money Laundering & Terrorism Financing Risks Through the use of Virtual Assets

# and

# Virtual Asset Service Providers

## IMPLICATIONS IN THE CARIBBEAN REGION



The Caribbean Financial Action Task Force (CFATF) is an organisation of states and territories of the Caribbean basin which have agreed to implement common countermeasures against money laundering and terrorism financing.

For more information on the work of the CFATF, visit www.cfatf-gafic.org



Photo by Shubham's Web3 on Unsplash

# Table of Contents

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AML** | Anti-Money Laundering |
| **CDD** | Customer Due Diligence |
| **CFATF** | Caribbean Financial Action Task Force |
| **CFT** | Counter-Financing of Terrorism |
| **CRTMG** | CFATF Risk, Trends and Methods Group |
| **DAB Act** | Digital Asset Business Act |
| **DARE ACT** | Digital Assets and Registered Exchanges Act |
| **FATF** | Financial Action Task Force |
| **FinTECH** | Financial Technology |
| **FIs** | Financial Institutions |
| **FIU** | Financial Intelligence Unit |
| **INR** | Interpretative Note to Recommendation |
| **LEAs** | Law Enforcement Agencies |
| **ML** | Money Laundering |
| **MLAT** | Mutual Legal Assistance Treaty |
| **MOU** | Memorandum of Understanding |
| **PF** | Proliferation Financing |
| **R.** | FATF Recommendation |
| **SA** | Supervisory Authority |
| **SAR** | Suspicious Activity Report |
| **SOF** | Source of Funds |
| **SWIFT** | The Society of Worldwide Interbank Financial Telecommunication |
| **TF** | Terrorist Financing |
| **VASPs** | Virtual Asset Service Providers |
| **VAs** | Virtual Assets |

# GLOSSARY

| | |
|---|---|
| **DECENTRALIZED AND CENTRALIZED EXCHANGES** | Decentralized exchanges are platforms which allow peer-to-peer transactions without going through an intermediary while Centralized exchanges are platforms that act as intermediaries between buyers and sellers of VAs. |
| **MARKET MAKERS**[1] | The term market maker refers to a firm or individual who actively quotes two-sided markets in a particular security, providing bids and offers (known as asks) along with the market size of each. Market makers provide liquidity and depth to markets and profit from the difference in the bid-ask spread. They may also make trades for their own accounts, which are known as principal trades. |
| **P2P TRANSACTIONS**[2] | VA transfers conducted without the use or involvement of a VASP or other obliged entity (e.g., VA transfers between two (2) unhosted wallets whose users are acting on their own behalf) |
| **PSEUDONYMITY**[3] | Means that a name, term or descriptor that is different to an individual's actual name is being used. |
| **TRACEABILITY**[4] | The ability to track something as it moves through a process. |
| **TRANSFER SPEED**[5] | A measure of data that is transferred from one location to another in a given amount of time. Data transfer speeds are measured in bits per second (b) or bytes per second (B). |

[1]https://www.investopedia.com/terms/m/marketmaker.asp#:~:text=The%20term%20market%20maker%20refers,in%20the%20bid%2Dask%20spread.
[2] https://docs.oracle.com/cd/E92727_01/webhelp/Content/obdx/retail/p2paymnt/p2pintro.htm
[3] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity#:~:text=Anonymity%20means%20that%20an%20individual,to%20an%20individual's%20actual%20name
[4] https://www.perforce.com/blog/alm/what-traceability
[5] https://www.2brightsparks.com/resources/articles/file-sizes-and-transfer-speeds.html#:~:text=Data%20transfer%20speed%20is%20a,bytes%20per%20second%20(B).

# EXECUTIVE SUMMARY

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

2. Members of the CFATF, with the guidance of the CRTMG, therefore embarked upon a study of how VAs function, integrate and contribute to the financial sector in the Caribbean region.

3. A survey was sent to 24 CFATF members to collect data on the usage of VAs and VASPs within the Caribbean region, the applicability of the Travel Rule, the Regulatory Landscape which entails AML/CFT and Prudential Frameworks, Law Enforcement Authorities' experience in investigating/prosecuting matters relating to VAs & VASPs and their ability to provide international co-operation and the inherent ML/TF/PF risks. The Project Team received responses from 15[6] CFATF member jurisdictions and was able to identify information gaps, types of risks affecting the Caribbean and the extent of these risks.

4. Analysis revealed there is still a lack of knowledge about the extent of VA and VASP activity in the region, with 20% of responding CFATF member jurisdictions stating that the extent of usage was not known and just over a third indicating that the purpose was not known (which could include investment purposes or payment purposes). Only a small proportion (6.7%) indicated that they had identified moderate usage, with no jurisdiction indicating that usage was frequent. This suggests that further work may be done by CFATF member jurisdictions to gather information on VA usage and VASPs. Indeed, most responding CFATF members indicated that they have not yet conducted a ML/TF/PF risk assessment of the VASP sector in their jurisdiction (53.8%).

5. By far the most common type of VASP activity identified by responding CFATF member jurisdictions appears to be VA trading platforms and exchanges, followed by custodian services and issuances. Higher risk activities such as decentralized exchanges and over the counter ("OTC") broker services are also identified in the region.

6. Just over half of the responding CFATF member jurisdictions have implemented legislation to regulate VASPs and/or have commenced the registration of VASPs. Of these, all have the power to issue financial penalties for non-registration/licensing. However, none have taken any penalties or sanctions to date. Furthermore, less than half of the responding CFATF member jurisdictions have the power to issue criminal sanctions to VASPs.

7. Responding CFATF member jurisdiction have indicated that their existing mechanisms such as MOUs and MLATs do not prohibit, and have been utilised to facilitate, the sharing of information on matters involving VAs and VASPs domestically and internationally. Law enforcement authorities have been using the existing communication channels and technology, established for reporting when there is suspicion related to funds that are the proceeds of criminal activity or TF, to facilitate the filing of suspicious transaction reports related to VAs and VASPs.

8. The majority of respondents lacked the expertise and capabilities to investigate cases in relation to VAs and VASPs in their jurisdiction. However, there have been investigations originating from FIUs on VA-related offences during the reported period, 2019 – 2021.

9. Resultantly, it was recommended that jurisdictions should take the necessary steps to enact suitable legislation in line with FATF recommendations and guidelines and improve their data gathering regarding the usage of VAs and VASPs. CFATF member jurisdictions should also consider

[6] Anguilla, Antigua and Barbuda, Bermuda, Cayman Islands, Curaçao, Dominica, Grenada, Guyana, Jamaica, Montserrat, Saint Lucia, The Bahamas, Trinidad & Tobago, Turks and Caicos Islands, and Venezuela.

seeking technical assistance in conducting a National Risk Assessment of their VASP sector and training their SA staff in how to effectively supervise the VASP sector.

# INTRODUCTION

## Background

10. CFATF members are required to identify ML/TF/PF risks arising from the misuse of VAs and the threats they pose to the Caribbean region. As these threats evolve, so too must the strategies to mitigate these risks. For this to be accomplished, these risks must be identified and understood so that measures can be implemented to prevent the misuse of VAs and their implications[7].

11. Where VAs and VASPs are not prohibited, CFATF members are obligated to implement measures aimed at regulating VAs and VASPs based on the FATF Recommendations. For jurisdictions that choose not to fully implement R.15 and R.16 with respect to VASPs and VAs, legislation should be in place to prohibit the use and operation of VAs and VASPs, respectively. R.15 and R.16 describe how countries and obliged entities must comply with the FATF Recommendations to prevent the misuse of VAs for money laundering and terrorist financing and the financing of proliferation.

12. CFATF members initiated the VAs and VASPs Research Project to gain insight into the status of its 24 member jurisdictions and their implementation of measures to prevent the misuse of VAs and VASPs. The intent is to foster an understanding of the degree of VA/VASP adoption within each member's jurisdiction and to establish a sound regulatory framework for VASPs. It is understood that there will be members with more developed and sophisticated VA markets and VASP regulatory regimes than others.

13. The Project Team, supported by the CFATF Secretariat, conducted a survey of members to gather the data in this report. Just over half of the members participated in this survey[8], and therefore this report does not depict a comprehensive view of VAs and VASPs in the Caribbean, but rather a snapshot/current view of the degree of VA/VASP adoption within each member's jurisdiction and to establish a sound regulatory framework for VASPs. albeit narrower view, based on the data received. There remains a significant knowledge gap among CFATF member jurisdictions in understanding the level and usage of VAs and VASPs within the region. This poses additional challenges in conducting national risk assessments, ensuring effective supervision of the VASP sector and conducting ML/TF/PF-related investigations with a nexus to VASPs and VAs.

## Project Team

14. This project was formalized in November 2021 by the CFATF, and its Project Team is comprised of members from regulatory agencies located in the following jurisdictions:

- The Bahamas, Project Co-lead (Gawaine Ward, Senior Manager, Enforcement, Securities Commission of the Bahamas; Vivienne Dean, Manager Enforcement, Securities Commission of the Bahamas).
- Trinidad & Tobago, Project Co-lead (Debbieann Sealey, Analyst, FIUTT; John Cozier, Financial Research Officer, TTSEC; Terri Timothy, Analyst, FIUTT; Salisha Ali, Financial Research Officer, TTSEC).
- Antigua and Barbuda (Sheryl Walker-Gore, Financial Compliance Examiner, ONDCP-FCU).
- The Cayman Islands (Sarah Wheeler, Head of Division, AML/CFT Division, CIMA; Shana Donovan, Chief Risk & Policy Officer, AML/CFT Division, CIMA; and Shastri Singh, Senior Analyst AML/CFT Division, CIMA)
- Dominica (Patrick George, Senior Financial Investigator/Analyst; FIU – Dominica)

[7] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

[8] Participating Members: Anguilla, Antigua and Barbuda, Bermuda, Cayman Islands, Curaçao, Dominica, Grenada, Guyana, Jamaica, Montserrat, Saint Lucia, The Bahamas, Trinidad & Tobago, Turks and Caicos Islands and Venezuela.

- Montserrat (Donilia Cuffy, Deputy Commissioner, Financial Services Commission)
- Suriname (Xanagay Huur, Economist, Central Bank of Suriname)
- Jamaica (Paulette Burnett-Gilfillian, AML Chief Compliance Officer, Financial Services Commission)

15. Significant support was provided to the team by the Co-Chairs of the CRTMG Mrs. Berdie Dixon-Daley and Mrs. Mary Martinez-Campbell and by members of the CFATF Secretariat Mr. Kerry Lucio and Mr. Jefferson Clarke and former members of the project, Ms. Dana Munnings-Gray and Ms. Shakeira Dunkley.

## Purpose of the Project

16. The purpose of this project is to produce a coherent and comprehensive report on existing laws and practices within the Caribbean region regarding VAs and VASPs and their attendant risks, particularly in the context of the FATF's R.15. Further, the report may assist jurisdictions contemplating a framework for VAs and VASPs, by providing relevant considerations for the implementation of same.

17. As indicated previously, CFATF members are faced with the need to identify and assess ML/TF/PF risks arising from VAs activities and VASPs operations, and the threats they pose to their individual jurisdictions within the Caribbean region. As a result, this project seeks to identify and recommend national strategies to manage and mitigate these risks.

18. CFATF members are obligated to implement measures for the regulation of VASPs based on the FATF Recommendations. R.15 and R.16 describe how countries and obliged entities must prevent the misuse of VAs and VASPs for money laundering and terrorist financing and the financing of proliferation. Consequentially, CFATF members have developed a research project reflecting the current state of play regarding VAs popularity and usage, members understanding of the fledgling industry and considerations for developing or integrating VASPs into existing regulatory frameworks.

## Project Objectives

19. This project has the following objectives:

a. **GENERAL OBJECTIVE**

- To examine how VAs function, integrate and contribute to the financial sector in the Caribbean region.
- To have an understanding of how the inherent risks are mitigated by the financial and corporate sector when providing virtual asset services.

b. **SPECIFIC OBJECTIVES**

- To identify the ML/TF/PF risks posed by VAs and VASPs in the Caribbean.
- To identify the extent to which VASPs are licensed, regulated or prohibited in the region and the nature of implementation.
- To identify methods and best practices of CFATF members to mitigate risks relative to virtual assets and VASPs in the financial and corporate system in the Caribbean region.
- To guide the allocation of institutional resources with the purpose of achieving greater efficiency in mitigating ML/TF/PF risks posed by VAs and VASPs.

## Methodology

20. The methodology engaged for this project was survey-based. A questionnaire was developed to gather secondary information, both quantitative and qualitative, from authorities within the region's AML/CFT framework. Member jurisdictions of the CFATF were requested to nominate one point of contact within their country to co-ordinate the collection of data, which was collated and then used to complete an online questionnaire. The CFATF Secretariat distributed six (6) thematic fillable Microsoft

Word versions of the questionnaire electronically to the 24 CFATF members. Data was collected for a three-year period (from 2019 to 2021).

21. Further to this, the Project Team conducted open-source research and reviewed several documents and reports, from the FATF and other international organizations. Additionally, some of the Project Team members participated in an Experts Meeting hosted by the CFATF Secretariat on VAs and VASPs.

22. The questionnaire sought to gather general and specific information in relation to the following areas:

- Usage of VAs and VASPs in the region
- The Regulatory Landscape
- Prudential frameworks
- AML/CFT frameworks
- Travel Rule
- Intelligence, reporting requirements and international co-operation
- Inherent ML/TF Risks:
  i. Type of risks
  ii. Extent of risks
  iii. Trends of risk

## Scope and Limitations of the Report

23. This research focused mainly on the usage of VAs and VASPs, AML/CFT frameworks, prudential frameworks, the Travel Rule, intelligence and information sharing and law enforcement engagements and inherent risks among CFATF member jurisdictions. Thus, this report should be considered and interpreted in the context of the survey limitations.

24. In conducting the project, the Project Team experienced many challenges in relation to timeliness and completeness of data collection and the timeliness of submissions. Of the 24 member jurisdictions poled, 15[9] jurisdictions (63%) responded to the questionnaire. However, not all 15 respondents answered all the questions. Wherever possible this report identifies the number of responses to the specific question being asked.

25. Several countries are currently developing their VASP supervision regime and do not yet have the data to contribute to this project. Of the 15 member jurisdictions that responded, seven (7) do not have legislation.

26. Further to this, there was a lack of both sectoral and entity level risk assessments which may have hindered the understanding of the inherent risks in the Caribbean region. When consideration is given to the fact that most respondents indicated that VAs and VASPs were mainly used in the retail sectors (non-institutional investors), then exposure to the financial sector is somewhat muted. As for the corporate sector, that information may only be available through the receipt of direct information from them or through any outreach activities conducted by the VAs/VASPs supervisors which are limited in the Caribbean region at present.

27. Some questionnaires were received beyond the requested deadline and methods used to collect the data, resulted in delays in the project timelines. Establishing a secure and common mechanism where documents can be shared among the Project Team also was challenging. There were also some technical difficulties with some jurisdictions which impeded the information received and the analysis of the information during the data collection.

[9] Anguilla, Antigua and Barbuda, Bermuda, Cayman Islands, Curaçao, Dominica, Grenada, Guyana, Jamaica, Montserrat, Saint Lucia, The Bahamas, Trinidad & Tobago, Turks and Caicos Islands and Venezuela.

# FATF STANDARDS AND EXPECTATIONS

## Virtual Assets – Definitions; Regulated and Unregulated activities

28. The FATF uses the term "virtual asset" to refer to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value. The FATF emphasises that virtual assets are distinct from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the money of a country that is designated as its legal tender. Fiat currency has no intrinsic or fixed value and is not backed by any tangible asset.

29. VAs have many potential benefits. They can make payments easier, faster, and cheaper; and provide alternative methods for those without access to regular financial products. However, without proper regulation, they create new opportunities for criminals and terrorists to perpetrate predicate offences[10], launder their proceeds or finance their illicit activities. Even though regulating VASPs is challenging, national authorities need to develop skills to understand the technology involved, while the VASPs have to learn about and abide by the regulatory rules that now apply to their sector. In October 2018, the FATF updated its Standards to extend AML/CFT requirements to VAs and VASPs. In June 2019, the FATF adopted an INR.15 to clarify how the FATF requirements apply in relation to VAs and VASPs. The FATF recommends all countries to apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF/PF risks are commensurate with the risks identified in their respective jurisdictions.

30. Among the CFATF member jurisdictions, The Bahamas, Bermuda and the Cayman Islands were the first countries to regulate VASPs. Bermuda passed the DAB Act in 2018, and created one of the first FinTech-specific regulatory regimes. The Cayman Islands, with its Virtual Asset Service Providers Act, and The Bahamas with its DARE Act, followed later on. The Bahamas, Bermuda and the Cayman Islands have each built a legal and regulatory architecture to bring balance between encouraging innovators, while demonstrating soundness, safety, and the protection of customers' interests and the VAs ecosystem.

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

- Exercise due care, skill and diligence.
- Establish and maintain effective security systems.
- Establish and maintain effective corporate governance and robust resilience of their systems.
- Have appropriate systems, policies, processes and procedures for the prevention, detection and disclosure of financial crime and to ensure compliance with AML/CFT laws.
- Establish and maintain adequate and effective systems for the protection and segregation of customer assets and data.

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

33. The next phase of regulation will require VASPs to obtain and hold originator and beneficial ownership information on all transfers of virtual assets under Part XA of the Anti-Money Laundering (Amendment) Regulations of the Cayman Islands. The "Travel Rule", took effect on July 1, 2022 and its successful implementation was critical to investor confidence and security. It demonstrated the

[10] E.g. Fraud related to a VASP, receive ransomware payments, etc

Cayman Islands' ability to effectively supervise VAs and those who provide certain services in relation to them.

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

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

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

37. The DAB regime, overseen by the Bermuda Monetary Authority, caters to Digital Asset Businesses at differing stages of development, offering the F (Full) license; the M (Modified) license, for those planning to expand operations for a limited period; and the T (Test) license for those seeking to test their proof of concept. Mindful of deterring bad actors and reducing reputational risk to the country, Bermuda incorporates prudential rules into its regime, with requirements including cybersecurity audits and customer due diligence. Regulators in all three (3) jurisdictions run efficient registration and licensing regimes. When delays occur, they are often a result of incomplete applications. Compliance is a new challenge for many in a hitherto unregulated sector.

## VASPs – Definitions

38. The FATF defines VASPs within its Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (updated October 2021) as follows:

> *Any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.*

39. In furtherance of the questionnaires sent to participating member jurisdictions of the CFATF, member jurisdictions were asked whether their respective countries apply the FATF definition to define VASPs and or VAs or whether an alternate definition was used.

40. The majority of member jurisdictions who responded indicated that they utilise the FATF definition within their respective legislative framework. However, only one (1) respondent indicated that they did not utilise the FATF definition, and they did not provide an alternate definition that was considered.

## Transparency and the "Travel Rule"

41. In June 2019, the FATF released clarification to its guidance to member nations regarding the regulation of VASPs and other crypto entities. In response to the money laundering and terrorist financing risks posed by the virtual assets sector, the updated guidance included a 'Travel Rule'. This rule requires VASPs to share sender (originator) and receiver (beneficiary) information for

cryptocurrency transactions above USD/EUR 1000[11] globally and is a key AML/CFT measure, which mandates that VASPs obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers (as per paragraph 7 of FATF's Interpretative Note to 15). This is similar to so-called Travel Rules that have for years required financial institutions to share this information when executing bank wire transfers and SWIFT electronic funds transfers.

42. The FATF guidelines require both sending and receiving VASPs to exchange and store originator and beneficiary identification information in addition to the cryptocurrency addresses and transaction identifications for each transaction. Regulators require the latter, since cryptocurrency addresses can be used by multiple beneficiary customers. For example, some exchanges use a single address to send all transactions. Also, cryptocurrency addresses can be recycled and consequently may be used by multiple customers at a VASP.

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

*a) The name of the originator;*

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

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

*d) the name of the beneficiary;*

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

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

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

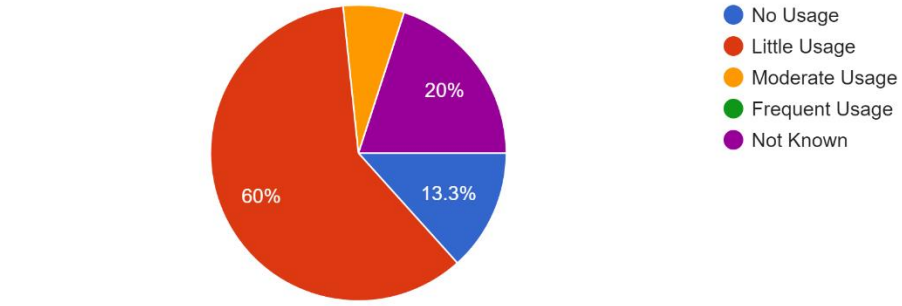
# VAs & VASPs WITHIN THE REGION

## Usage in the region

### VAs: Extent of usage

44. There appears to be relatively limited usage of VAs among CFATF members. Of the 15 respondents to the survey, a small proportion (6.7%) indicated that there was moderate usage of VAs in their jurisdictions. 13.3% of CFATF respondent jurisdictions reported no usage of VAs in their jurisdiction, and 60% indicated little usage of VAs. A further 20% of responding CFATF member jurisdictions stated that the volume of usage was not known. This suggests a significant knowledge gap around the popularity and utility of VAs among CFATF members.

Diagram 1 below illustrates the extent of VAs usage in the region




45. Ten (10) CFATF members were able to provide a reasonable estimate of how many residents own or have dealt in VAs. Of the ten (10), 70% assessed that only 6% of residents own or have dealt in VAs, 20% assessed this value at 2% and finally, 10% indicated that just 1% of residents have engaged in this type of activity. This indicates that even where VAs are utilised, there are only a small proportion of users relative to population size.

### VAs: Types of usage

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

### VAs: Profile of users

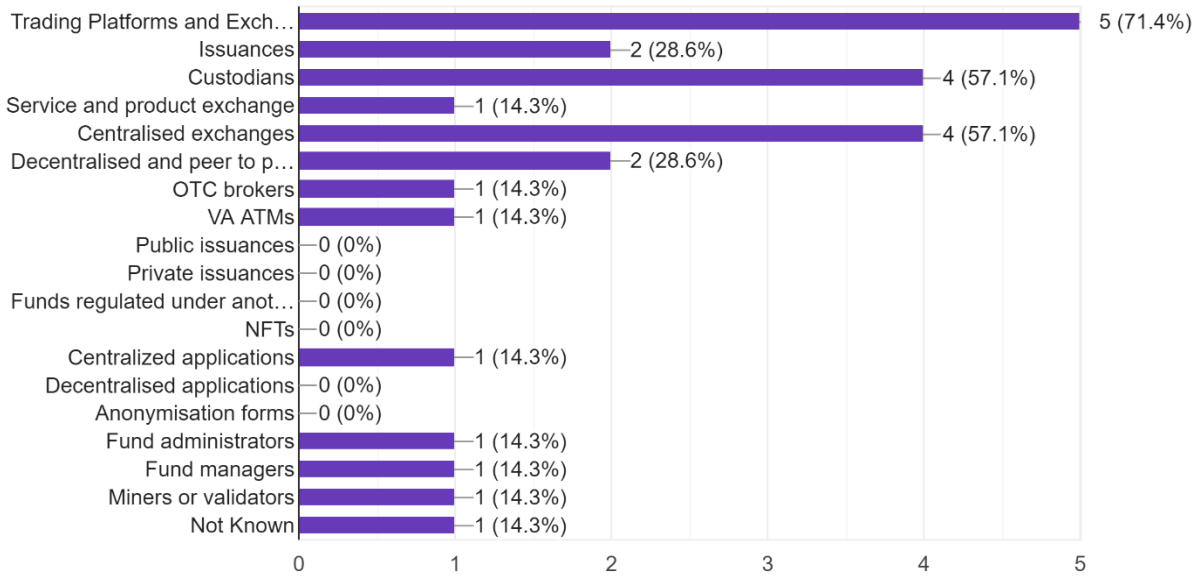
47. Of the 14 responses to the question on what the primary uses of VA were, it was discerned VAs are mostly used by individual non-institutional customers and investors (53.3%). No corporate entities or companies were identified as using VAs and only 21.4% of responding jurisdictions said that VAs are mostly used by institutional investors. The current usage of VAs is therefore different to traditional fiat financial products and services with a greater emphasis on individual and retail (e.g. non-institutional) customers.

### VASPs: Nature, size and complexity

48. Of 15 CFATF members that responded, 93.3% indicated that they applied the FATF definitions to define VASPs. From the information provided by seven (7) responding CFATF members, VASP entities take various forms, including stand-alone VASPs, commercial banks, offshore banks, trust and

company service providers and administrators. There are also state actors such as the Crypto Asset Treasury of Venezuela. From information provided by seven (7) CFATF members that responded, the main activities undertaken by VASPs in the CFATF region are set out below.

Diagram 2 illustrates the main activities undertaken by VASPs in the region.




49. By far the most common type of activity appears to be VA trading platforms and exchanges, with 71.4% of VASPs providing this service. This can be further broken down between centralized exchanges (57.1%), decentralized and peer-to-peer exchanges (28.6%), service and product exchange (14.3%) and over the counter ("OTC") brokers (14.3%). There are also a significant number of custodians (57.1%) and issuances (28.6%).

# THE REGULATORY LANDSCAPE

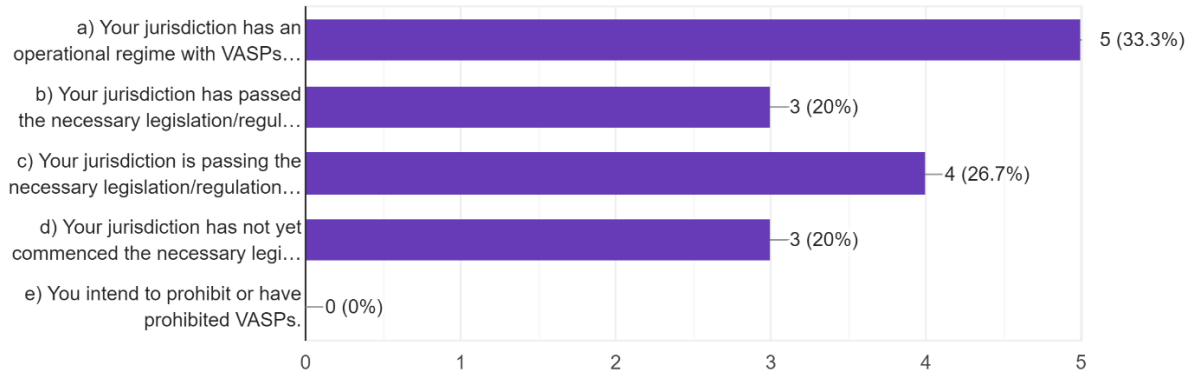
## Extent of regulation by CFATF members

50. From the information provided by 15 CFATF members, the extent of regulation differs: Anguilla, The Bahamas, Bermuda, Cayman Islands and Venezuela have an operational regime with VASPs licensed/registered, while others, such as Antigua and Barbuda, Dominica and Grenada have passed the necessary legislation/regulation but VASPs are not yet licensed/registered. The remaining CFATF members that responded have either not commenced the necessary legislative/regulatory process or are in the early stages of passing the relevant laws. Based on the 15 responses received, no jurisdictions have declared their intent to prohibit VASPs.

51. Of the five (5) jurisdictions without the necessary legislation who responded, 20% stated that this would be in place by September 2022, 20% by December 2022, 20% by April 2023 and the remaining 40% of countries indicated that legislation will be implemented by the end of 2023. This shows that the regulation of VASPs is a key area of focus in the region, even for those jurisdictions without legislation in place.

52. The stages of implementation are captured below, with a minority of the 15 respondents (20%) indicating that they had not yet commenced the necessary legislative changes to incorporate VASPs into the regulatory regime. 11 of the 15 countries responding to the survey (73%) countries) have taken steps to regulate/license VASPs with seven (7) of these already having passed legislation.

Diagram 3 illustrates the different extent of regulation of VAs and VASPs within the region

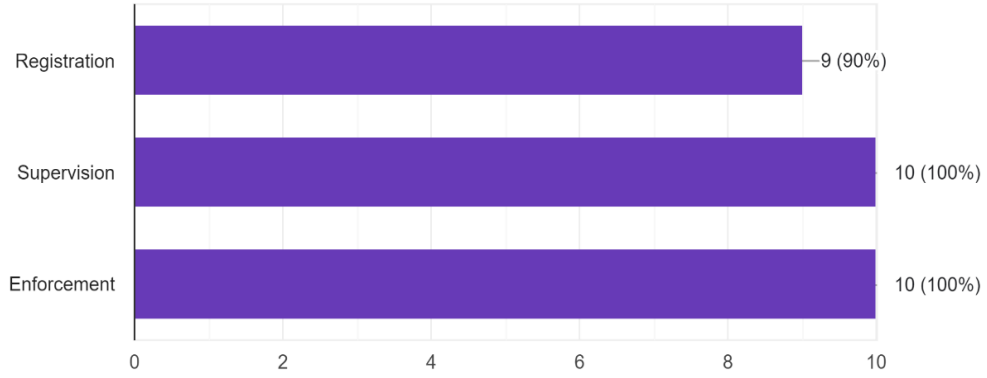



## The role of the Supervisory Authority (SA)

53. Of 15 responses provided by CFATF members, 53.3% indicated that VASPs need to be registered or licensed with a SA and that financial penalties can be applied to VASPs who conduct VA activities without being licensed or registered. SAs include Monetary Authorities, Financial Commissions, a Securities Commission, Central Banks, AML Units and a National Superintendency. Additionally, in one (1) instance, supervision was split between a prudential authority and an AML authority. One (1) jurisdiction had created a new SA. A further two (2) jurisdictions did not yet have a designated SA.

54. Of ten (10) respondents, 100% stated that the role of the SA was for supervision and enforcement. Nine (9) of the ten (10) respondents (90%) indicated that the SA was also responsible for registration.

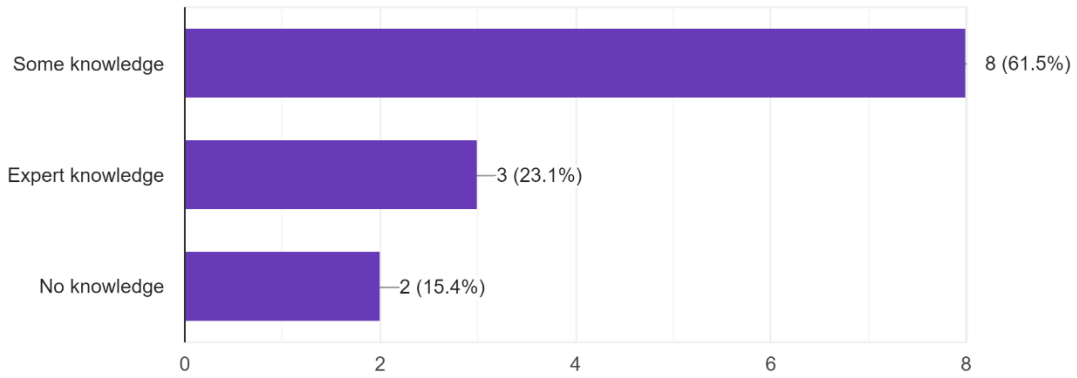
Diagram 4 illustrates the role of the SAs for VASP regulation




## Expertise of the SA

55. Responses from 13 CFATF member jurisdictions indicated that three (3) SAs had expert knowledge of VASPs, eight (8) had some knowledge of VASPs, and two (2) had no knowledge. Of the 13 responses, 84.6% said that they had provided SAs with training and 15.4% said they had not.

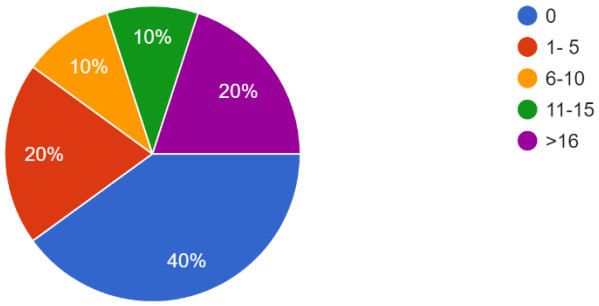
Diagram 5 illustrates the varying degrees of knowledge of SAs regarding VASPs




## Number of registered VASPs

56. Of ten (10) respondents, 40% indicated that they have not yet registered any VASPs. Conversely, 20% of respondents indicated that they had registered over 16 VASPs.

Diagram 6 illustrates the number of registered VASPs by responding CFATF member jurisdictions




## Procedures for registering and/or licensing VASPs

57. Eight (8) of the 11 responding jurisdictions provided a brief description on their registration and/or licensing procedure, six (6) of which are currently in force. The other two (2) jurisdictions have a process in place, but the legislation has not yet been enacted and is not in force. Generally, the process includes, inter alia.

- A submission of an application along with a prescribed fee.
- KYC procedures.
- Written policies, rules, and procedures specific to their VA and VASP operations.
- Risk assessments of the products and services, and
- Fit and proper criteria.

## Physical presence requirements and VASPs outside of the jurisdiction

58. Of the 11 jurisdictions that responded, 72.7% require VASPs to have a physical presence in the jurisdiction in which they operate. Three (3) of the ten (10) responding jurisdictions allowed natural persons to offer VA services as a business and they are required to be licensed/registered to do so. Of the nine (9) jurisdictions that responded, 100% confirmed that their domestic legislation does not prohibit nationals from using VASPs services operating outside of the jurisdiction. Indeed, 25% of

respondents indicated a regulatory regime that only covered persons within the jurisdiction. This may present a risk of regulatory arbitrage by VASPs seeking to evade regulation.

59. Of the nine (9) CFATF members that require VAs and VASPs to be registered and/or licensed with the relevant SA, where the VASP is a legal person:

- Eight (8) of the nine (9) respondents required the VASPs to be incorporated in the jurisdiction.
- Six (6) of the nine (9) jurisdictions allowed VASPs that were incorporated elsewhere but are offering their services in the jurisdiction of registration and/or licensing; and
- One (1) of the nine (9) jurisdictions did not require incorporation in the jurisdiction or elsewhere.

60. All eight (8) CFATF member jurisdictions that responded and that have legislation in place, indicated that it is a criminal offence for VASPs to conduct VA activities without being licensed and/or registered and financial penalties can be applied for this offence.

# Prudential Frameworks

## Prudential regulatory powers

61. Of the ten (10) CFATF members that responded, 80% confirmed that VASPs are subject to risk based prudential supervision. All ten (10) respondents have adequate powers to conduct inspections, compel the production of information/documents and to impose sanctions (financial, criminal or any other) including the power to withdraw, restrict or suspend the VASPs license/registration.

## Trading Platforms, Issuances and Exchange Services

62. Eight (8) out of the nine (9) jurisdictions that responded to the questionnaire stated that VAs have established criteria for the trading of VAs. Of ten (10) CFATF members that responded, five (5) indicated that there is a requirement for supervisory approval for a VA to be traded. Of nine (9) CFATF members that responded, seven (7) indicated that there are reporting obligations imposed on the operator of the trading platform. Furthermore, all nine (9) jurisdictions that responded stated that they have no restrictions on the type of investors that are allowed to participate (e.g., professional investors only).

63. Of seven (7) responses, 57% indicated that VASPs are allowed to conduct "off chain" transactions and of seven (7) responses, three (3) jurisdictions responded that VASPs customers are allowed to use mixers and tumblers. This presents a significant delivery channel risk and increases the ability of bad actors to obfuscate the originator of any transaction.

64. Three (3) jurisdictions set out the criteria for the trading of VAs as follows:

- As part of the application process, the VASPs must include a prospectus for the sale of the asset,
- The prospectus must be approved by the Unit for the license to be granted, and
- The duties are listed in the relevant legislation.

65. Additionally, of the nine (9) CFATF member jurisdictions that responded, 55.6% confirmed that there are requirements for the operator of the trading platform to disclose certain information pertaining to risks to investors. All nine (9) CFATF member jurisdictions that responded to the questionnaire stated that there were no entry barriers to the number and persons that are allowed to offer trading platforms. This allows for any qualified entrepreneur seeking to enter the VA marketspace to own and operate a VASP trading platform within these jurisdictions, subject to the relevant registration/licensing and fitness and proprietary tests.

66. Of the eight (8) CFATF member jurisdictions that responded to the questionnaire, 25% of jurisdictions' trading platforms facilitates the inclusion of Market Makers and there are no restrictions on the persons/entities that are allowed to be Market Makers. From the eight (8) responses, Market Makers are subjected to licensing/registration regimes in 50% of jurisdictions.

## Custody Arrangements

67. Of the eight (8) responses that already established a regulatory regime, the wait time before an e-wallet is granted/approved by a regulator can be within 1-3 months as provided by three (3) jurisdictions, while one (1) jurisdiction stated that it can be over three (3) months. In four (4) jurisdictions, this was not applicable.

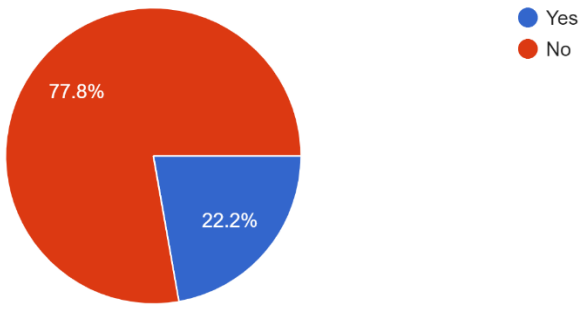
68. The requirements for the custody of clients' assets (VAs and funds) were described by seven (7) jurisdictions as follows:

- There are provisions for assets to be held by a trust (two (2) jurisdictions),
- There is a percentage of assets to be stored in cold wallets (one (1) jurisdiction),
- Funds to be held are segregated accounts (six (6) jurisdictions), and
- There is insurance coverage (four (4) jurisdictions).

## Sandbox Regimes

69. Of ten (10) CFATF members that responded, eight (8) indicated that they developed a sandbox as part of their regulatory framework. Only one (1) jurisdiction indicated that it had any 'players' in its sandbox at present, and this was limited to one entity. The sandbox experience is therefore at nascent stages across the region.

Diagram 7 illustrates the proportion of responding CFATF jurisdictions that have developed a sandbox




## Sanctions

70. Of the eight (8) responses for the year 2019, the six (6) responses for the year 2020 and the five (5) responses for the year 2021, no fines or other enforcement actions have yet been taken against VASPs. However, of ten (10) member jurisdictions that responded, nine (9) of the respondents indicated that their SA has adequate powers to:

- Impose sanctions (financial, criminal or any other)
- Restrict or suspend the VASPs license and registration

71. Furthermore, approximately 60% of the ten (10) jurisdictions that responded have legislative provisions for the detection and prevention of market manipulation and abuse. Furthermore, 40% have legislative provisions for conflict of interest ("COI") as follows:

- The power to impose the requirements for identification and management of conflicts of interest for entities licensed as trading platforms.

- Requirements for COI and codes that are enforceable.
- Directors, Shareholders and Senior Officers are subject to fit and proper tests.
- The licensees must have approved policies and procedures on COI including identification of material COI between the interest of the licensed undertaking and the credit disclosure to the clients of any such material COI.

72. Of the ten (10) CFATF members that responded, nine (9) jurisdictions indicated that sanctions are applicable to the institution, directors, and senior management.

# AML/CFT FRAMEWORKS

## Powers of the SA

73. Of 11 CFATF members that responded, 100% stated that the SA has adequate powers to:

- Supervise and Monitor VASPs to ensure compliance with AML/CFT legislation.
- Conduct inspections.
- Compel the production of information /documents
- Impose sanctions (Financial, Criminal or any other)

74. However, of ten (10) CFATF members that responded, only 90% confirmed that VASPs are subject to risk-based AML/CFT supervision. An explanation for this anomaly may be that the SA in that particular jurisdiction has yet to commence risk-based supervision.

## Reporting Obligations of VASPs

75. Of ten (10) respondents, 75% stated that reporting obligations are imposed on VASPs. These include:

- KYC and CDD information.
- Data on the number and value of accounts held.
- Transactions data.
- Financial Statements.
- Counter of Terrorism Property Reports.
- AML/CFT Risk assessments, and
- Independent AML/CFT Risk assessments.

## CDD Onboarding Procedures

76. Of the 11 CFATF members that responded, 100% stated that their legislation prohibits VASPs from allowing users to access their platforms without providing KYC information.

77. Responses from ten (10) CFATF member jurisdictions suggest that the majority (80%) require/accept a government ID or passport; 70% require/accept a drivers' license; 30% require/accept a voters' ID or social security card and only 10% require/accept a proof of address or company ID. Of 11 respondents 54.5% confirmed that this information must be verified and certified. Of ten (10) respondents, 60% confirmed that they had assurance and authentication frameworks and standards for identity in place.

## Source of Funds Requirements

78. Information provided from eight (8) respondents indicated that there are a range of SOF requirements:

- One jurisdiction indicated that VASPs are required to obtain relevant information that will allow them to identify and verify the SOF of all customers but, this will vary based on context
- One jurisdiction indicated that a SOF declaration is required for more than USD $10,000

- One jurisdiction asked for information to identify the accounts from which funds are transferred or source account, funds used to open e-wallets or to conduct business and information on the identification of the source account.
- One jurisdiction indicated that AML/CFT regulations and laws were being amended to include VASPs.

### Monitoring and Screening Requirements for VASP Customers

79. Of the ten (10) CFATF members that responded, only 40% confirmed that transaction monitoring was conducted by VASPs to inform reporting and sanctions screening compliance. A further 50% of the ten (10) jurisdictions confirmed there was a threshold for occasional transactions, prompting CDD to be conducted.

80. Of the respondents, only five (5) countries provided information on the monitoring processes which entailed the implementation of VASPs own internal controls, AML framework requirements and VASPs are required to file Terrorism Property Reports. One country stated that VASPs were monitored through manual checks, but their SA was taking steps to enable VASPs to implement IT systems or technology tools that will facilitate ongoing monitoring.

### Supervisory Authority Technology Tools

81. Of 11 CFATF members that responded, six (6) confirmed that they have access to technology tools such as blockchain analytics. Of 11 responses, four (4) jurisdictions deploy special software to conduct AML/CFT onsite inspections, but only two (2) jurisdictions utilise block chain analytics to tests the adequacy of VASP compliance. This suggests that technology has yet to be implemented for regulatory compliance monitoring and surveillance. Jurisdictions use a range of providers, including Chainalysis, Cyphertrace, Elliptic, TRM Labs and Coinfirm. One jurisdiction, Venezuela, has developed its own blockchain analytical tool.

### Training, Guidance and Outreach

82. Of nine (9) CFTAF members that responded, only 33.3% said that training had been provided by the relevant SA on identifying and mitigating ML/TF/PF risk faced by the VASP Sector. From the information provided in eight (8) responses, jurisdictions have issued a combination of guidance notes, sector specific guidelines, regulations and notices to the VASP sector, however one jurisdiction had not issued any of these to their VASP sector. From six (6) responses, 83.3% of jurisdictions have not provided any guidance or training to VASPs on Travel Rule compliance.

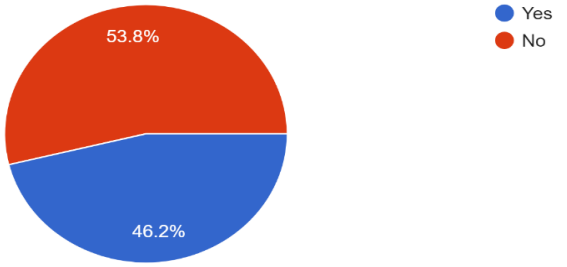
83. Of the ten (10) CFATF members that responded, the majority (80%) indicated that VASPs are required to receive training on AML/CFT. To a lesser extent, VASPs were required to receive training on risk assessment (50%), cybersecurity (40%) and information technology (20%).

## TRAVEL RULE

### Implementation of Travel Rule legislation

84. Of 13 responses, six (6) jurisdictions, 46%, indicated that they have enacted legislation mandating VASPs to comply with the Travel Rule, whilst the majority have not. With only seven (7) respondents who could potentially answer further questions about the Travel Rule, the data sample may be too small to be instructive of general trends. Nevertheless, the results may still be informative to member jurisdictions who are in the process of implementing Travel Rule legislation.

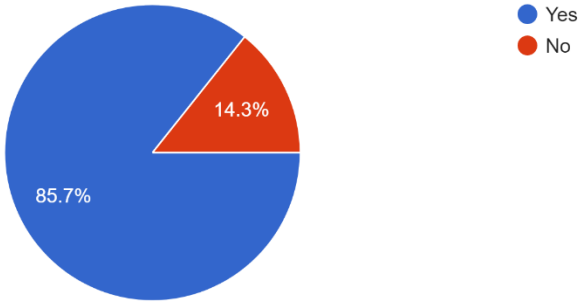
Diagram 8 illustrates the number of jurisdictions that have enacted legislation for the Travel Rule.




## Authority for assessing compliance with the Travel Rule

85. Of the seven (7) CFATF members that responded, 85.7% confirmed that they used the same SA to assess compliance with the Travel Rule and to regulate VASPs for AML/CFT. However, there was one jurisdiction that indicated that it has separate authorities to monitor this information.

Diagram 9 illustrates the number of jurisdictions that use the same competent authority for regulation of VASPs and assessing compliance with the Travel Rule.




## CDD measures when conducting VA transfers

86. Of the seven (7) jurisdictions that have enacted Travel Rule legislation, six (6) require VASPs to undertake CDD measures and exchange Travel Rule information when conducting VA transfers, in accordance with FATF R.16.

- Two (2) jurisdictions require the exchange of travel rule information ***for all*** transactions, regardless of the threshold. Three respondents require it only for transactions equal to or above USD/EUR 1,000, in accordance with FATF R.16.
- Of seven (7) respondents, 85.7% require all transfers of USD/EUR 1,000 or more to be accompanied by the originating customer's verified/certified name, account number, physical address, national ID number or date/place of birth.
- Similarly, of seven (7) respondents, 85.7% require the VASP to retain the beneficiary customer's name and account number. Of six (6) respondents, 83.3% indicated that recipient VASPs are required to retain the same information as the originator.
- Finally, of seven (7) respondents, 71.4% prohibit VASPs from executing VA transfers where they do not comply with the requirements of R.16.

## Monitoring compliance with the Travel Rule

87. Of six (6) CFATF members that responded, 83.3% confirmed that they assess the procedures used by VASPs to implement the Travel Rule. From the information provided by five (5) further responses, there are a range of approaches to monitoring compliance:

- More than half (60%) of respondents indicated that they used audits/assessments to verify that VASPs have implemented the Travel Rule. One (1) jurisdiction noted that 'findings [show] varying degrees of implementation'. Another jurisdiction replied that, as the Travel Rule had only been implemented in 2021, it was not yet included in the audits/inspections conducted by the SA. One (1) jurisdiction confirmed that it had not yet commenced its regulatory supervision of VASPs.
- One (1) respondent indicated that Travel Rule reporting is primarily undertaken via third party service providers, with some VASPs communicating information directly to their counterparty VASP. Another jurisdiction indicated that compliance by VASPs with the Travel Rule is monitored solely through the onsite inspection process. A further respondent indicated that Travel Rule reporting is done quarterly by the VASP to the SA, who analyses and monitors the data accordingly.
- None of the respondents indicated that there were any significant challenges and/or obstacles to assessing VASP compliance with the Travel Rule, given the nascent stage of monitoring and supervision. However, one (1) jurisdiction commented that this would be verified during their upcoming cycle of onsite inspections in the latter half of 2022.

# INTELLIGENCE, REPORTING REQUIREMENTS AND INTERNATIONAL CO-OPERATION

## Reporting requirements

88. For the period 2019 to 2021, a total of 34 SARs with a nexus to VAs and VASPs were filed with FIUs in the respective responding member jurisdictions. In the year 2019, only one (1) SAR was filed.

89. In 2020, jurisdictions had not received any SARs. In 2021, one (1) jurisdiction indicated that their FIU received 33 SARs and the FIU of the remaining jurisdictions received zero (0).

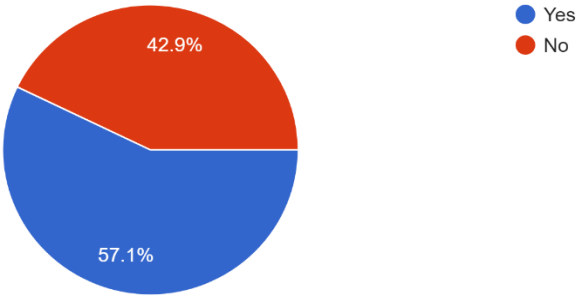
Table 1 illustrates the submission of SARs over the three-year period (2019-2021)

| YEAR | No. of SARs Submitted to FIU |
|---|---|
| 2019 | 1 |
| 2020 | 0 |
| 2021 | 34 |

90. Out of the 15 responding CFATF member jurisdictions, nine (9) jurisdictions stated that monitoring transactions were done on an ongoing basis which met their requirements of reporting unusual or suspicious transactions. It was also stated that they had implemented sanction screening procedures for VASPs relative to terrorism financing.

## International Co-operation, MOUs and Information Sharing for VAs/VASPs in the Region

Diagram 10 illustrates MOUs and Information Sharing for VAs and VASPs in the Caribbean region.

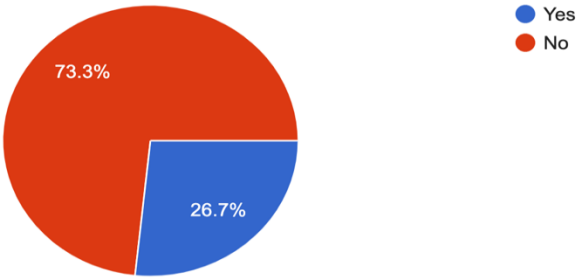



91. A majority of the jurisdictions (57.1%) stated they had existing MOUs covering the sharing of information while 42.9% stated they did not. Jurisdictions with existing MOUs indicted that the MOUs for ML/TF/ PF matters also extend to the VA & VASP sector. Others stated that they were still in the process of passing legislation and others have now signed MOUs to facilitate information exchange relative to VASPs.

### Capacity of Law Enforcement

92. Information provided by the 15 CFATF member jurisdictions indicated that 73.3% lacked the expertise and the capabilities to investigate ML/TF/PF cases with a nexus to VAs and VASPs in their jurisdiction. Only 26.7% indicated that they possess the expertise and capabilities.

Diagram 11 illustrates the expertise and capacity to investigate ML/TF/PF cases.



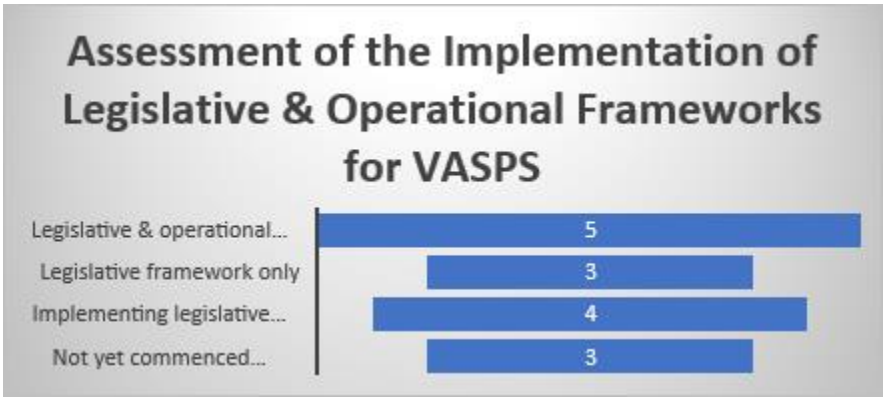

## INHERENT ML/TF/PF VULNERABILITIES

93. The inherent ML/TF/PF vulnerabilities that are associated with VAs and VASPs tend to reflect the general vulnerabilities of the AML/CFT ecosystem that have been established regionally, nationally and by the obliged entities themselves.

94. For the responding CFATF member jurisdictions, 13% have indicated that VAs are not used in their jurisdictions and only 53% of respondents have indicated that there exists legislation for the AML/CFT regulation and supervision of VASPs.

95. Of these jurisdictions, only five (5) representing approximately 33% have implemented an operational framework for the AML/CFT regulation and supervision of VASPs. Of note, another four (4) jurisdictions are currently in the process of implementing the legislative framework for the regulation of VASPs. Whilst a further three (3) jurisdictions have not yet commenced any process for the promulgation of the requisite legislation as demonstrated in diagram 12 below:

Diagram 12 illustrates the assessment of the implementation of legislative and operational frameworks for VASPs.




96. With so many countries in the region without any AML/CFT regulatory framework for VASPs, this effectively inhibits the effects of measures to mitigate the associated risks. In any assessment of ML/TF/PF vulnerabilities, consideration must be given to the fact that many VA activities occur outside of any regulated sphere, irrespective of whether a jurisdiction has established a regulatory framework.

## Types of Risks

97. Only seven (7) countries in the region have reported that a ML/TF/PF risk assessment on the VASP sector has been conducted to date. Based on the limited data available, there are obvious constraints in the identification of all of the key ML/TF risks. Data garnered from the very few responding countries indicates there is a medium-high to high ML risk as it relates to the VASP sector and medium-low to low TF risk. This however can be considered limited, as the majority of the CFATF members have yet to conduct a risk assessment on the VASP sector.

Diagram 13 illustrates jurisdictions ML risk rating from VASP Risk Assessment

Diagram 14 illustrates jurisdictions TF risk rating from VASP Risk Assessment


## Extent of the Risks

98. Akin to often high-risk sectors such as money service providers, payment providers and bureaus de exchange, VASPs face similar challenges in ensuring that their businesses are not exploited for ML/TF/PF purposes.

### The Nature of VAs & VASPs

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

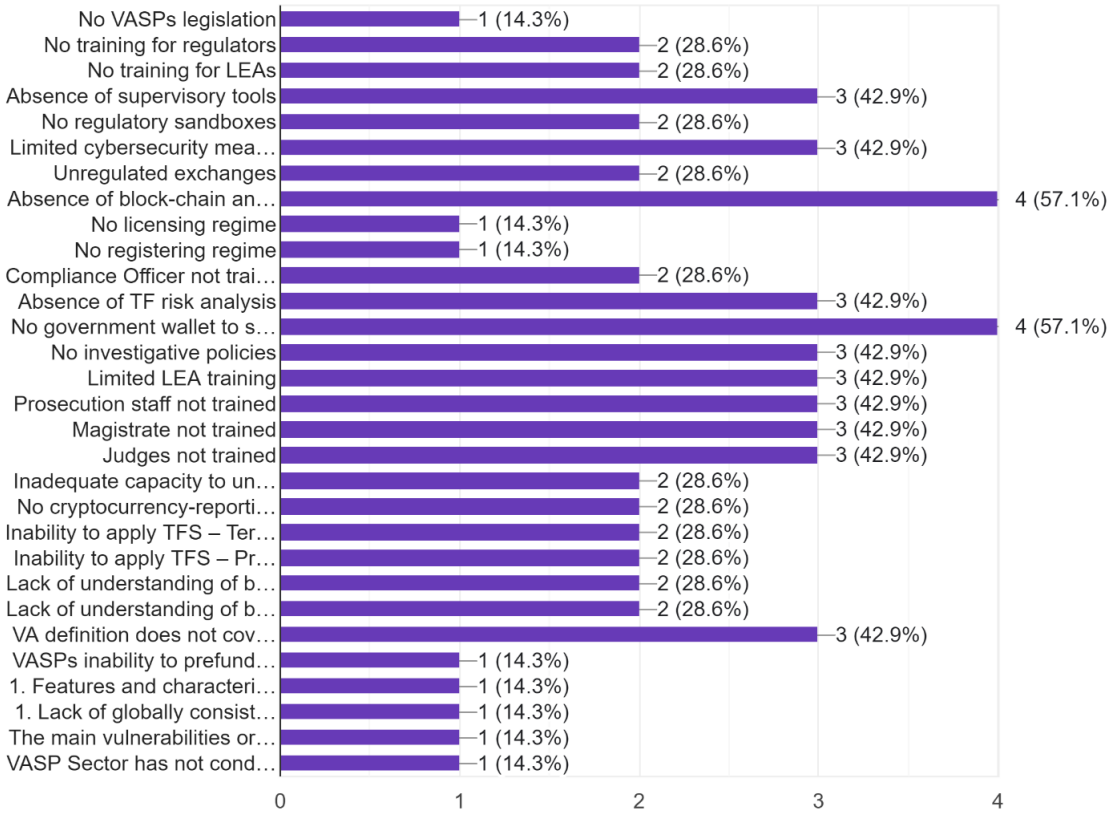
- Anonymity/pseudonymity;
- Traceability;
- Transfer speed;
- P2P transactions;
- Decentralized or centralized exchanges; and
- Convertible/non-convertible.

100. A lack of centralized control within certain services and structures may increase the risk of anonymity as there is no intermediary oversight. Of seven (7) responses, two (2) jurisdictions have indicated that decentralized exchanges and P2P transactions are allowed. Although all responding jurisdictions reported that anonymity or pseudonymity VAs are prohibited, four (4) CFATF Members indicated that their legislation permitted transactions to be conducted "off chain" and four (4) responded that their legislation permitted customers to use mixers and tumblers. This presents a significant delivery channel risk and increases the ability of bad actors to obfuscate the originator of any transaction.

### Lack of specialist resource and appropriate technological tools

101. Of seven (7) jurisdictions, the following risks, as seen in Diagram 15, were identified by the VASP sector in their jurisdiction. These include but are not limited to the "absence of block-chain analysis tools at FIs/DNFBPs", "no government wallet to seize cryptocurrencies", "absence of supervisory tools", and "limited cybersecurity measures", "absence of TF risk analysis", and "no investigative policies". This suggests that lack of specialist resource and appropriate technological tools is perceived as a key risk.

Diagram 15 illustrates the ML/TF risks identified by the VASP Sector in CFATF member jurisdictions.




## New Payment System

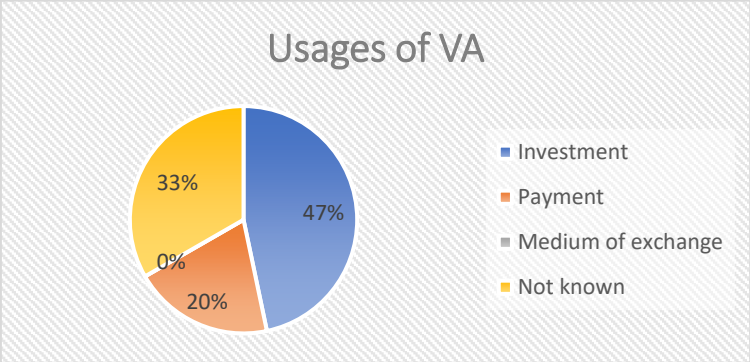
102. Traditional financial institutions normally facilitate the conversion of fiat currency into virtual currency through payment methods such as:

- Wire transfers;
- Other transfers to third party payment providers;
- Cash transactions; and
- Credit/debit card payments.

103. Increasingly, there are VASPs offering services to provide a bridge between a customer desirous of using cryptocurrency to make a payment, and a merchant who prefers to receive payment in fiat currency. This VA service is referred to as a cryptocurrency payment gateway. It enables the merchant to accept virtual currency, but receives fiat currency immediately in exchange.

104. Correspondingly, VAs are also used to make payments directly to those merchants/vendors who have no reservations in accepting these payments. However, based on the survey results, VAs are still being used predominantly for investment purposes in the region. This is depicted in the Diagram 16 below:

Diagram 16 illustrates the usages of VAs.




## Cross Border Transactions

105. Cross border VA transactions are found to be vulnerable to ML/TF/PF risks, with the consideration of the following factors:

- Correspondent country risk;
- Traceability of funds; and
- Degree of international cooperation.

106. Of nine (9) responses, six (6) jurisdictions have reported that VASPs licensed/registered in their jurisdictions are allowed to provide services to customers outside of their jurisdiction.

107. The AML/CFT controls in the sending or receiving country for any VA transaction, will impact that country's own risks. The transaction speed and global reach of VAs, along with weak regulation or supervision in a correspondent country, can result in VA activities posing a significant risk to the legitimate financial sector.

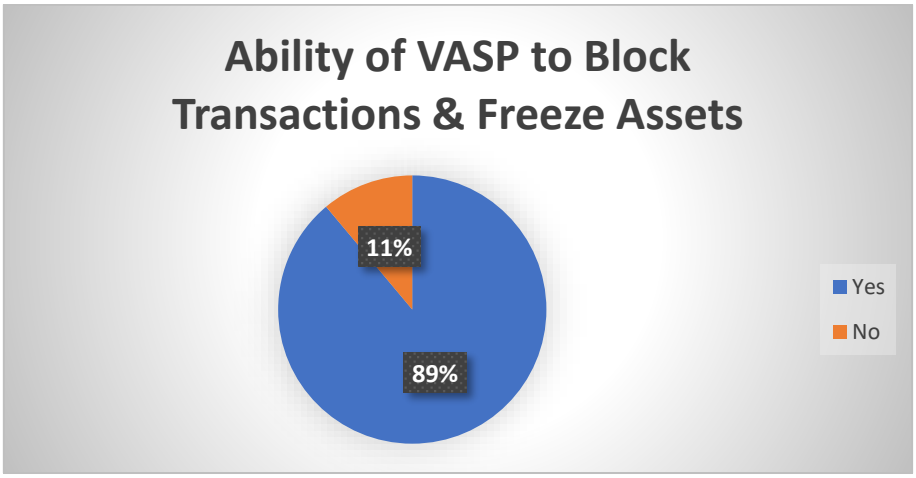
## Accessibility for Criminal Activities

108. Accessibility to criminals is another risk factor to be taken into consideration with respect to:

- Dark web access;
- Anonymity/pseudonymity;
- Disguising the source of funds;
- Traceability of funds; and
- Seizing of funds.

109. With 89% of respondents (nine (9) responses) indicating that a licensed/registered VASP has the ability to block transactions and freeze assets, there is significant mitigation of the risks associated with the retention by criminals of illicit VAs. See Diagram 17 below:

Diagram 17 illustrates the ability of VASPs to block transactions and freeze assets.




110. Similarly, 91% of respondents (eleven (11) responses) have indicated that there are legislative safeguards to prevent transactions from being conducted anonymously. Additionally, 89% of respondents (nine (9) responses) have reported that there are legislative measures preventing transactions from being conducted pseudonymously.

111. It can therefore be concluded that of the fifteen (15) respondents, the legislative framework for VASPs has been constructed to ensure compliance with prescribed CDD measures relating to anonymity.

### Operation of Foreign Unregistered VASPs

112. The operation of foreign unregistered VASPs in local jurisdictions gives rise to the following risks:

- Underground unregulated market;
- Tax evasion; and
- Funding of illicit activities.

113. Significantly, all respondents (nine (9) responses) to the question of whether domestic legislation prohibits nationals from utilizing VA services operating from outside their jurisdiction have stated that this is not the case. Domestically, there is no obligation to require the registration or licensing of these foreign VASPs.

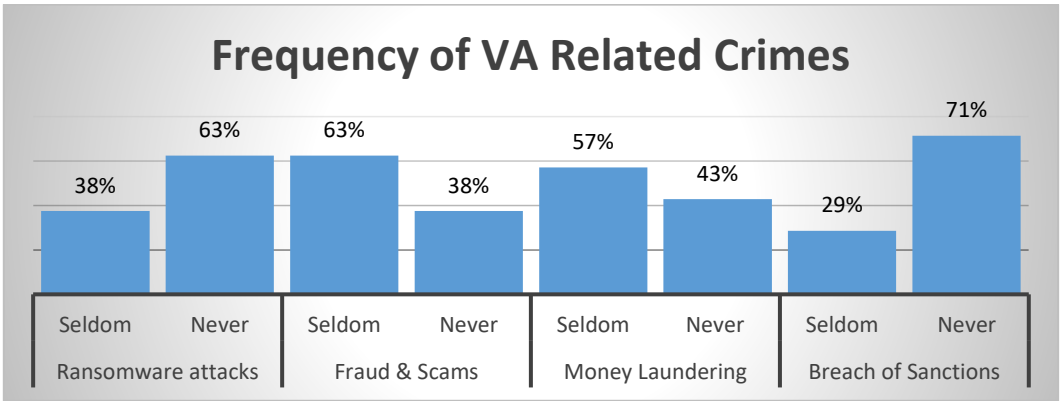
114. A higher level of risk is associated with a resident using the services of a VASP located in a country that is not regulated. With many unregulated VA platforms not having a physical presence in the country of operation, it is extremely difficult for law enforcement to investigate illicit activities and take actions to freeze or seize assets. Since the VASP sector is not yet regulated in many countries in the region, VASPs can legitimately offer their services to persons in foreign jurisdictions and are at risk to abuse for ML/TF/PF and can be utilized as vehicles to perpetrate such crimes..

## Trend of Risks

115. Global illicit cryptocurrency activities continue to grow at a rapid rate, with the predominant predicate offence being fraud. This reflects the regional situation for CFATF members where fraudulent activities (including Ponzi or pyramid schemes) seem to be featured more frequently in the reported misuse of VAs. Other illicit activities linked to VAs include money laundering and tax offences. Although CFATF member jurisdictions have been experiencing these activities there have been 23 investigations originating from SARs on VA offences over the three-year period, 2019 – 2021.

116. Diagram 18 below provides a graphical illustration of the frequency of illicit activities linked to VAs as reported by eight (8) regional FIUs:

Diagram 18 illustrates the frequency of VA related crimes




117. It is expected that these types of VA criminal activities will continue to thrive, to parallel the increasing usage of VAs.

# RECOMMENDATIONS

i. All member jurisdictions should take the necessary steps to enact suitable VASP/VA legislation in line with FATF recommendations and guidelines as fast as possible.

ii. Where legislation exists in relation to VAs and VASPs, jurisdictions should ensure that legislation provides for the enforcement of administrative and criminal sanctions, inclusive of financial penalties.

iii. All member jurisdictions need to improve their data gathering regarding the usage of VAs (knowledge gap).

iv. Member jurisdictions need to be more proactive in understanding the number of VASPs operating within the jurisdiction and the nature, volume and value of VA transactions.

v. Member jurisdictions should consider seeking technical assistance in the following capacities areas:

**National ML/TF NRA Committee**

**a.** Providing specific training and guidance to National ML/TF NRA Committee members on how to conduct a ML/TF risk assessment of the VASPs sector, inclusive of the identification of the risk factors synonymous with the VASPs sector.

**Supervisory Authorities**

a. Providing specific training for supervisory authority staff on how to conduct ML/TF risk assessment of the VASPs sector.

b. Training of supervisory authority staff on registering and licensing of VASPs.

c. Providing training to supervisory authority staff on how to effectively supervise the VASPs sector.

d. Providing training to the VASPs sector on how to:

I. identify, understand, assess, and take effective action to mitigate ML/TF risk.

II. apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

**Law Enforcement Agencies & Financial Intelligence Units**

a. Providing specific training to LEAs on how to investigate VASPs/VAs-related cases.

b. Developing VASPs/VAs investigative policies for LEAs.

c. Acquiring blockchain analytical tools for LEAs to facilitate investigations undertaken by these agencies.

d. Establishing government wallets to facilitate the seizure of VAs.

vi. Where not prohibited under law, member jurisdictions should consider utilising either a licensing and/ or registration regime for the regulation of VAs and VASPs operating within the respective jurisdictions.

vii. It is recommended that SAs make use of technology to aid in the supervision of VAs and VASPs.

viii. SAs should ensure that VASPs possess the requisite tools required for ongoing monitoring of transactions for the purpose of sanction screening and reporting of terrorist-link transactions.

# CONCLUSION

118. Among the participating CFATF members, there is little to no usage of VAs in the region. However, there is a knowledge gap in relation to the popularity and utility of VAs among CFATF members. VAs are used mostly for investments and payment purposes and are mostly used by individual retail customers and investors. As a result, VA trading platforms and exchanges appear to be the most common type of activity in the region. VASPs appear to be operating in most responding jurisdictions, and in some instances, unlicensed and unregistered. Half of the respondents have some form of legislation as it relates to VAs and VASPs. Jurisdictions do not intend to prohibit VAs and VASPs, but where regulations do not exist, jurisdictions signalled intent to implement such, at the very latest by December 2023.

119. Among jurisdictions, it is common practice to augment the staffing of the existing SA rather than forming a new entity. Representatives of SAs were trained as it relates to VAs and VASPs however, expert knowledge on the subject was the exception rather than the norm. The minority of SAs are equipped with the necessary analytical tools and the legislative powers to deal with AML/CFT/CPF issues. Although there was a lack of expert knowledge, most of the jurisdictions have indicated that they have some form of MOUs covering information sharing with other SAs and are maintaining proper CDD, monitoring and screening processes in the region. In spite of maintaining proper CDD and monitoring processes, most of the jurisdictions have indicated that they do not possess investigative capabilities as it relates offences relating to VAs and VASPs. Furthermore, there appears to be a lack of technology implemented for regulatory compliance and a suitable enforcement regime within the Caribbean region.

120. Less than half of the responding jurisdictions have implemented the Travel Rule. However, an information gap exists as it relates to the process of implementing the Travel Rule legislation. ML risk associated with VAs and VASPs appears to be between medium-high and high whilst the TF risk appears to be between low and medium-low. This project highlights five (5) key risks applicable to VAs and VASPs which are the nature of the VA, new payment systems, cross-border transactions, ease of accessibility for criminal activities and the operation of foreign unregistered VASPs in local jurisdictions. As global illicit cryptocurrency activities and the usage of VAs continue to increase so too will VA criminal activities and the risks associated with them.

# BIBLIOGRAPHY

2BrightSparks, & Naraharisetty, S. (n.d.). *File Sizes and Transfer Speeds*. Retrieved October 14, 2022, from https://www.2brightsparks.com/resources/articles/file-sizes-and-transfer-speeds.html#:~:text=Data%20transfer%20speed%20is%20a,bytes%20per%20second%20(B).

Australian Government: Office of the Australian Information Commissioner. (2019, July 22). *Australian Privacy Principles Guidelines*. Retrieved from Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity#:~:text=Anonymity%20means%20that%20an%20individual,to%20an%20individual's%20actual%20name

Corporate Finance Institute. (2022, August 30). *Cryptocurrency Exchanges*. Retrieved October 14, 2022, from https://corporatefinanceinstitute.com/resources/knowledge/other/cryptocurrency-exchanges/

Financial Action Task Force (FATF). (2014). *FATF Report: Virtual Currencies - Key Definitions and Potential AML/CFT Risks.* France: Financial Action Task Force. Retrieved October 14, 2022, from https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Internal Revenue Service. (2022, October 13). *Digital Assets*. Retrieved October 14, 2022, from https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets#:~:text=A%20digital%20asset%20that%20has,of%20a%20convertible%20virtual%20currency.

Oracle. (n.d.). *Peer to Peer Payments*. Retrieved October 14, 2022, from https://docs.oracle.com/cd/E92727_01/webhelp/Content/obdx/retail/p2paymnt/p2pintro.htm

Perforce. (2022, March 17). *What is Traceability?* Retrieved October 14, 2022, from https://www.perforce.com/blog/alm/what-traceability

# APPENDIX 1 - CFATF – VAs & VASPs Project - QUESTIONNAIRE

PREAMBLE
CFATF members are faced with the need to identify money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks arising from the misuse of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). As these threats evolve, so must the strategies to mitigate these risks be developed. In order for this to be accomplished, these risks must be identified and understood so that measures can be implemented to prevent the misuse of virtual assets and virtual asset service providers.

The CFATF Risk Trends and Methods Group (CRTMG) is conducting research on the measures implemented by its member jurisdictions to prevent the misuse of VAs and VASPs within the Caribbean region. Information gathered during this study will inform the production of a comprehensive report that will be shared with member jurisdictions.
In order to complete the project, the CRTMG would be grateful for your assistance in completing this questionnaire. Completion of the questionnaire should take approximately 45 minutes and all responses will be kept confidential. You may only take the survey once, but you can edit your response until the survey is closed on June 10, 2022.

We thank you for your time and consideration to this project. If you have any questions about the survey, please email us at cfatf-rtmg@cfatf.org

***Note that this survey has 142 questions.***

***Please answer only those questions that are applicable to your jurisdiction.***

## GENERAL INFORMATION

### Virtual Assets (VA)

### Definition

According to the Financial Action Task Force (FATF) the term "virtual asset" refers to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value. The FATF emphasizes that virtual assets are distinct from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the money of a country that is designated as its legal tender.

### Usage of VAs in the region

1. Please indicate the usage of VAs in your country?
   - ☐☐ No usage
   - ☐☐ Little usage
   - ☐☐ Moderate usage
   - ☐☐ Frequent usage
   - ☐☐ Not known

2. Does your jurisdiction have any reasonable estimate of how many residents own or have dealt in VAs? If so, what percentage? Click here to enter text.

3. VAs are mostly used for?
   - ☐☐ Investment purpose
   - ☐☐ Payment purpose
   - ☐☐ Medium of exchange
   - ☐☐ Not known
   - ☐☐ Other

4. VAs are less used for?
   - ☐☐ Investment purpose
   - ☐☐ Payment purpose
   - ☐☐ Medium of exchange
   - ☐☐ Other, please specify Click or tap here to enter text.

5. VAs are mostly used by?
   - ☐ Retail
   - ☐ Corporate entities/companies
   - ☐ Institutional investors
   - ☐ Other, please specify Click or tap here to enter text.

**Virtual Asset Service Providers (VASPs)**

According to the Financial Action Task Force (FATF) the term "virtual asset service provider" refers to - any natural or legal person who is not covered elsewhere under the Recommendations and as a business conduct 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.

6. Does your country apply the FATF definition to define virtual asset service providers?
   ☐☐ Yes ☐☐ No ☐☐ Somewhat

7. If your country uses another definition for VASPs, please can you provide the definition? Click or tap here to enter text.

8. Please provide the reason why the definition for VASPs differs from that of the FATF? Click or tap here to enter text.

9. Does your jurisdiction have Virtual Asset Service Providers (VASPs)?
   ☐☐ Yes ☐☐ No ☐☐ Not known

   a. If yes, how are the VASPs registered?
   ☐☐ Foreign
   ☐☐ Domestic
   ☐☐ Unregistered/Unlicensed
   ☐☐ Other: Click or tap here to enter text.

10. What stage is your jurisdiction's AML/CFT regime for licensing/ registration of VASPs?

    ☐☐ a) Your jurisdiction has an operational regime with VASPs licensed/registered
    ☐☐ b) Your jurisdiction has passed the necessary legislation/regulation, but VASPs are not yet licensed/registered.
    ☐☐ c) Your jurisdiction is passing the necessary legislation/regulation to license/register VASPs (e.g this could include public consultations on draft legislation/regulation, laws)
    ☐☐ d) Your legislation has not yet commenced the necessary legislative/regulatory process
    ☐☐ e) You intend to prohibit or have prohibited VASPs.

***NOTE: If you have answered b) to e) above, please skip to the sections on Supervision and Travel Rule. If your answer is a), please continue to question 11 below.***

11. What types of entities are licensed to operate as VASPs in your jurisdiction?
    ☐☐Offshore Banks
    ☐☐Credit Unions
    ☐☐Commercial Banks
    ☐☐Insurance Companies
    ☐☐Car Dealerships
    ☐☐Jewelry Businesses
    ☐☐Private sector entities
    ☐☐Casinos
    ☐☐Gaming Houses
    ☐☐Sports Betting
    ☐☐Money and value transfer services
    ☐☐Trust and company service providers
    ☐☐Other. Please specify Click or tap here to enter text.

12. How many VASPs are registered in your jurisdiction?

☐☐0
☐☐1 to 5
☐☐6 to 10
☐☐11 to 15
☐☐ Greater than 15 - Please specify amount Click or tap here to enter text.

13. What types of products/services do the VASPs in your jurisdiction provide? Please choose all applicable products/services from the list below:

| VASP type | VASP sub-type |
|---|---|
| ☐ **Trading Platforms and Exchanges** | ☐Centralised exchanges |
| | ☐Decentralised and peer to peer exchanges |
| | ☐OTC brokers |
| | ☐VA ATMs |
| ☐ **Issuances** | ☐Issuances |
| | ☐Public issuances |
| | ☐Private issuances |
| | ☐Funds regulated under another law<br>☐NFTs |
| ☐**Custodians** | ☐Custodians |
| ☐**Service and Product Exchange** | ☐Centralized applications |
| | ☐Decentralised applications |
| ☐**Other** | ☐Anonymisation forms |
| | ☐Fund administrators |
| | ☐Fund managers |
| | ☐Miners or validators |

14. Please state the number of persons who have applied for registration for different types of VA activities such as exchanges, custodian wallet services etc. (*add rows as needed*)

| VA activities | Number of persons registered |
|---|---|
| | |
| | |
| | |

15. Please indicate the number and type of virtual assets exchanges that exist in your jurisdiction.

| **Type of Virtual Assets Exchange** | **Number of Virtual Assets Exchanges** |
|---|---|
| Centralised | |
| Decentralised | |
| Peer to peer | |

## REGULATORY LANDSCAPE

16. Does your Jurisdiction have legislation for VAs and VASPs? ☐☐ Yes ☐☐ No

17. Are VASPs in your jurisdiction required to be registered and/or licensed with the Supervisory Authority?

☐☐ Yes ☐☐ No

a. If no, provide a projected date for the legislative framework to be implemented for the regulation of VASPs Click here to enter text.

b. If yes, where the VASP is a legal person, do the licensing/registration requirements include:

i. Persons incorporated in your jurisdiction? ☐☐ Yes ☐☐ No

ii. Persons incorporated elsewhere but offering their services in your jurisdiction? ☐☐ Yes ☐☐ No

18. Who is the designated VASP Supervisory Authority in your jurisdiction? Click here to enter text.

a. Is this a new supervisory authority? ☐☐Yes ☐☐No

19. Is it a criminal offence for VASPs to conduct virtual asset activities without being licensed and/ or registered? ☐Yes ☐ No

20. Can financial penalties be applied to VASPs who conduct virtual asset activities without being licensed and/ or registered? ☐☐Yes ☐☐ No

21. Are other sanctions available where VASPs conduct virtual asset activities without being licensed and/ or registered? ☐Yes ☐ No

22. Briefly explain the VASP registration/licensing procedure in your jurisdiction. Click or tap here to enter text.

23. Are natural persons allowed to offer virtual asset services as a business and if so, are they required to be licensed/ registered? Click here to enter text.

24. What is the VASP Supervisory Authority's role in your jurisdiction?

    ☐☐Registration
    ☐☐Supervision
    ☐☐Enforcement

25. What is the level of expertise of VASP Supervisory Authority Personnel in your jurisdiction?

    ☐☐ Some knowledge
    ☐☐ Expert knowledge
    ☐☐ No knowledge

26. Is VASPs training being provided to the VASP Supervisory Authority Personnel?
    ☐☐ Yes ☐☐ No

27. Have any supervisory technology tools (for example, block chain analytical tools) been made available to the Supervisory Authority?
    ☐☐ Yes ☐☐ No

    a. If yes, briefly describe the type of analytical tools available to the Supervisory Authority? Click or tap here to enter text.

28. Have the relevant supervisory authorities began/intend to conduct onsite/virtual examinations of the VASPs? ☐☐ Yes ☐☐ No

29. What training does your Supervisory Authority require VASPs to receive? Please specify:

    ☐☐ Information Technology
    ☐☐ Risk-Assessment
    ☐☐ Cybersecurity
    ☐☐ Anti-Money Laundering/Counter Financing of Terrorism
    ☐☐ Other. Please specify Click or tap here to enter text.

30. Are transactions monitored on an ongoing basis to inform reporting and the sanction screening procedures of VASPs relative to terrorism and proliferation financing?
    ☐☐ Yes ☐☐ No

    a. If yes, please briefly say how they are monitored? Click or tap here to enter text.

31. Are VASPs operating in your jurisdiction required to maintain a physical presence?
    ☐☐ Yes ☐☐ No

32. Are VASPs clients typically individuals (natural persons) or entities (legal persons)?

    ☐☐ Individuals
    ☐☐ Entities
    ☐☐ Both

33. Are VASPs allowed to provide services to entities without requiring beneficial owner information? ☐☐Yes ☐☐ No

34. What CDD checks are conducted on VASPs customers during onboarding? Click or tap here to enter text.

35. Do VASPs allow users to access its platform without providing KYC information?

    ☐☐ Yes ☐☐ No
    a. If yes, what is the extent of the services that can be accessed by these customers? Click or tap here to enter text.

36. What type of identification information is required/accepted to register with a VASP? Please select all that apply:

☐☐ Driver's License
☐☐ Passport
☐☐ Social Security Card
☐☐ Voter ID Card
☐☐ National ID
☐☐ Company ID
☐☐ College ID
☐☐Other. Please specify Click or tap here to enter text.

37. Please indicate whether the identification information provided during registration or licensing is verified and or certified.

☐☐ Verify
☐☐ Certified
☐☐ Both

38. How long is the information referenced at questions 24 - 28 above kept?

☐☐ 3 to 5 years
☐☐ 5 to 7 years
☐☐ Greater than 7 years

39. Are there any assurance and authentication frameworks and standards for identity in place?

☐☐ Yes ☐☐ No

40. Are indices kept by VASPs of customer wallet IDs and their corresponding CDD information?

☐☐ Yes ☐☐ No

a. If yes, how often are VASPs required to update these indices?

☐☐Daily
☐☐Weekly
☐☐ Monthly
☐☐ Quarterly
☐☐ Annually
☐☐ Other

41. Are VASPs required to enter into an agreement with other VASPs, which will facilitate the production of the CDD information of both the sender and receiver who executes a transaction?

☐☐ Yes ☐☐ No

42. What automated blockchain analytics software systems are in place within VASPs within your jurisdiction?

☐☐ Chainanalysis
☐☐ AnChain.ai
☐☐ Crystal Blockchain
☐☐ TokenAnalyst
☐☐ Elementus
☐☐ Coinfirm
☐☐ Coin Metrics
☐☐ Uppsala Security
☐☐ Coinpath
☐☐ Dune Analytics
☐☐ Coinbase Analytics
☐☐ CipherTrace
☐☐ Codefi Product Suite
☐☐ TRM Labs
☐☐ Elliptic
☐☐ Breadcrumbs.app
☐☐ Other. Please Specify Click or tap here to enter text.

43. What is the wait time before an e-wallet is granted/approved?

☐☐ Within 1 month
☐☐ Within 2 months
☐☐ Within 3 months
☐☐ Greater than 3 months

44. Are VASPs mandated to include within their AML/CFT/CPF policies, procedures and processes measures detailing the procedures to be adopted for customers who deal with VAs?

☐☐ Yes ☐☐ No

45. Are VASPs required to maintain chat logs of their customers on the network?

☐☐ Yes ☐☐ No

46. Are logs kept of all fiat to crypto transactions?

☐☐ Yes ☐☐ No

47. Are logs kept of all crypto to fiat transactions?

☐☐ Yes ☐☐ No

48. What source of funds information is requested by VASPs? Click or tap here to enter text.

49. Is the hash or wallet address sufficient when completing source of funds information?

☐☐ Yes ☐☐ No

50. Are VASPs required to have cybersecurity measures to counter threats?

☐☐ Yes ☐☐ No

51. How is VASP's customer information collected, collated and stored? Click or tap here to enter text.

52. Does the VASP have the ability to block/halt transactions and to freeze assets?

☐☐ Yes ☐☐ No

53. Can transactions be completed anonymously?

☐☐ Yes ☐☐ No

a. If yes, please provide the type of transactions that can be completed Click or tap here to enter text.

54. Can transactions be completed pseudonymously?

☐☐ Yes ☐☐ No

a. If yes, please provide the type of transactions that can be completed Click or tap here to enter text.

55. Does your domestic legislation prohibit nationals from using VASPs services operating outside of your country? ☐☐ Yes ☐☐ No

56. Please indicate which of the following items have been issued by your jurisdiction to the VASP sector?

☐☐ Guidance Notes
☐☐ Sector-Specific Guidelines
☐☐ Regulations
☐☐ Notices
☐☐ Other

57. Please state the applicable law, regulations or guidelines, if any, that require applicants for licensing/registration to have AML/CFT compliance controls in place and/or submit them as a part of the licensing/registration process. Click or tap here to enter text.

58. Are VASPs subject to risk-based AML/CFT supervision? ☐☐ Yes ☐☐ No

59. Are VASPs subject to risk-based prudential supervision? ☐☐ Yes ☐☐ No

60. Does the Supervisory Authority have adequate powers to:

a) Supervise/monitor VASPS to ensure compliance with AML/CFT/CPF legislation? ☐☐ Yes ☐☐ No

b) Conduct inspections? ☐☐ Yes ☐☐ No

c) Compel the production of information/documents? ☐☐ Yes ☐☐ No

d) Impose sanctions (financial, criminal or any other) including the power to withdraw, restrict or suspend the VASPs' licence/registration? ☐☐ Yes ☐☐ No

61. Is there any special software being utilised to conduct AML/CFT examinations?
☐☐ Yes ☐☐ No

    a. If yes, please detail supervisory tools being used Click or tap here to enter text.

62. Have you used blockchain analytics to tests the adequacy of VASPs compliance?
☐☐ Yes ☐☐ No

    a. If yes, how has it been used? Click or tap here to enter text.

63. Please state the types of sanctions applicable to legal and natural persons for breaches of AML/CFT requirements. Click or tap here to enter text.

64. Are sanctions applicable to the institution, the directors and senior management?
☐☐ Yes ☐☐ No

65. For the period 2019-2021, please provide statistics on any criminal, administrative or civil sanctions applied to VASPs for breaches of ML/TF obligations, whether by domestic or foreign law enforcement.

| YEAR | Type of Sanction *Criminal, Administrative, Civil)* | Number of Sanctions applied | Body which applied the sanction | Nature of the breach |
|---|---|---|---|---|
| 2021 | | | | |
| 2020 | | | | |
| 2019 | | | | |

66. Is there a threshold for occasional transactions for which CDD is applicable?
☐☐ Yes ☐☐ No

    a. If yes, state the threshold Click or tap here to enter text.

67. For prudential supervision, is there a requirement for supervisory approval for a VA to be traded? ☐☐ Yes ☐☐ No

68. Is there a criterion established for the trading of a VA? ☐☐ Yes ☐☐ No

    a. If yes, describe Click or tap here to enter text.

69. Are there requirements for treating with the custody of clients' assets (VAs and funds) such as:
    a) Provision for assets to be held by a trust; ☐☐ Yes ☐☐ No
    b) Percentage of assets to be stored in cold wallets; ☐☐ Yes ☐☐ No
    c) Funds to be held in segregated accounts; ☐☐ Yes ☐☐ No
    d) Insurance coverage? ☐☐ Yes ☐☐ No

70. Are there provisions to detect and prevent market manipulation and abuse?
    ☐☐ Yes ☐☐ No
    a. If yes, please indicate what those provisions are Click or tap here to enter text.

71. Are there legislative provisions for the prevention of conflicts of interest?
    ☐☐ Yes ☐☐ No
    a. If yes, please state Click or tap here to enter text.

72. Are there requirements for the operator of the trading platform to disclose certain information pertaining to risks etc. to investors? ☐☐ Yes ☐☐ No

73. Are there restrictions on the type of investors that are allowed to participate (for e.g. professional investors only)? ☐☐ Yes ☐☐ No
    a. If yes, please state the type of investors and reasons for the restriction(s) Click or tap here to enter text.

74. Are there reporting obligations imposed on the operator of the trading platform?
    ☐☐ Yes ☐☐ No
    a. If yes, what are those obligations Click or tap here to enter text.

75. Are there entry barriers to the number and persons that are allowed to offer trading platforms? ☐☐ Yes ☐☐ No

76. Will the trading platform facilitate the inclusion of market makers (MM)?
    ☐☐ Yes ☐☐ No

77. Are there restrictions on the persons/entities that are allowed to be a MM?

☐☐ Yes ☐☐ No

a. If yes, what are those restrictions Click or tap here to enter text.

78. Are MMs subject to a licensing/registration regime? ☐☐ Yes ☐☐ No

## AML/CFT Risk Assessment and Mitigation

79. Has your jurisdiction conducted a ML/TF/PF risk assessment on the VASP Sector?

☐☐ Yes ☐☐ No

a. If yes, was it part of a national risk assessment or sectoral risk assessment?

☐☐ National
☐☐ Sectoral
☐☐ Both
☐☐ Other, please provide details Click or tap here to enter text.

80. What was the ML risk rating from the risk assessment for the VASP sector?

☐☐ Very High
☐☐ High
☐☐ Medium-High
☐☐ Medium
☐☐ Medium-Low
☐☐ Low

81. What was the TF risk rating from the risk assessment for the VASP sector?

☐☐ Very High
☐☐ High
☐☐ Medium-High
☐☐ Medium
☐☐ Medium-Low
☐☐ Low

82. Has the VASP Sector adopted a Risk Based Approach to identify, measure, monitor and Mitigate ML/FT risks faced? ☐☐ Yes ☐☐ No

83. Has training been conducted by the relevant supervisory authority on identifying and mitigating ML/TF/PF risk faced by the VASP Sector? ☐☐ Yes ☐☐ No

84. Do the VASPs provide services outside of your jurisdiction? ☐☐ Yes
☐☐ No

    a. Briefly explain due diligence measures required for clients outside your jurisdiction Click or tap here to enter text.

85. Did your jurisdiction develop a sandbox as part of your regulatory framework?
☐☐ Yes ☐☐ No

    a. If yes, are there currently any players in the sandbox? ☐☐ Yes
    ☐☐ No

    b. If yes, please indicate the number of players that are currently in your sandbox:

        ☐☐ Less than 10
        ☐☐ Greater than 10, less than 20
        ☐☐ Greater than 20

86. What are the ML/TF risks identified by the VASP Sector in your Jurisdiction? (Please select all that apply)

☐☐ No VASPs legislation
☐☐ No training for regulators
☐☐ No training for LEAs
☐☐ Absence of supervisory tools
☐☐ No regulatory sandboxes
☐☐ Limited cybersecurity measures at FIs/DNFBPs
☐☐ Unregulated exchanges
☐☐ Absence of block-chain analysis tools at FIs/DNFBPs
☐☐ No licensing regime
☐☐ No registering regime
☐☐ Compliance Officer not trained
☐☐ Absence of TF risk analysis

☐☐ No government wallet to seize cryptocurrencies
☐☐ No investigative policies
☐☐ Limited LEA training
☐☐ Prosecution staff not trained
☐☐ Magistrate not trained
☐☐ Judges not trained
☐☐ Inadequate capacity to understand lightning network
☐☐ Prosecution staff not trained
☐☐ No cryptocurrency-reporting threshold
☐☐ Inability to apply TFS – Terrorism Financing
☐☐ Inability to apply TFS – Proliferation Financing
☐☐ Lack of understanding of blockchain technology by LEAs
☐☐ Lack of understanding of blockchain technology by supervisors
☐☐ VA definition does not cover NFTs
☐☐ VASPs inability to prefund trades
☐☐ Other. Please Specify Click or tap here to enter text.

87. Are VASPs allowed to conduct off-chain transactions[12]?

☐☐ Yes ☐☐ No

88. Are VASPs allowed to exchange one type of VA for another? (E.g. Exchange Bitcoin for Ether)

☐☐ Yes ☐☐ No

89. Are VASPs customers in your jurisdictions allowed to use mixers/ tumblers?

☐☐ Yes ☐☐ No

## TRAVEL RULE

**Definition**

According to the Financial Action Task Force (FATF) the 'travel rule' is a key AML/CFT measure, which mandates that VASPs obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers.

[12] *Off-chain transactions refer to those transactions occurring on a cryptocurrency network that move the value outside of the blockchain, for example, the lightening network. Due to their zero/low cost, off-chain transactions are gaining popularity, especially among large participants.*

90. Has your jurisdiction enacted legislation mandating VASPs to comply with the travel rule?

☐☐ Yes ☐☐ No

***Only if you have answered No above, please skip to the next section on Intelligence and Information Sharing. If you have answered Yes, please continue with question 91.***

91. Are VASPs required to undertake CDD measures when conducting VA transfers (i.e. exchange travel rule information) in circumstances outlined in FATF Recommendation 16?

☐☐ Yes ☐☐ No

a. If yes, please state the legislative provision that applies Click or tap here to enter text.

92. What is the threshold for the exchange of travel rule information? (i.e.USD/EUR 1000 or does it applies to all transactions irrespective of value.) Click or tap here to enter text.

93. Are VASPs required to ensure that all transfers of USD/EUR 1000 or more are accompanied by

a. The originating customer's verified/certified name ☐☐ Yes ☐☐ No
b. The originating customer's verified account number ☐☐ Yes ☐☐ No
c. The originating customer's verified physical address, national ID No., or date or place of birth ☐☐ Yes ☐☐ No ☐☐ SOME
d. The beneficiary customer's name ☐☐ Yes ☐☐ No
e. The beneficiary customer's account number ☐☐ Yes ☐☐ No

94. Are recipient VASPs required to retain the same information as the originator?

☐☐ Yes ☐☐ No

95. Are ordering VASPs prohibited from executing VA transfers where they do not comply with the requirements of R.16? ☐☐ Yes ☐☐ No

96. Are audits/assessments conducted to verify that VASPs have implemented the travel rule? ☐☐ Yes ☐☐ No

    a. If yes, for the period under review, please indicate the number of such audits conducted:

| YEAR | NUMBER OF AUDITS |
|---|---|
| 2021 | |
| 2020 | |
| 2019 | |

97. What were the findings with respect to the audits conducted? Click here to enter text.

98. Please describe the compliance mechanism, tools or protocols implemented by VASPs to comply with the travel rule. Click here to enter text.

99. Please describe any challenges or obstacles encountered (if any) in assessing VASPs compliance with the travel rule. Click here to enter text.

100. Does the same competent authority that regulates VASPs assess compliance with the Travel Rule? ☐☐ Yes ☐☐ No

101. Is compliance with the Travel Rule:

    a. Assessed by the same part of the competent authority that assesses AML/CFT compliance? ☐☐ Yes ☐☐ No

    **OR**

    b. Dealt with by a wider VASP licensing division/group/department? ☐☐ Yes ☐☐ No

102. Does your jurisdiction test that VASPs have implemented the travel rule? ☐☐ Yes ☐☐ No

103. Is this testing through regulatory supervision? ☐☐ Yes ☐☐ No
☐☐ Other

Please explain. Click here to enter text.

104. Do you assess the procedures used by VASPs to implement the Travel Rule?

☐☐ Yes ☐☐ No

105. Do you assess the technological tools used by VASPs? ☐☐ Yes ☐☐ No

106. What technological tools, if any, have VASPs in your jurisdiction utilized to assist their compliance with the travel rule requirement? ☐☐ Yes ☐☐ No

107. What challenges have VASPs in your jurisdiction encountered in implementing the travel rule? Click here to enter text.

***Counterparty VASPs due diligence***

108. Are VASPs required to assess the risks associated with and involved in transacting with another VASPs ? ☐☐ Yes ☐☐ No

a. If yes, when are such assessments required to take place? (tick all that applies)

☐☐ Prior to engaging in a transaction;
☐☐ On a periodic basis;

i. If on a periodic basis, please indicate the frequency required Click here to enter text.

109. Have guidelines in relation to counterparty VASPs due diligence been issued by the Supervisory Authority? ☐☐ Yes ☐☐ No

a. If yes, please indicate what information VASPs are required to collect on counterparty VASPs (that is "the VASP on the opposite side of a Travel Rule data transfer")

☐☐ Evidence that the VASP is regulated

☐☐ Evidence of the sufficiency of the VASP's AML/CFT compliance framework

☐☐ Evidence that the jurisdiction in which the VASP resides is compliant with FATF recommendations

☐☐ Publicly available information such as whether the VASP has been subject to regulatory action

☐☐ Other, please specify Click or tap here to enter text.

110. In assessing VASPs' compliance with the travel rule, what, if any, solutions or tools have been identified as being used by VASPs to enable them to perform comprehensive due diligence on their VASP counterparties? Click or tap here to enter text.

111. How do VASPs in your jurisdiction verify that the receiving VASP is regulated? Click or tap here to enter text.

112. How do VASPs obtain the identity of the beneficiary if the beneficiary is the customer of another VASP that may operate in another jurisdiction? Click or tap here to enter text.

113. How do VASPs ensure the security of identification information of clients whilst retaining and transmitting to the receiving or intermediary VASPs? Click here to enter text.

## INTELLIGENCE AND INFORMATION SHARING

**Intelligence**

114. Does your country have investigative expertise and capability to investigate ML/TF/PF utilizing VAs and VASPs? ☐☐ Yes ☐☐ No

115. For the period 2019 – 2021, please state the number of SARs/STRs your FIU has received that were submitted by VASPs.

| Number of SARs/STRs | | |
|---|---|---|
| 2021 | 2020 | 2019 |
| | | |

116. For the period 2019 – 2021, please state the number of SARs/STRs your FIU has received that were submitted by any Reporting Entities whose narrative mentions VAs or VASPs.

| Number of SARs/STRs | | |
|---|---|---|
| 2021 | 2020 | 2019 |
| | | |

117. What were the underlying suspected offences relating to these VAs/VASPs-related SARs/STRs?

| YEAR | Underlying Offences |
|---|---|
| 2021 | |
| 2020 | |
| 2019 | |

118. State the aggregated amount in United States Dollars (USD) reported over this period. Click or tap here to enter text.

119. Of the SARs/STRs related to VA/VASPs filed during the period 2019-2021, please indicate the number of local transactions **only,** and the number involving transactions from other jurisdictions.

| YEAR | Number of local transactions | Number of foreign transactions |
|---|---|---|
| 2021 | | |
| 2020 | | |
| 2019 | | |

120. Of these SARs/STRs, how many were converted to case disclosures and submitted for investigation purposes?

| YEAR | Number of disclosures | Number submitted for investigations |
|---|---|---|
| 2021 | | |
| 2020 | | |
| 2019 | | |

a. State the aggregated value of transactions in USD in these case disclosures Click or tap here to enter text.

121. State the number of investigations (if any) arising from these disclosures

| YEAR | Number of disclosures | Number of investigations |
|---|---|---|
| 2021 | | |
| 2020 | | |
| 2019 | | |

122. State the number of persons charged (if any) stemming from these SARs/STRs related investigations and the number of convictions if any

| YEAR | Number of SARs/STRs related investigations | Number of persons charged | Number of convictions |
|---|---|---|---|
| 2021 | | | |
| 2020 | | | |
| 2019 | | | |

123. For the period 2019-2021 please indicate whether or not there were any forfeiture/confiscation proceedings involving VAs and the value of the assets in USD recovered

| YEAR | Number of forfeiture proceedings | Value of assets recovered (USD) |
|---|---|---|
| 2021 | | |
| 2020 | | |
| 2019 | | |

124. Please give details of any VASPs that were fined or subject to investigation or adverse media.

| **No.** | **Fined** | **Investigations** | **Adverse Media** |
|---|---|---|---|
| 1. | | | |
| 2. | | | |

125. With respect to civil recovery of assets, are the existing powers contained within your anti-money laundering legislation sufficient? ☐☐ Yes ☐☐ No

a. If yes, please explain Click or tap here to enter text.

**Information Sharing**

126. Do existing MOUs cover the sharing of information for VA/ VASPs?

☐☐ Yes ☐☐ No

a. If no, please describe measures your country has taken to facilitate effective domestic cooperation, coordination and information sharing on VASPs Click or tap here to enter text.

127. Please indicate circumstances under which mutual legal assistance is prohibited, restricted or refused with regard to information on VAs that is held by VASPs?

☐☐ Yes ☐☐ No

128. Has your jurisdiction provided international cooperation information relating to VASPs concerning ML/TF/PF or associated predicate offences investigations?

☐☐ Yes ☐☐ No

a. If yes, please provide information on the following:

| No. | No. of Requests | Jurisdiction | Underlying Offences |
|---|---|---|---|
| 1. | | | |
| 2. | | | |

129. Have you requested any information on VAs/VASPs from other jurisdictions?

☐☐ Yes ☐☐ No

a. If yes, using the Table below, please indicate:

i. The number of requests made;
ii. The underlying offences cited in the request;
iii. The jurisdictions to which the requests were made; and
iv. whether or not the information requested was provided:

| YEAR | Number of requests | Underlying offences | Jurisdictions | Instances in which information was received |
|---|---|---|---|---|
| 2021 | | | | |
| 2020 | | | | |
| 2019 | | | | |

130. Please describe mechanisms in place to protect information received Click or tap here to enter text.

131. Please describe and indicate specific provisions that will facilitate and allow for prompt and constructive exchange of information directly between counterparts. (e.g MOUs) ) Click or tap here to enter text.

## LAW ENFORCEMENT

132. Does the FIU have the technical capacity to set up encrypted channels to facilitate submission of suspicious transactions/activities from VASPs in your jurisdiction?

☐☐ Yes ☐☐ No

133. Has your jurisdiction established a secure encrypted channel to facilitate submissions of suspicious transaction/activity reports from VASPs? ☐☐ Yes ☐☐ No

134. Do Law Enforcement Agencies (LEAs) have the requisite skills to investigate money laundering, terrorism financing or proliferation financing utilizing VAs and VASPs?

☐☐ Yes ☐☐ No

135. What types of block-chain analytical tools are being used by LEAs in your country?

☐☐ Chainanalysis
☐☐ AnChain.ai
☐☐ Crystal Blockchain
☐☐ TokenAnalyst
☐☐ Elementus
☐☐ Coinfirm
☐☐ Coin Metrics
☐☐ Uppsala Security
☐☐ Coinpath
☐☐ Dune Analytics
☐☐ Coinbase Analytics
☐☐ CipherTrace
☐☐ Codefi Product Suite
☐☐ TRM Labs
☐☐ Elliptic
☐☐ Breadcrumbs.app
☐☐ None
☐☐ Other. Please Specify Click or tap here to enter text.

136. Has your country established a forfeiture wallet to store seized or confiscated crypto currencies? ☐☐ Yes ☐☐ No

    a. If yes, what measures are in place to identify the receiving customer of the receiving VASPs? Click or tap here to enter text.

137. Do VASPs retain the IP address data of other VASPs? ☐☐ Yes ☐☐ No

138. How are suspicious transaction reports submitted?

    ☐☐ via a web service
    ☐☐ E-filing platform
    ☐☐ Encrypted channel
    ☐☐ Physical forms
    ☐☐ Channel
    ☐☐ Other. Please specify Click or tap here to enter text.

139. What VASP-specific information is required to be submitted to the FIU in the event of a SAR/STR? Click or tap here to enter text.

140. Within your jurisdiction, have there been any suspicion of the following predicate or criminal offences using virtual assets?

    ☐☐ Ransomware attacks [often, seldom, never]
    ☐☐ Fraud and scams [often, seldom, never]
    ☐☐ Money laundering [often, seldom, never]
    ☐☐ Breach of sanctions [often, seldom, never]
    ☐☐ Terrorist financing [often, seldom, never]
    ☐☐ Other Click or tap here to enter text.

141. Has your jurisdiction identified any emerging risks/threats arising from VAs and VASPS?

142. Are there any other measures your country has implemented to ensure that it can effectively investigate and gather information held by VASPs?

    ☐☐ Yes ☐☐ No

    a. If yes, please specify Click or tap here to enter text.

***END OF QUESTIONNAIRE***
**Thank you for your responses.**