TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

JUNE 2023

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2023), *Targeted Upate on Implementation of the FATF Standards on Virtual Assets/VASPs,* FATF, Paris, France,
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023

Photocredits coverphoto ©Gettyimages

Table of Contents

Executive summary

It has now been four years since the Financial Action Task Force (FATF) extended its global standards on anti-money laundering and counter-terrorist financing (AML/CFT) to apply to virtual assets (VAs) and virtual asset service providers (VASPs). Some of the more significant virtual asset markets in terms of materiality and scale of virtual asset activity have AML/CFT regulation in place or in progress. However, it is a serious concern that 75% of jurisdictions assessed against the revised standards are only partially or non-compliant with FATF's requirements. Compliance remains behind most other areas of the financial sectors. The FATF has observed some private sector players collaborate to amend Travel Rule compliance tools, showing a willingness to improve industry compliance, even if shortcomings remain.

In that context, this report provides a fourth targeted review of implementation of the FATF's Standards on VAs and VASPs[1], including the Travel Rule, and an update on emerging risks and market developments in this area.

Key Findings

- Four years after the FATF's adoption of standards on VAs and VASPs (Recommendation 15; R.15), some jurisdictions have introduced regulations, but global implementation is relatively poor and compliance remains behind most other financial sectors. Based on 98 FATF mutual evaluation and follow-up reports since the standards on VAs and VASPs were adopted, three quarters of jurisdictions (75%; 73 of 98) are only partially or not compliant with the FATF's requirements.
- Jurisdictions continue to struggle with fundamental requirements. Out of 151 respondents to a March 2023 survey on R.15 implementation (compared to 98 responses in 2022), over one third (52 of 151) have not conducted a risk assessment. The results of mutual evaluation and follow-up reports show that 73% (71 of 98 jurisdictions) are not conducting adequate risk assessments. Almost one third of survey respondents (45 of 151) have not yet decided if and how to regulate the VASP sector. While 60% of respondents (90 of 151) decided to permit VAs and VASPs, 11% (16 of 151 jurisdictions) report opting to prohibit VASPs. Mutual evaluation and follow-up results indicate that effectively prohibiting VASPs is difficult; only one jurisdiction taking this approach has been assessed as largely compliant with the FATF requirements. It is further unclear to what extent the decision to prohibit VASPs is the result of a thorough risk assessment.
- Jurisdictions have made insufficient progress on implementing the Travel Rule, leaving VAs and VASPs vulnerable to misuse. More than half of the survey respondents (73 of 135, excluding those that prohibit VASPs) have taken no steps towards Travel Rule implementation, and this group is expected to be even larger in reality as it is likely to include the additional 54 jurisdictions

[1] FATF (2020) 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs; FATF (2021) Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs; FATF (2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*.

that did not respond to the FATF's survey. Two thirds (25 of 38 respondents) of the jurisdictions who assessed VAs/VASPs as high risk and do not take a prohibition approach have not yet passed legislation implementing the Travel Rule. The situation is evolving with some progress being made since the survey; for example, the European Union passed legislation that establishes a regulatory framework for VASPs[2] and implements the travel rule.[3] This brings the number of jurisdictions that have passed legislation or regulation to implement the travel rule to 58, reflecting more significant progress since 2022, although global compliance remains unsatisfactory. Even among jurisdictions implementing the Travel Rule, supervision and enforcement is low: only 21% (13 of 62 respondents) have issued findings or directives or taken enforcement or other supervisory actions against VASPs focused on Travel Rule compliance.

- The private sector now offers a range of technological tools to enable VASPs to implement the Travel Rule. However, these tools generally do not fully comply with all the FATF's Travel Rule requirements. Limited progress has been made since last year to improve interoperability between Travel Rule compliance tools, although interoperability is not a precondition for Travel Rule implementation under the FATF Standards. Some jurisdictions and private sector participants believe that enforcement of Travel Rule violations may be a necessary step to push progress in this area.
- Recent reports[4,5,6] raise serious concerns about the threat posed by the Democratic People Republic of Korea's (DPRK) illicit VA-related activities, including ransomware attacks and sanctions evasion, for financing the proliferation of weapons of mass destruction. This activity has enabled an unprecedented number of recent launches of ballistic missiles (including inter-continental ballistic missiles). This threat is significant given both the scale of the funding (USD 1.2 billion worth of stolen VAs since 2017, including VAs stolen from DeFi arrangements) and the serious consequences of proliferation financing. Virtual assets are also posing increasing terrorist financing risks, including for fundraising by ISIL, Al Qaeda and right-wing extremist groups, although the vast majority of terrorist financing still takes place using fiat currency.

---

2 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance).

3 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance).

4 UN Security Council (March 2023) S/2023/171 "Letter dated 3 March 2023 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council", pgs.4, 74-78.

5 AP News (22 December 2022) "Seoul: North Korean hackers stole $1.2B in virtual assets".

6 U.S. Department of the Treasury (24 April 2023) "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs", available at: https://home.treasury.gov/news/press-releases/jy1435; U.S. Department of the Treasury Office of Foreign Assets Control (15 May 2022) "Publication of North Korea Information Technology Workers Advisory", available at: https://ofac.treasury.gov/recent-actions/20220516.

- Decentralised finance (DeFi) and unhosted wallets, including peer-to-peer (P2P) transactions, although a subset of the overall virtual asset ecosystem, pose money laundering, terrorist financing and proliferation financing risks, including abuse by sanctioned actors. Some jurisdictions reported challenges in mitigating these risks, including in identifying specific natural or legal persons responsible for VASP obligations in DeFi arrangements, assessing the illicit finance risks associated with unhosted wallet transactions including P2P transactions, and filling data gaps. As the VA ecosystem continues to evolve, and more VASPs implement AML/CFT controls, the risks posed by DeFi and P2P transactions could increase. This is particularly the case if VAs are mass-adopted and more commonly used for payments (without needing to access fiat currency). Both jurisdictions and the private sector should strengthen efforts to monitor these risks, share approaches, and identify challenges to mitigate such risks, in addition to implementing the FATF Standards.

Recommendations for the public and private sectors

It is vital that countries act rapidly to implement the FATF's requirements on VAs and VASPs. The recommendations below identify actions that jurisdictions should urgently take based on the findings of this report, and next steps for the FATF and the Virtual Assets Contact Group (VACG).

Recommendations for the Public Sector

Risk assessment, mitigation and licensing/registration

- Jurisdictions that have not yet assessed the risks of VAs and VASPs should make use of available resources, including the FATF's 2021 guidance[1] and the *Community Workspace on Virtual Assets*[2], to identify the risks, and put in place risk mitigation measures, including measures to combat identified regulatory and supervisory challenges.
- Both jurisdictions that permit VAs and VASPs and those that prohibit them should commence or continue monitoring or supervising their VASP population and enforcing against non-compliance, including sanctioning illicit VASPs.
- In light of increasing TF and PF threats related to VAs, jurisdictions should take immediate action to mitigate these risks, including by ensuring full implementation of R.15 and adopting other risk-based measures (e.g., enhancing cybersecurity).
- Jurisdictions should assess illicit finance risks of DeFi arrangements, consider how DeFi arrangements fit into their AML/CFT frameworks, and share their experiences, practices and remaining challenges with the FATF's global network to mitigate the risk of DeFi arrangements.

- Jurisdictions are encouraged to assess and monitor the risks associated with unhosted wallets, including P2P transactions, and share their experiences, including on data collection and risk assessment methodologies and findings, as well as practice in mitigating risks.

Implementation of the Travel Rule

- Jurisdictions that have not yet introduced legislation/regulation to implement the Travel Rule should urgently do so.
- Jurisdictions that have introduced the Travel Rule should rapidly operationalise it, including through effective supervision and enforcement against non-compliance.
- To facilitate counterparty due diligence in line with R.16 as well as R.13, jurisdictions are strongly encouraged to maintain and publicise information on VASPs that are registered or licensed in their jurisdiction.
- Jurisdictions could consider engaging with their VASP sector to promote the adoption of Travel Rule compliance tools that meet all the FATF requirements. This could include optionally engaging with tool providers to identify possible shortcomings and impress the importance of full compliance.

Recommendations for the Private Sector

- VASPs and Travel Rule compliance tool providers should:
  - review their Travel Rule compliance tools to ensure they fully comply with the FATF requirements, and should rapidly address any shortcomings; and
  - improve the interoperability of their Travel Rule compliance tools globally, whether through technological advancements that allow interoperability between tools or by developing relationships that permit transactions to be made through a chain of interoperable tools.
- In light of increasing TF and PF threats related to VAs, the private sector and particularly VASPs should ensure they have appropriate risk identification and mitigation measures in line with R.15 and adopt other risk-based measures (e.g., cyber security measures).
- The private sectors should continue to monitor and assess the risks across the VA ecosystem, including related to DeFi and unhosted wallets, including P2P transactions. They should also take steps to mitigate these risks and to consult with regulators as necessary to ensure a common risk understanding.

Notes

1. FATF (2021), *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* /www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
2. The Community Workspace on Virtual Assets is available to government officials of the FATF Global Network only. To request access, authorities should contact their lead ministry or authority in their country's delegation to the FATF, or their FSRB's Secretariat.

Next steps

The FATF will also continue work in this space. In February 2023, the FATF adopted a roadmap through to June 2024 to improve implementation of R.15. The FATF and its Virtual Assets Contact Group (VACG) will continue to conduct outreach and provide assistance to low-capacity jurisdictions to encourage compliance with R.15. In the first half of 2024, the FATF will publish a table showing the steps FATF member jurisdictions and other jurisdictions with materially important VASP activities have taken towards implementing R.15 (e.g., undertaking a risk assessment, enacting legislation to regulate VASPs, conducting a supervisory inspection, etc.). In addition, the FATF and VACG will continue to share finding, experiences and challenges, including relating to DeFi and unhosted wallets, including P2P, and monitor market trends in this area for developments that may necessitate further FATF work.

Introduction

1. In October 2018, the FATF updated Recommendation 15 (R.15) to extend AML/CFT requirements to virtual assets (VAs) and virtual asset service providers (VASPs). In June 2019, the FATF adopted an Interpretive Note to R.15 to further clarify how the FATF requirements apply to VAs and VASPs. Since then, the FATF has undertaken a significant amount of work to identify and address gaps in implementation, provide guidance to jurisdictions to facilitate implementation (see Table 1.1), and monitor emerging risks in the VA sector.

Table 1.1 Overview of FATF work on VAs and VASPs

2018	• Recommendation 15 amended
2019	• Adoption of Interpretive Note to R.15 • Creation of the FATF Virtual Assets Contact Group (VACG) • Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021)
2020	• 12 month review of the new FATF Standards: 1st12-month review • Report to the G20: FATF Report to the G20 on So-calledStablecoins • Risk indicators: List of Red Flag Indicators of ML/TF through VAs
2021	• Updated guidance[7]: Updated Guidance for a Risk-Based Approach to VA and VASPs • 24 month review of the FATF Standards: 2nd12-month review
2022	• Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs
2023	• Report on ransomware, with focus on VA risks and trends: Countering Ransomware Financing

2. This report is the FATF's fourth report on the global implementation of the FATF's Standards on VAs and VASPs, in particular the Travel Rule. It provides an overview of global implementation of R.15; outlines challenges in implementing the FATF Standards; shares suggested solutions or progress made by the public and private sectors; and provides an overview of emerging risks relating to VAs and how jurisdictions and industry are responding to these risks. This report is based on:

- A March 2023 survey on jurisdiction implementation of R.15, the Travel Rule, and responses to emerging risks. The voluntary survey collected responses from 151 jurisdictions (37 FATF members and 114 FSRB members), an increase from 98 responses to the 2022 survey. Responses were self-reported and not verified. The survey applied conditional branching/skip logic, meaning respondents would be directed to certain questions based on their answer to a previous question (e.g., respondents that indicated that they had not yet decided whether to prohibit or regulate VASPs were not asked questions on licensing/registration or Travel Rule implementation). As a

[7] The 2021 Guidance includes updates focusing on the following six key areas: clarification of the definitions of virtual assets and VASPs; guidance on how the FATF Standards apply to stablecoins; additional guidance on the risks and the tools available to jurisdictions to address the ML/TF risks for peer-to-peer transactions; updated guidance on the licensing and registration of VASPs; additional guidance for the public and private sectors on the implementation of the Travel Rule; and principles of information-sharing and co-operation amongst VASP supervisors.

result, the number of respondents to each question group varied[8]. The report considers that the 54 jurisdictions that did not espond to the survey have not made progress on R.15.

- Meetings of the FATF's Virtual Assets Contact Group (VACG) throughout late 2022 and early 2023, including consultations with representatives from the VA sector in November 2022 and April 2023.[9]
- Results from completed and published FATF mutual evaluations reports (MERs) and follow-up reports (FURs), as of April 2023.

3. This report comprises the following sections:

- Section 1 provides an overview of jurisdictions' implementation of R.15 across the FATF's global network and the major challenges they faced in assessing ML/TF risks and licensing or registering VASPs.
- Section 2 provides information on global implementation of the FATF's Travel Rule and shares public and private sector progress and challenges in implementing the Travel Rule, including advances and outstanding difficulties in the development of compliance tools.
- Section 3 considers market developments and emerging risks, in particular decentralised finance (DeFi), unhosted wallets [10] including peer-to-peer transactions (P2P), non-fungible tokens (NFTs), and the use of VAs for financing the proliferation of weapons of mass destruction and terrorist financing.
- Section 4 provides recommendations and suggesting actions for the public and private sectors.
- Section 5 sets out the next steps for the FATF and VACG

[8] Risk assessment and policy approach to VASPs: 151 respondents; licensing/registering and supervising VASPs: 90 respondents; Travel Rule implementation: 62 respondents; treatment of DeFi, NFTs, unhosted wallets, and P2P transactions: 62 respondents; final comments: 150 respondents.

[9] VACG meetings with private sector outreach were held in November 2022 in Paris, France and in April 2023 in Tokyo, Japan. These meetings brought together officials from jurisdictions, international organisations and industry representatives from virtual assets service providers, blockchain analytics companies, industry bodies and financial institutions.

[10] Also referred to as non-custodial, self-custodial or self-hosted wallets.

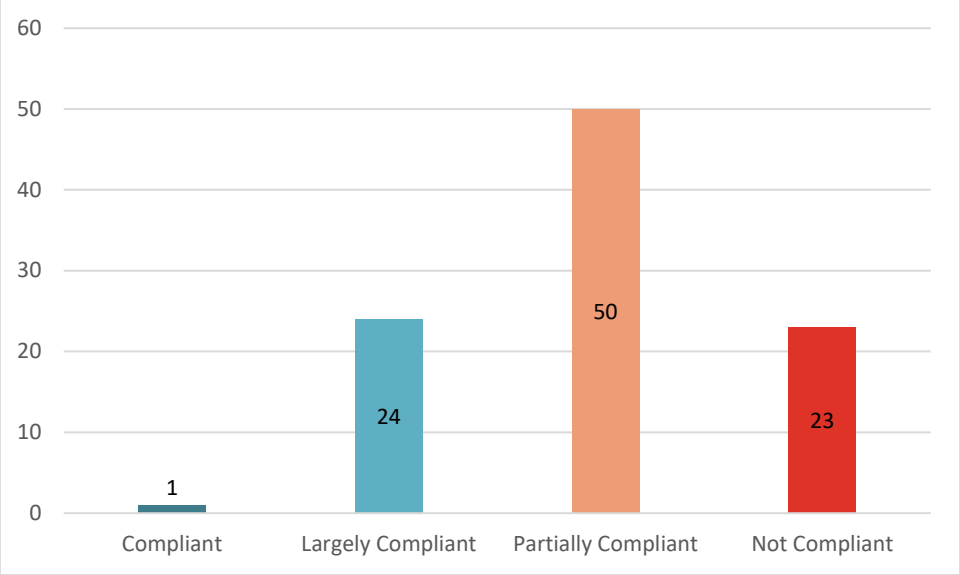
SECTION ONE:
Jurisdictions' Implementation of FATF Standards on VAs/VASPs (R.15)

Overall Status of R.15 Implementation in Mutual Evaluation and Follow-up Reports

4. Jurisdictions are making limited progress implementing the FATF's requirements on VAs and VASPs (as set out in R.15 and INR.15). As of April 2023, the FATF and its FATF Style Regional Bodies (FSRBs) have assessed 98 jurisdictions' compliance with the revised R.15[11]. Most jurisdictions (73 of 98 jurisdictions) are only partially or not compliant with the FATF's requirements[12]. Only 24 jurisdictions (25%) are largely compliant and one jurisdiction is fully compliant (see Figure 1.1).

Figure 1.1 Compliance with R.15

Based on assessment results for 98 jurisdictions, as of April 2023

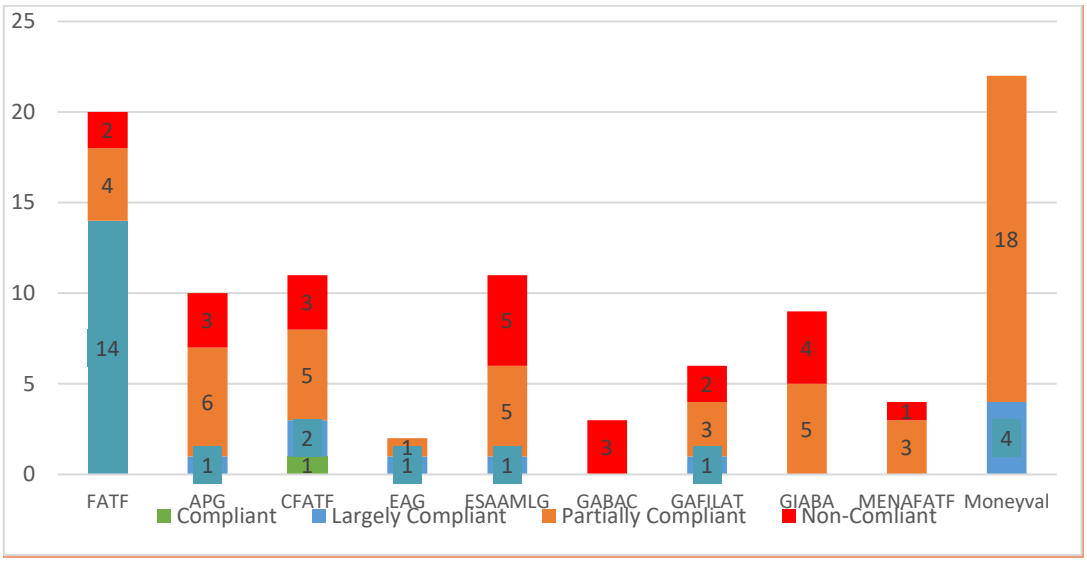


[11] This consists of technical compliance ratings of 98 jurisdictions which have been assessed on the revised R.15 as of April 2023.

[12] While most of the requirements of R.15 are related to VAs and VASPs, the Recommendation also includes broader requirements around new technologies. A jurisdiction's performance on these elements will also impact their overall R.15 rating.

Figure 1.2. Compliance with R.15 by FATF/FSRB as of April 2023

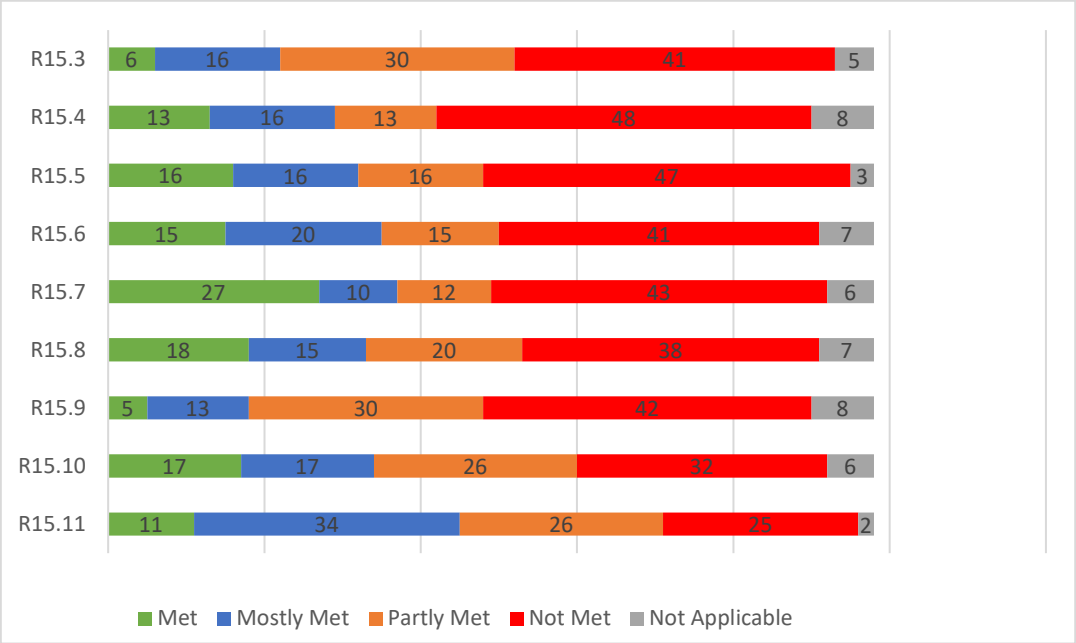
Based on assessment results for 98 jurisdictions, as of April 2023



5. Assessment results indicate that countries continue to struggle with several fundamental requirements, including conducting a risk assessment, developing a regime for VASPs (i.e., registering/licensing or prohibiting VASPs) and implementing the Travel Rule (see Figure 1.3). These issues are therefore explored in more detail in this report (either below or in Section 2). Many jurisdictions seemingly do not know where to start when it comes to regulating the VA sector for AML/CFT. For example, while authorities may be aware of the FATF requirement to conduct a risk assessment, they may not know what information, data, or methodology to use for this analysis. This is particularly the case for lower capacity jurisdictions and/or those with shortcomings in general AML/CFT regulation and supervision. In response, the FATF's VACG has promoted and encouraged compliance through developing guidance, reports, and Q&A documents; participating in training and outreach and presenting on R.15; holding a specific VASP Supervisors' Forum in January 2020; maintaining and sharing supervisory contact information and links to regulation, guidance and enforcement action; and engaging with the private sector. In addition, if jurisdictions still require assistance after reviewing available material, several jurisdictions have offered to provide assistance to support jurisdictions in implementing R.15. In line with the FATF's roadmap to improve R.15 compliance, jurisdictions, particularly those in the FATF and VACG, should continue efforts to provide information, expertise-sharing and technical assistance. In all cases, jurisdictions should begin by assessing their risks, which serves as a necessary foundation for effective risk-based regulation and supervision. Jurisdictions must assess risk even where a VA/VASP prohibition is in place.

Figure 1.3. Compliance with individual R.15 criteria (as of April2023)[1]

Based on the assessment results for 98 jurisdictions, as of April 2023



For details on R.15 criteria see *FATF Methodology for assessing compliance with the FATF Recommendations*, www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html

Table 1.2. FATF Assessment Methodology for requirements on VAs/VASPs

R15.3	Risk assessment and application of a risk-based approach
R15.4	Licensing/Registration of VASPs
R15.5	Identification of natural persons or legal entities that conduct VASP activities
R15.6	Supervision/Regulation of VASPs to ensure AML/CFT compliance
R15.7	Establishment of guidelines which assist VASPs in AML/CFT compliance
R15.8	Sanctions compliance
R15.9	Preventative AML/CFT measures including the Travel Rule
R15.10	Targeted Financial Sanctions compliance
R15.11	International cooperation

Source: FATF Methodology for assessing compliance with the FATF Recommendations, available at: www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html

Challenges assessing ML/TF risks of VAs and VASPs

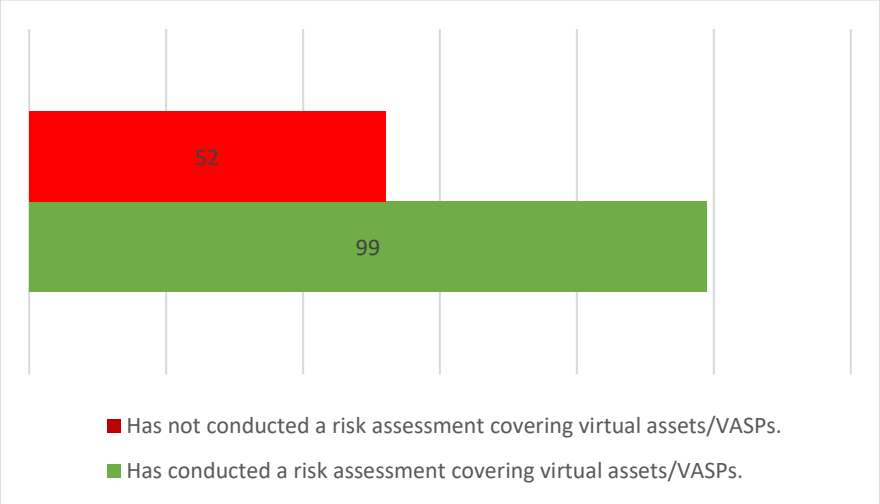
6. As in 2022, jurisdictions continue to face challenges assessing and mitigating the ML/TF risks emerging from VAs and VASPs (see Figures 1.3 and 1.4). Based on mutual evaluation and follow-up results, 71 of 98 jurisdictions (72%) are not sufficiently implementing this requirement.[13] This aligns with the results of the FATF's March 2023 survey of the global network, in which 52 of 151 jurisdiction

[13] I.e., Criteria 15.3 is rated *not met* or *partially met*.

respondents (34%) reported not having conducted a risk assessment on VAs and VASPs. Jurisdictions report two common challenges undertaking a risk assessment: first, a lack of reliable and easily available data (e.g., on VA usage, the VASP population, the extent of suspicious or illicit transactions, etc.); and secondly, limited guidance or methodologies on conducting such a risk assessment. To address these challenges, the FATF has developed and shared resources that jurisdictions should consult to identify and assess the risks posed by VAs and VASPs emanating from or impacting on their jurisdiction. Jurisdictions are encouraged to refer to the FATF's 2021 guidance, which includes factors that jurisdictions should consider in undertaking a VA risk assessment [14]. In addition, jurisdictions could consult the FATF's Community Workspace on Virtual Assets which includes several examples of VA risk assessments[15].

Figure 1.4. Has your jurisdiction conducted a risk assessment of VAs/VASPs?

Based on 151 survey results, as of April 2023.



Challenges developing, implementing and enforcing a regime for VASPs

7. Many countries are still in the process of deciding what approach to take to the VA sector (see Figure 1.5). Almost one third of survey respondents (45 of 151 jurisdictions) reported that they had not yet decided if and how to regulate the sector. Most jurisdictions (90 of 151 respondents) have decided to permit the use of VAs and operation of VASPs. The proportion of jurisdictions that opted to prohibit VASPs has increased slightly over the last year, rising from 7% of survey respondents in 2022 to 11% in 2023 (16 jurisdictions), although this may also be impacted by the increased number of survey respondents (98 in 2022 and 151 in 2023). The survey responses indicated that a prohibition approach appears to be more common in certain regions.

[14] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, paras.31-43.

[15] The workspace is available to all members of the global network. To request access, authorities should contact their lead ministry or authority in their country's delegation to the FATF, or their FSRB's Secretariat.

As shown in Figure 1.6, members of MENAFATF (Middle East and North Africa region) and APG (Asia Pacific region) are more likely to opt for a prohibition approach.

Figure 1.5. What is your jurisdiction's approach to VAs and VASPs?

Based on survey results of 151 jurisdictions, as of April 2023

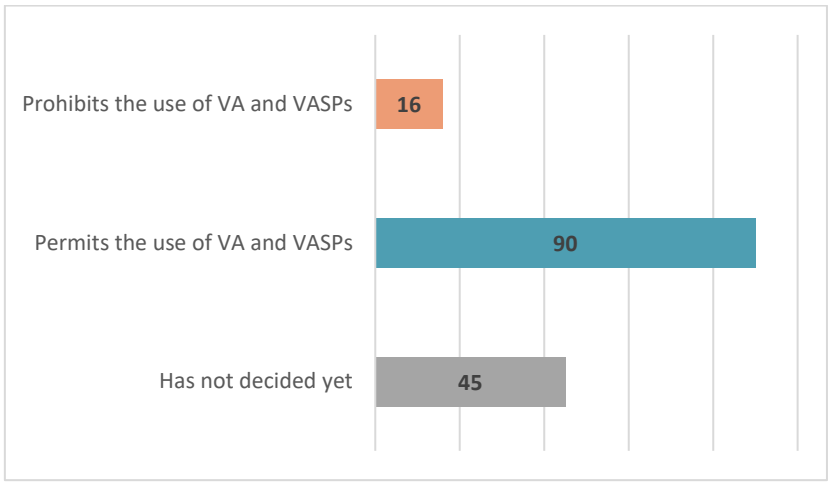
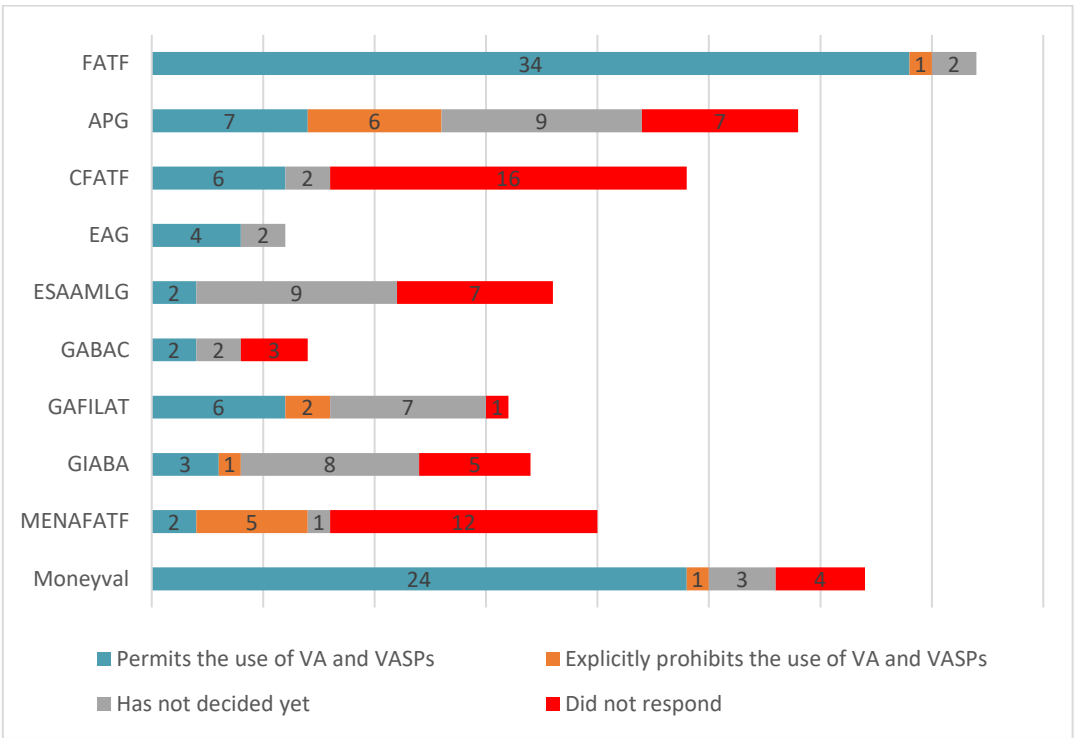


Figure 1.6. Approach to VA and VASPs by FATF/FSRB

Based on survey results of 151 jurisdictions, as of April 2023



8. There are many factors beyond ML/TF concerns that may impact a jurisdiction's decision to regulate or prohibit VASPs. The IMF comprehensively considered these factors in its February 2023 paper *Elements of Effective Policies for Crypto Assets* (see Annex A). Some jurisdictions, however, appear to be opting for a prohibition approach not based on risk, but on the assumption that prohibition requires fewer resources or is easier to manage than creating and enforcing a licensing/registration and supervisory regime[16]. A large percentage (38%; 6 of 16 jurisdictions) of jurisdictions that report prohibiting VASPs have done so *without* having undertaken any assessment of the risks relating to VAs and VASPs in their jurisdiction. Only one jurisdiction prohibiting VASPs identified them as high risk.

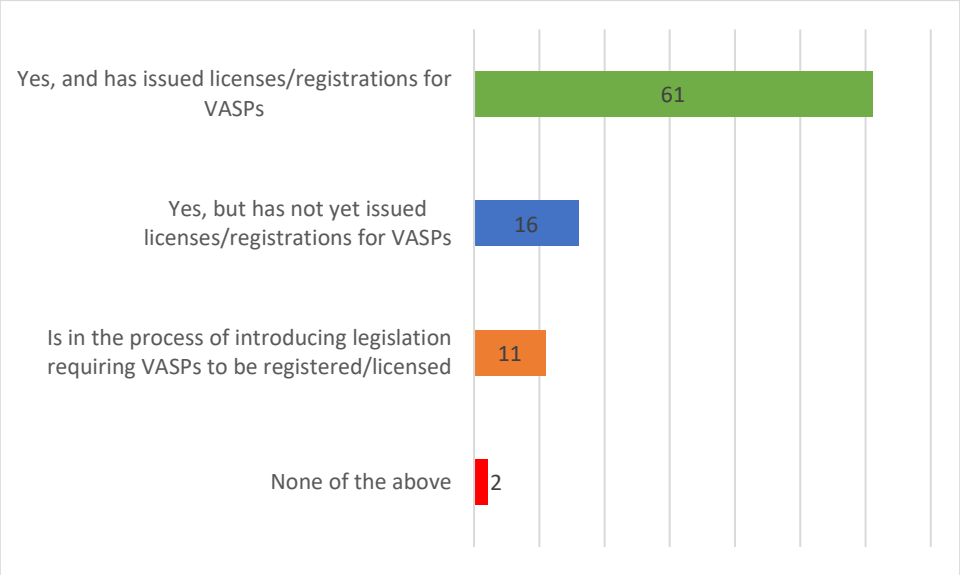
9. Assessment results indicate that successfully prohibiting VASPs is difficult; only one jurisdiction taking this approach has been assessed as largely compliant with the FATF requirements. No jurisdiction received a fully compliant rating. To effectively implement a prohibition approach, jurisdictions must undertake a comprehensive risk assessment (to identify the VASP population and determine if prohibition is appropriate), actively identify and sanction unauthorised VASP activity, and have strong and effective mechanisms for international co-operation to help detect and respond to prohibited activity. As noted above, many jurisdictions with a prohibition approach have not undertaken a risk assessment. In addition, a significant portion (44%;7 of 16 jurisdictions) of prohibition jurisdictions have not taken any supervisory or enforcement action to sanction illegal VASPs operating within their jurisdictions.

10. Jurisdictions also face challenges licensing or registering VASPs, both in law and in practice. Assessment results indicate that only 30% of assessed jurisdictions (29 of 97) satisfactorily require VASPs to be licensed or registered (i.e., criteria 15.4 is rated *met* or *mostly met*; see Figure 1.3). This figure is slightly better in the self-reported survey, with 51% of respondents (77 of 151 respondents) reporting that they require VASPs to be licensed or registered. Fewer jurisdictions (40%; 60 of 151 respondents) report having licensed or registered a VASP in practice. Of jurisdictions who assessed VAs/VASPs as high risk (and who do not take a prohibition approach), 16% (6 of 38 respondents) do not yet have legislation in force requiring VASPs to be registered/licensed. Unlicensed or unregistered VASPs operating in jurisdictions without a licensing or registration regime create ML/TF risks, as they are subject to minimal or no oversight or AML/CFT requirements. These VASPs are vulnerable to abuse by illicit actors, and their lack of effective AML/CFT obligations complicates law enforcement efforts to address abuse. Licensed or registered VASPs may also face increased challenges obtaining and verifying information on unlicensed or unregistered VASP counterparties. Those challenges can reduce the effectiveness of risk mitigation measures and the ability of a VASP to fulfil their own AML/CFT obligations (see Section 2 below).

[16] Under the FATF Standards, jurisdictions that take a prohibition approach are exempt from implementing the full suite of R.15 requirements (e.g., licensing/registration of VASPs, supervision of VASPs, applying AML/CFT preventive measures to VASPs, etc.). See the FATF Methodology, footnote 44.

Figure 1.7. Does your jurisdiction have legislation in force requiring VASPs to be registered/licensed?

Based on survey results of 90 jurisdictions, as of April 2023



11. Jurisdictions that face difficulties in licensing/registration often have shortcomings in supervision and sanctioning for non-compliance, perhaps indicating an overall lack of capacity as an underlying challenge. Few jurisdictions (36%; 35 of 98 jurisdictions) were assessed to have adequate supervision or monitoring systems in place. A similar number (34%; 33 of 98 jurisdictions) had proportionate and dissuasive sanctions available for VASPs (including their directors and senior management) that breach AML/CFT requirements (see Figure 1.3, criterion 15.8 above). Only a similarly low proportion (25%; 34 of 98 jurisdictions) have effective requirements in place to ensure VASPs complied with targeted financial sanctions requirements (see Figure 1.3, criterion 15.10 above).

12. Jurisdictions that have successfully established a registration or licensing regime, are making relatively good progress in supervising and enforcing VASPs' AML/CFT obligations. Over three quarters of jurisdictions that permit VASPs report having conducted a supervisory inspection or have included VASPs in their current inspection plan (68 of 90 respondents). A reasonable number (61%; 55 of 90 respondents) have also taken enforcement actions or other supervisory action against VASPs that failed to comply with their obligations.

13. Regardless of the approach taken (either licensing/registering or prohibiting VASPs), jurisdictions should commence or continue monitoring or supervising their VASP population and enforcing compliance.

SECTION TWO:
Implementation of FATS's Travel Rule

14. The Travel Rule applies the FATF's wire transfer requirements (FATF Recommendation 16) to the VA context. The Travel Rule requires VASPs and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when transferring VAs.

Box 2.1. What is the purpose of the FATF's Travel Rule?

The Travel Rule is a key AML/CFT measure that enables VASPs and financial institutions to prevent terrorists, money launderers, and other criminals from accessing wire transfers to move their funds (including VAs), and to detect such misuse when it occurs. Specifically, these requirements ensure that basic originator and beneficiary information is available to:

- law enforcement authorities to detect, investigate and prosecute terrorists or other criminals, and trace their assets;
- financial intelligence units to analyse suspicious or unusual activity; and
- ordering, intermediary and beneficiary VASPs and financial institutions to identify and report suspicious transactions, and to freeze funds and prevent transactions with sanctioned persons or entities.

Source: FATF Recommendations, Interpretive Note to Recommendation 16

Overall status of jurisdiction implementation and enforcement of the Travel Rule

15. Since the FATF's last targeted update in June 2022, jurisdictions have made limited progress implementing and enforcing the FATF's Travel Rule. Based on the April 2023 survey, 54% of respondents (73 of 135 respondents, excluding those that prohibit VASPs) have thus far taken no steps towards Travel Rule implementation. This group is expected to be even larger in reality as it is likely that the additional 54

jurisdictions that did not respond to the FATF's survey in 2023 have not made progress implementing the Travel Rule [17].

16. According to survey responses, a total of 35 jurisdictions have passed legislation/regulation to implement the Travel Rule and 27 are in the process of adopting legislation/regulation (e.g., have tabled draft legislation, issued a draft law, undertaken public consultations on draft legislation, etc.). This is insufficient progress since 2022 (when 30 jurisdictions had passed legislation and 25 were in the process of doing so). It is a concern that, two-thirds (25 of 38 respondents) of the jurisdictions who assessed VAs/VASPs as high risk and do not take a prohibition approach have not yet passed legislation implementing the Travel Rule. The situation is evolving, with some progress being made since the survey; for example, the European Union passed legislation that establishes a regulatory framework for VASPs [18] and implements the travel rule.[19] This brings the number of jurisdictions that have passed legislation or regulation to implement the travel rule to 58, reflecting more significant progress since 2022, although global compliance remains unsatisfactory. As in 2022, enforcement of the Travel Rule remains weak. Only 21% of jurisdictions (13 of 62[20] respondents) indicated that they had issued supervisory findings or directives, or taken enforcement actions or other supervisory actions against VASPs focused on Travel Rule compliance.

17. The lack of progress in this area is a serious concern as the nature of the Travel Rule means that its effectiveness depends on consistent, global implementation and enforcement. The FATF urges jurisdictions to make immediate progress to enact and enforce legislation implementing the Travel Rule.

[17] On the basis of assessment results, the 2022 report hypothesised that the level of progress of non-responsive jurisdictions was likely minimal. The 2023 survey results confirm this hypothesis; the response rate has been much higher, but new respondents generally report little progress.

[18] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance).

[19] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance).

[20] Only the 35 jurisdictions which have passed legislation/regulation to implement the Travel Rule and 27 which are in the process of adopting legislation/regulation were asked to provide responses relating to Travel Rule enforcement.

Figure 2.1. Has your jurisdiction passed the Travel Rule for VASPs?

Based on survey results of 135 jurisdictions, as of April 2023

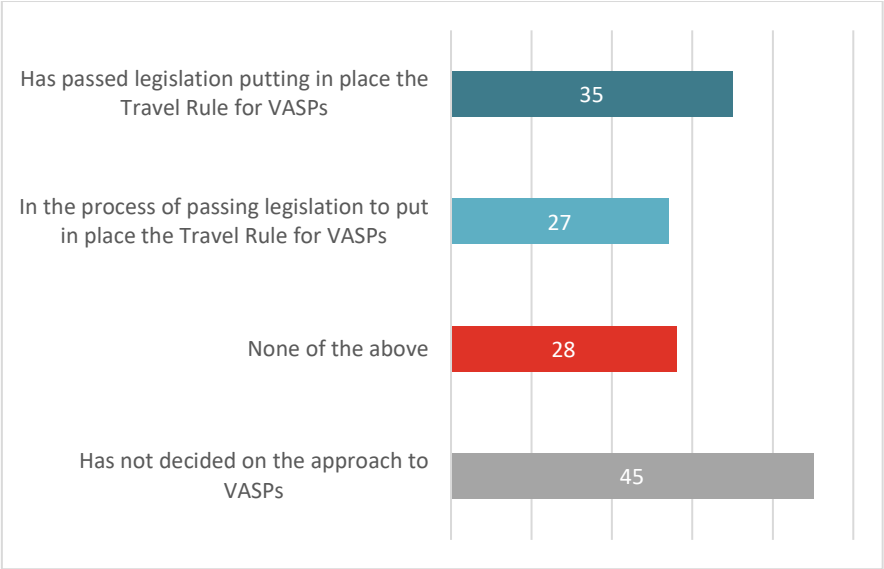
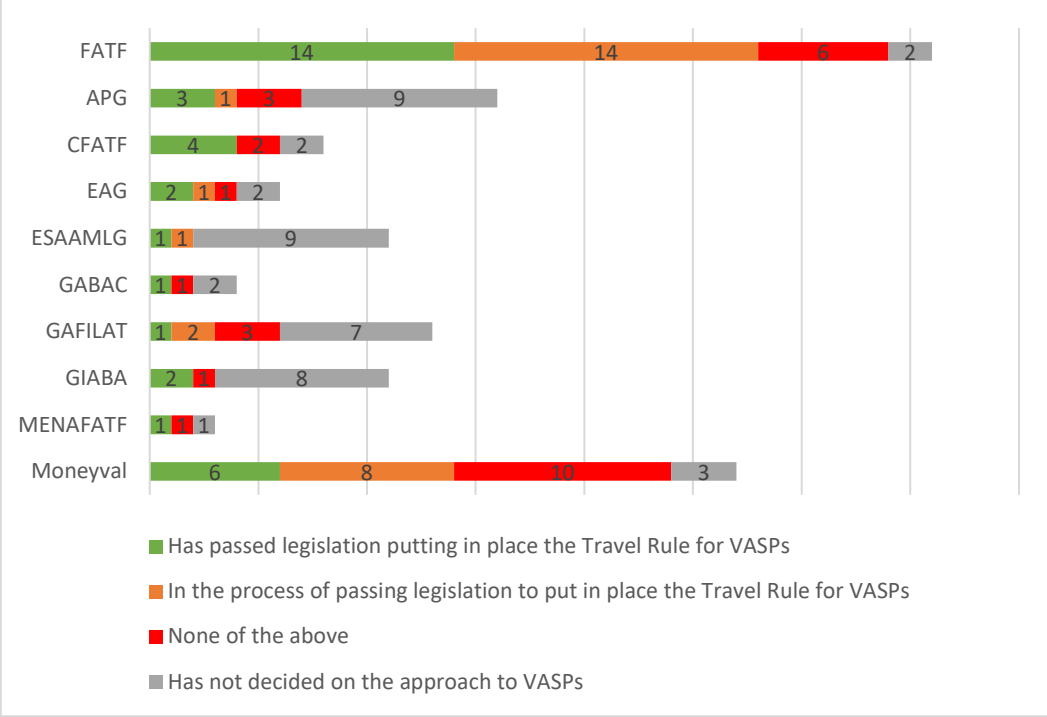


Figure 2.2. Implementation of the Travel Rule by FATF/FSRB

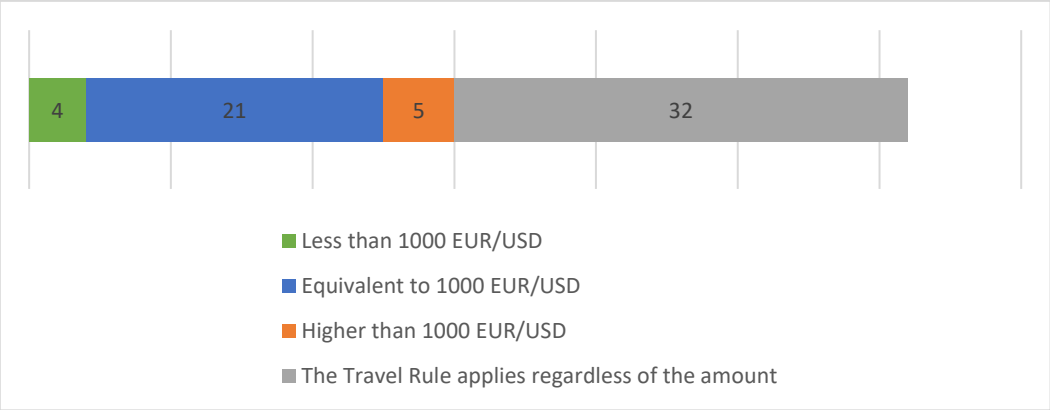
Based on survey results of 135 jurisdictions, as of April 2023



Public and private sector challenges and solutions in Travel Rule implementation

Figure 2.3. Does your jurisdiction take a threshold approach to Travel Rule implementation?

Based on survey results of 62 jurisdictions, as of April 2023



18. Jurisdictions and VASPs face a range of challenges implementing the Travel Rule. For many jurisdictions, the source of these challenges is the same as those experienced when implementing other R.15 requirements, e.g., a lack of resources, technical expertise and capacity, as well as potentially a lack of recognition of urgency.

Differences in jurisdiction requirements and the sunrise issue

19. The VASP industry reports that differences between national Travel Rule requirements can prove challenging. Based on survey responses, a majority of jurisdictions have the same requirements regarding the information that the ordering and beneficiary VASP must collect and submit (name and physical address). However, national requirements vary regarding the beneficiary information that must be collected and submitted. Survey results also identified several jurisdictions that required the ordering VASP to collect additional information for risk mitigation purposes. The FATF Standards permit variation in general, provided the minimum requirements are met. Further, complete global harmonisation is unrealistic given differences in national frameworks, risk profiles, contexts, and approaches to risk mitigation. A lack of harmonisation also exists across other sectors such as correspondent banking. Authorities should ensure that domestic regulations meet the FATF's minimum requirements and that national requirements are clear, and should consider harmonisation where possible and helpful for risk mitigation. Authorities should also continue to co-ordinate across jurisdictions on how to deal with common challenges, and should support the private sector in its responsibility to adopt tools that can accommodate national differences.

20. Delays in implementation and different timelines for enforcement of the Travel Rule across jurisdictions results in what is commonly referred to as the 'sunrise issue'. This issue continues to cause challenges for the private sector given the inherently borderless and international nature of virtual assets. Compliance with the Travel Rule requires that both the ordering and beneficiary VASPs collect information on their customers and be able to transmit, receive, and sufficiently protect this information. Given that many jurisdictions have not yet implemented the

Travel Rule, it is unlikely that both VASPs involved in any given transaction will have national requirements to comply with these obligations. Until all VASPs are required to implement the Travel Rule, VASPs operating in or from jurisdictions with Travel Rule obligations will continue to face challenges executing all covered transactions in a compliant manner.

21. Jurisdictions that have implemented the Travel Rule continue to take a range of approaches to deal with the sunrise issue, many of which were covered in detail in the FATF's June 2022 report. As in 2022, of jurisdictions that have implemented the Travel Rule or are in the process of doing so, 13% (8 of 62 respondents) are taking a phased approach to implementation (e.g., only requiring VASPs to implement the Travel Rule in certain circumstances, setting a higher transaction amount threshold for Travel Rule requirements to apply, or permitting manual data processing with short delay for transmission of Travel Rule implementation). Other jurisdictions (18%; 11 of 62 jurisdictions that have implemented the Travel Rule or are in the process of doing so) have allowed a grace period for Travel Rule compliance, during which there are exemptions or flexibility in how VASPs are expected to comply.

22. Additionally, some jurisdictions qualify how domestic VASPs can interact with foreign counterparts. Of jurisdictions implementing the Travel Rule, about half have measures in place to ensure domestic VASPs are transacting with regulated and/or Travel Rule compliant counterparts, or otherwise taking steps to mitigate the risks associated with VASPs that lack AML/CFT obligations. Measures include permitting domestic VASPs to transact only with licensed/registered foreign counterparts (3 of 62 respondents); allowing domestic VASPs to transact only with licensed/registered and Travel Rule compliant foreign counterparts (13 of 62 respondents); allowing domestic VASPs to transact with foreign VASPs that are licensed/registered in specific jurisdictions and/or complying with the Travel Rule (3 of 62 respondents); or permitting VASPs to transact with unlicensed/unregistered foreign counterparts but only where risk mitigating measures are taken (11 of 62 respondents). However, a significant portion of jurisdictions (17 of 62 respondents) that have implemented the Travel Rule or are in the process of doing so allow domestic VASPs to transact with any foreign VASP, regardless of licensing/registration, Travel Rule compliance, or related risk mitigating measures.

23. The sunrise issue will only be resolved with widespread implementation of the FATF Standards on VAs and VASPs, including the Travel Rule. This highlights the importance of the FATF's work to accelerate implementation of R.15. The FATF calls on all jurisdictions to rapidly enact and enforce the Travel Rule.

VASP counterparty due diligence

24. For a VASP to transmit the required Travel Rule information, they need to identify and conduct due diligence on their counterparty VASP or financial institution.[21] Discussions with the public and private sectors indicate that this remains a challenge. As noted above, the survey results show that many jurisdictions

[21] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, para.169, 196. Counterparty due diligence ensures VASPs avoid dealing with illicit or sanctioned actors and provides assurance that a counterparty can comply with the Travel Rule, including protecting the confidentiality of shared information. Note that counterparty due diligence for the purpose of complying with R.16 is distinct from the obligations applicable to cross-border correspondent relationships (R. 13).

allow domestic VASPs to transact with foreign VASPs that are not licensed/registered and/or do not comply with the Travel Rule. This demands additional risk mitigation measures for the private sector to avoid submitting customer data to inappropriate counterparties. VASPs struggle to effectively conduct due diligence on counterparty VASPs that are unlicensed/unregistered and/or with weak levels of compliance.

25. VASPs cited difficulties in readily identifying counterparty VASPs that were not registered/licensed or obtaining information on the VASP. This information includes the VASP's ability to securely hold Travel Rule information; whether it was tied to illicit actors or sanctioned persons; and the VASP's level of AML/CFT compliance. In some cases, VASPs have challenges identifying licensed/registered VASPs. This can result from both the lack of public information on licensed or registered VASPs (e.g., through a database or public register of licensed/registered VASPs), as well as the design of some Travel Rule compliance tools that are only able to identify counterparties that are subscribers to that particular tool. To facilitate counterparty due diligence in line with R.16 as well as R.13[22], jurisdictions are encouraged to maintain and publicise information on VASPs that are registered or licensed in their jurisdiction. Shortcomings with Travel Rule compliance tools can also impact a VASP's ability to conduct counterparty due diligence, as is explored in the next section.

Issues with Travel Rule compliance tools

26. When the Travel Rule for VASPs was included in the FATF Standards in 2019, the tools to allow VASPs to comply with the Travel Rule (and similar national requirements) had largely not been developed. The VA industry has responded to the FATF Standards on VAs and VASPs by developing a range of compliance tools that allow VASPs to collect information on the originator and beneficiary to a transaction and provide this information to the VASP at the other end of a transaction. However, these compliance tools face two key challenges: compliance with the FATF Travel Rule requirements, and friction related to the lack of interoperability between Travel Rule compliance tools.

27. At present, many of the compliance tools fall short of the FATF Standards. As set out in Table 2.1 below, examples of shortcomings include transmitting the information after the on-chain VA transaction. To comply with their freezing obligations in practice, VASPs must submit Travel Rule information in sufficient time for both institutions to conduct sanctions screening, identify any designated persons/entities, and freeze funds before any sanctioned actor can access or dissipate the funds. Given the speed of a VA transaction, this means information must be submitted simultaneously or before the transaction is executed.[23]

28. Both the public and private sectors can help avoid the largescale adoption of non-compliant tools. Some jurisdictions and the VACG are engaging with VASPs to identify commonly used compliance tools and ensure these meet all the FATF requirements, and with compliance tool providers to identify possible shortcomings

[22] R.13 requires institutions to conduct due diligence on institutions with which they have a correspondent banking or other similar relationship, e.g., providing VASP services to another VASP. This includes understanding the nature of the respondent's business, obtaining information the reputation of the institution and the quality of supervision, and assessing the respondent's AML/CFT controls.

[23] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, para.185, 187

and impress the importance of complete implementation of the FATF requirements. Policymakers can also signal the importance of compliance with the FATF Standards. For cases in which shortcomings in Travel Rule compliance tools persist, competent authorities can alert and warn VASPs of non-compliant tools operating within the jurisdiction, remind VASPs to only use compliance tools that meet the FATF requirements, and/or take supervisory or enforcement action as appropriate. VASPs themselves should be cautious in selecting any compliance tool provider and take steps to ensure their provider will allow them to meet all FATF Travel Rule requirements. Box 2.2 below sets out guiding questions that VASPs should ask to determine whether potential Travel Rule compliance tools will comply with all FATF requirements.

Table 2.1. Examples of shortcomings in available Travel Rule compliance tools

Shortcoming	FATF Requirements on VASPs	Reference to FATF Standards
Tool permits VASP to transmit a transaction ID instead of the originator's wallet address	VASPs must transmit the originator's wallet address or customer account number where such an account is used to process the transaction.	Interpretive note to Recommendation 16, para.6(b)
Tool does not require an ordering VASP to collect and submit beneficiary information, and may instead ask the ordering VASP to obtain this information solely from the beneficiary VASP.	Ordering VASPs must provide required beneficiary information immediately and securely. Beneficiary VASPs must obtain and retain that data. Beneficiary VASPs must confirm that beneficiary information received is sufficient. Reasonable measures are required by the beneficiary VASPs to identify the VA transfers that lack required information.	Interpretive note to Recommendation 15, para.7(b)
Tool does not require VASP to send information immediately or before the transaction is executed	Ordering VASPs must submit originator and beneficiary information to the beneficiary VASP or financial institutions "immediately", which means prior, simultaneously or concurrently with the transfer itself (to permit sanctions screening and ensure funds are not made available to sanctioned persons/entities).	Interpretive note to Recommendation 15, para.7(b)
Tool does not permit the VASP to transmit information for transactions involving all types of VA and/or transactions of any amount	Accurate information must be transmitted for transactions over USD/EUR 1000 involving any type of VA or fiat currency. While some jurisdictions may choose to implement the Travel Rule at a lower threshold, VASPs must still submit the name of originator and beneficiary as well as the wallet address, although such information need not be verified unless there is a ML/TF suspicion or where required by the jurisdiction.	Interpretive notes to Recommendation 16, para.5(a)
Tool does not permit VASP to download or otherwise retain transmitted information (for recordkeeping or transaction monitoring purposes)	VASPs must "hold" originator and beneficiary information and be able to "make it available on request to appropriate authorities".	Interpretive note to Recommendation 15 Recommendation 11
Tool does not enable a VASP to locate a counterparty VASP for all VA transfers and provide a communication channel for the purpose of due diligence	VASPs must identify their counterparty VASP to transmit required Travel Rule information securely and in line with data protection/privacy requirements, and conduct due diligence to avoid unknowingly dealing with a counterparty VASP that is an illicit or sanctioned actor.	FATF 2021 Guidance (R.13 and R.16 sections)

Source: FATF Standards; VACG analysis led by Japan of five major Travel Rule compliance tools.
Note: For more detail, see FATF (2021) Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

29. In addition to compliance, Travel Rule compliance tools face challenges of interoperability and at present, there is only very limited interoperability among Travel Rule compliance tools, which can limit the ability of tools to meet the FATF Standards. A lack of interoperability could limit the ability of VASPs to send Travel Rule information to a VASP using a different tool. VASPs are therefore only able to process transactions for VASPs using the same tool or must use multiple tools to enable global transfers.

30. According to some compliance tool providers, issues relating to data protection and privacy and/or VASP counterparty due diligence may warrant limited interoperability. Specifically, the rationale is that compliance tool providers may screen users of their tool to ensure adequate data protection controls or even a level of counterparty due diligence. Compliance tool providers may therefore consider that allowing information sharing only between their users (i.e., no interoperability) will prevent information being shared with unreliable counterparties (e.g., illicit users or those with insufficient data protection controls). The challenge with this approach is that, as set out in the FATF's 2021 Guidance[24], VASPs are required to independently assess counterparty risk. While this approach may provide potential opportunities to simplify some aspects of counterparty due diligence (e.g., facilitating the identification of a counterparty VASP), it does not remove the need for VASPs to independently verify the information and ensure all relevant domestic obligations are met.

31. While not explicitly required to meet the FATF standards, interoperability would be valuable and could improve the effectiveness of the Travel Rule by ensuring that VASPs around the world are able to securely and systematically transmit required information. Interoperability will also enable VASPs to lower compliance costs by reducing the need for acquiring multiple compliance tools. Progress is being made in this area, although it remains slow. Some private sector participants have noted that a siloed approach is more profitable for the compliance tool providers, although other industry participants are developing Travel Rule compliance tool aggregators to provide broader coverage amongst VASPs using different tools.

32. Interoperability is not a precondition for implementation or enforcement of the Travel Rule at the jurisdiction level. In the absence of interoperability, VASPs can comply with the Travel Rule by sending back VAs for transactions with VASPs that are using non-interoperable tools, quarantining VAs until appropriate information can be collected, or investing in multiple tools to permit a broader scope of transactions (noting that this comes with cost implications). Some jurisdictions consider that enforcement of the Travel Rule may be a necessary step to push progress in this area by driving demand by VASPs for compliance tool providers to develop more efficient compliance tools. The FATF urges the private sector to progress towards interoperability, whether through technological advancements that allow interoperability between tools or by developing relationships that permit transactions to be made through a chain of interoperable tools.

[24] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, paras.286-292.

Box 2.2. Guiding questions for Travel Rule compliance tool providers

The below questions may be useful to help VASPs and jurisdictions engage with Travel Rule compliance tool providers. This is not an exhaustive list, but instead a compilation of questions that jurisdictions have found useful in engaging with compliance tool providers and fostering tools that meet the FATF requirements. The purpose of the Travel Rule is to ensure institutions have sufficient information to identify customer and transaction risks and take appropriate action to mitigate these risks. VASPs and jurisdictions should also consult the more comprehensive information in the FATF's 2021 Guidance and the 2022 Targeted Update (including questions on interoperability).

Timing and scope of Travel Rule data submission

- Does the tool enable VASPs to submit Travel Rule data for small value VA transfers (i.e., below USD/EUR 1 000) to accommodate varying threshold requirements across jurisdictions?
- Does the tool cover all VA types?
- Does the tool enable beneficiary VASPs to obtain and handle a reasonably large volume of transactions from multiple destinations in a secure and stable manner?
- Does the tool enable ordering VASPs to submit the required and accurate originator and required beneficiary information to beneficiary VASPs immediately upon or prior to a VA transfer on a blockchain/distributed ledger technology platform?

Counterparty VASP identification and due diligence

- Does the tool enable an ordering VASP to locate the counterparty VASP for VA transfers? (This is not a mandatory tool function but identifying the counterparty can be the first challenge for ordering VASPs).
- Does the tool provide VASPs with a communication channel to help follow-up with a counterparty VASP to:
  - seek information on the counterparty VASP to allow the VASP to conduct required counterparty due diligence; and
  - request information on a certain transaction to determine if the transaction involves high-risk or prohibited activities?

Record-keeping and transaction monitoring

- What function does the tool provide to facilitate meeting record-keeping, transaction monitoring, and reporting obligations (e.g., securely retaining data for 5 years/ allow user VASPs to download data), while being in line with national data protection requirements?

Questions on interoperability with other Travel Rule compliance tools

- Does the tool allow Travel Rule information to be submitted to VASPs using different tools?

SECTION THREE:
Market Developments and Emerging Risks

Use of VAs for proliferation and terrorist financing

33. There are serious concerns about the threat posed by the DPRK's illicit VA-related activities to finance the proliferation of weapons of mass destruction (WMDs), enabling an unprecedented number of recent launches of ballistic missiles (including inter-continental ballistic missiles). In March 2023, the UN Panel of Experts for North Korea (UNSCR 1874) issued a report on funding streams for DPRK. Previous reports have indicated that the DPRK has resorted to illicit activities, including cyber-enabled heists from VASPs and financial institutions, to generate revenue for its unlawful WMD and ballistic missile programs and the newest report emphasises that this trend continues unabated. The report found that "a higher value of [virtual] assets was stolen by Democratic People's Republic of Korea actors in 2022 than in any previous year. The jurisdiction used increasingly sophisticated cyber techniques both to gain access to digital networks involved in cyber finance and to steal information of potential value, including to its weapons programmes."[25] The report found that DPRK cybercriminals used spear-fishing and other malware campaigns to infect victim devices to steal VAs. In addition to VA theft, the report also noted that DPRK engaged in ransomware attacks to extort payments in VA in exchange for restoring encrypted files and separately generated revenue from the creation of fraudulent non-fungible tokens.

34. These findings are supported by analysis by blockchain analytics firms as well as by the Republic of Korea, which found that that DPRK actors stole VAs worth USD 1.2 billion globally since 2017, including USD 630 million worth of VAs in 2022[26]. One delegation noted that DPRK also generated revenue in virtual assets through information technology (IT) workers. DPRK IT workers typically use fake personas to apply for jobs at companies and some request to be paid in VAs. Most of their salaries is sent back to DPRK through a complicated laundering pattern[27].

---

[25] UN Security Council (March 2023) S/2023/171 "Letter dated 3 March 2023 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council", pgs.4, 74-78.

[26] AP News (22 December 2022) "Seoul: North Korean hackers stole $1.2B in virtual assets".

[27] U.S. Department of the Treasury (24 April 2023) "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs", available at: https://home.treasury.gov/news/press-releases/jy1435; U.S. Department of the Treasury Office of Foreign Assets Control (15 May 2022) "Publication of North Korea

35. Both the scale of the funding and the serious consequences of proliferation financing render this a significant threat and delegations agreed that these risks required urgent action by countries across the global network to implement R.15. The FATF echoes the UN Panel of Experts call for jurisdictions to urgently implement the FATF Standards on VAs and VASPs and take other appropriate actions to mitigate the risks of proliferation financing through VAs.

36. The FATF has also observed an increase in the use of VAs, including anonymity enhanced coins/cryptocurrencies (AECs), for terrorist financing. In October 2022 and February 2023, the FATF's regular update on the financing of ISIL, Al Qaeda and affiliates noted a shift towards the use of VAs, including AECs. For example, various sources have identified ISIL-related websites soliciting funds in Monero.[28] Jurisdictions report that ISIL, Al Qaeda and affiliates are increasingly using VAs to raise and move funds in Africa, Europe and the Middle East, although these groups remain primarily reliant on more traditional financing methods. FATF work has also identified VA use as a typology for the financing of extreme right-wing terrorism, often via crowdfunding platforms[29]. This is a concerning trend that that FATF will continue to monitor.

Decentralised Finance (DeFi)

37. The FATF's 2022 report concluded that DeFi markets had grown significantly. This trend has generally continued throughout late 2022 and early 2023. There was a spike in DeFi trading volume in late 2022, with an increasing number of users turning to decentralised exchanges (DEXs) and decentralised applications (dApps) following the high-profile collapse of one centralised exchange.[30] Nonetheless, several jurisdictions noted that DeFi arrangements still account for a relatively low percentage of overall VA activity. One jurisdiction identified that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or otherwise outside the virtual asset ecosystem via more traditional methods[31].

38. Even so, jurisdictions recognise that DeFi remains an evolving market that can pose illicit finance risks as exemplified by the more than USD 1.1 billion stolen by DPRK actors in 2022 from DeFi arrangements.[32] The FATF will continue to work on

---

Information Technology Workers Advisory", available at: https://ofac.treasury.gov/recent-actions/20220516.

28 UN CTED (23 September 2022) "Trends in the financing of the so-called terrorism motivated by xenophobia, racism and other forms of intolerance with the misuse of new technologies"; Cointelegraph (25 June 2020) "ISIS-Affiliated News Website to Collect Donations with Monero"

29 FATF (2021) *Ethnically or Racially Motivated Terrorism Finance.*

30 DLNews (1 February 2023) "Hedge funds see bullish trends in DeFi even as Fed rate risk looms", available at: https://www.dlnews.com/articles/defi/hedge-funds-see-bullish-trends-in-defi-even-as-fed-rate-risk-looms/

31 U.S. Department of the Treasury (2023) *Illicit Finance Risk Assessment of Decentralized Finance*, pg.4. Available at: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

32 Chainalysis (1 February 2023) "2022 Biggest Year Ever for Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers". Available at: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/.

this area, including engaging with the DeFi community, VASPs and other VA stakeholders. Several jurisdictions are in the process of or just beginning a risk assessment focused on DeFi arrangements. One jurisdiction that had completed such an assessment found that threat actors misuse DeFi services to engage in and profit from illicit activity, in particular ransomware attacks, theft, fraud and scams, drug trafficking, and proliferation finance [33]. However, comprehensive DeFi risk assessments are challenging for most jurisdictions, in part due to the lack of reliable and complete data. Some jurisdictions have expressed challenges with assessing the risks of DeFi due to a lack of reliable data, and additional challenges resulting in a lack of law enforcement and enforcement cases that include DeFi.

39. While survey results illustrate some progress in mitigating illicit finance risks associated with DeFi, many jurisdictions face significant challenges. In many cases, DeFi arrangements are decentralised in name only and there are persons, entities or centralised elements that may be subject to the FATF requirements as VASPs [34]. However, it may be difficult for jurisdictions to identify whether certain entities in DeFi arrangements fall within their regulatory perimeter for VASPs and to ensure these entities comply with relevant AML/CFT requirements, including STR reporting. Private sector outreach also indicates that there is a gap in understanding between the private sector and VACG members about the types of DeFi arrangements that meet the VASP definition under the FATF Standards.

40. Focusing on jurisdictions that are relatively more advanced in regulating VASPs (i.e., those that have implemented the Travel Rule), more than half (37 of 62 respondents) reported that they require certain DeFi arrangements to be licensed or registered as a VASP (e.g., where the creator, owner or operator maintains control or sufficient influence in the arrangement). Of the remaining advanced jurisdictions (i.e., those that *do not* apply their AML/CFT framework for VASPs to DeFi entities), 40% (10 of 25 respondents) are taking steps to identify and address risks in this area (e.g., studying the risks or engaging with the private sector), 20% (5 of 25 respondents) are taking other steps (e.g., using innovation hubs to license DeFi arrangements or participating in regional work to monitor risks), and 40% (10 of 25 respondents) are not taking any specific steps or other initiatives related to DeFi.

41. As in the FATF's 2022 report, discussions with the public and private sectors indicate that identifying individuals or entities exercising control or sufficient influence over DeFi arrangements continues to be challenging. This can complicate effective supervision and enforcement. Most jurisdictions that require certain DeFi arrangements to be licensed or registered as a VASP have not identified any unregistered/unlicensed DeFi entities that qualify as VASPs (27 of 37 respondents). This may indicate the difficulties jurisdictions face in identifying DeFi entities, and challenges in ensuring these entities comply with relevant AML/CFT requirements, including STR reporting. Based on survey responses, only nine jurisdictions report having successfully identified unlicensed/unregistered DeFi entities that qualify as VASPs and/or report taking supervisory or enforcement action against DeFi entities (see Box 3.1). Only one jurisdiction stated that it had registered or licensed DeFi

[33] U.S. Department of the Treasury (2023) *Illicit Finance Risk Assessment of Decentralized Finance*, pg.5. Available at: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[34] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, paras.67-69. Individuals or entities who exercise control or influence over a DeFi arrangement would be captured as VASPs under the FATF Standards.

entities as VASPs in practice. This further confirms the difficulties jurisdictions face in identifying regulated entities in DeFi arrangements and determining whether they qualify as VASPs.

Box 3.1. Case study: Commodity Futures Trading Commission (CFTC) imposes penalty against bZeroX, LLC and its founders, and chargers its successor Ooki DAO

The US CFTC in September 2022 issued an order simultaneously filing and settling charges against a company, bZeroX LLC, and its two founders for illegally offering leveraged and margined retail commodity transactions in digital assets; engaging in activities only registered futures commission merchants (FCM) can lawfully perform; and failing to adopt a customer identification program as part of a Bank Secrecy Act compliance program, as required of FCMs. Simultaneously, the CFTC filed a federal civil enforcement action in the U.S. District Court for the Northern District of California charging a decentralized autonomous organisations (DAO)—the successor to the original company that operated the same software protocol—with violating the same laws as the original company and founder. Neither the original company nor the DAO maintained a required customer identification program, and the lack of AML measures was explicitly advertised as a positive feature of the service.

As part of the case, the CFTC's order found that bZeroX transferred control of the Protocol to the bZx DAO, which is now doing business as the Ooki DAO. By transferring control to a DAO, bZeroX's founders touted to bZeroX community members the operations would be enforcement-proof, allowing the Ooki DAO to violate the CEA and CFTC regulations with impunity, as alleged in the federal court action. The CFTC order found the DAO was an unincorporated association of which the two founding members were actively participating members and liable for the Ooki DAO's violations of the CEA and CFTC regulations. Similarly, in the federal court action, in upholding the CFTC's service on the Ooki DAO, the U.S. District Court for the Northern District of California held that the Ooki DAO had the capacity to be sued as an unincorporated association under applicable law.

Source: U.S Department of the Treasury (2023) Illicit Finance Risk Assessment of Decentralized Finance

42. Based on discussions, jurisdictions consider a range of sources in line with the FATF Guidance when identifying DeFi arrangements that fall under the VASP definition[35]. This includes looking at persons who hold administrative keys; persons

[35] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, para.67: "For example, there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols. Jurisdictions may wish to consider other factors as well, such as whether any party profits from the service or has the ability to set or change parameters to identify the owner/operator of a DeFi arrangement. These are not the only characteristics that may make the owner/operator a VASP, but they are illustrative. Depending on its operation, there may also be additional VASPs that interact with a DeFi arrangement."

involved in governance structures, including holders of governance tokens and/or participants in decentralized autonomous organisations (DAOs), based on concentration of influence and ability to amend, update or otherwise substantively affect the DeFi protocol; managers of applications to interface with DeFi arrangements; persons involved in promoting the DeFi arrangement and/or releasing updates to the DeFi protocol; and profit/fee structures. Some jurisdictions have issued risk assessments or guidance that provides information on how government authorities are determining control or sufficient influence over DeFi arrangements (see Box 3.1). The FATF will continue to operate as a platform to share experiences and developments in this area amongst VACG members, the FATF's global network and with the private sector, particularly to ensure existing guidance remains relevant and reflective of best practice.

Box 3.2. Identifying ownership/control: Key messages from FATF's 2021 Guidance

- Creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the FATF definition of a VASP.
- Jurisdictions need to evaluate the facts and circumstances of each individual situation to determine whether there is an identifiable person(s), whether legal or natural, providing a covered service.
- Owners/operators can often be distinguished by their relationship to the activities being undertaken. There may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols.
- Other factors to be considered to identify the owner/operator of a DeFi arrangement:
  - Whether any party profits from the service
  - Whether any party has the ability to set or change parameters

These are not the only characteristics that may make the owner/operator a VASP, but they are illustrative.

- Marketing terms or self-identification as DeFi is not determinative, nor is the specific technology involved in determining if its owner or operator is a VASP.
- Countries should apply the principles contained in the Standards in a manner that interprets the definitions broadly, but with regard for the practical intent of the functional approach.

43. The VA ecosystem is interconnected and jurisdictions need to take a holistic approach to risk assessments, to reflect the interconnectedness between DeFi arrangements, VASPs, unhosted wallets and P2P transactions.[36]

Unhosted Wallets, including Peer-to-Peer (P2P) Transactions

44. In P2P transactions, individuals transact directly with one another without intermediaries or centralised authorities with AML/CFT obligations[37]. At the time of a 2021 market analysis by FATF[38], available data indicated no clear shift away from regulated VASPs towards P2P transactions but found that the share of illicit transactions appears higher for P2P transactions compared to direct transactions with VASPs (although variations in data limited confidence in these findings). Unhosted wallets, including those used in P2P transactions, can be used to avoid AML/CFT controls, and therefore pose specific ML/TF/PF risks. These risks could potentially grow as more VASPs implement AML/CFT controls in line with the FATF Standards or if VAs, such as stablecoins, become widely used to purchase goods and services, reducing the need for covered financial intermediaries to access fiat currency[39]. In the latter scenario, actors, potentially including sanctioned actors, may be able to use illicit proceeds in VAs to perpetuate their activities without encountering a VASP or financial institution with AML/CFT obligations.

45. While P2P transactions fall outside the scope of the FATF Standards, implementation of the Standards can still play a critical role in mitigating illicit finance risks of P2P transactions and unhosted wallets. The FATF 2021 Guidance provides a menu of options[40] for how jurisdictions can address P2P transaction risks at the national level, such as improving P2P transaction market metrics and risk mitigation solutions, utilising blockchain analytics tools, and placing additional AML/CFT requirements on VASPs that allow transactions to or from non-obliged entities. At present, several delegations noted that they are assessing risk associated with P2P payments, albeit in some cases with challenges, and/or requiring VASPs to implement measures to mitigate risks associated with unhosted wallet transactions.

46. Several jurisdictions reported focusing on monitoring the risks related to P2P transactions. One jurisdiction is receiving quarterly updates on P2P transactions and another noted that they found that the percentage of transactions between VASPs and unhosted wallets was small, but relatively high risk compared to VASP-VASP

---

[36] One jurisdiction undertook and published a research report on this interconnectedness and data availability analysis with on-chain/off-chain data: Japan Financial Services Agency (2023), available at: www.fsa.go.jp/en/policy/bgin/information.html

[37] This section covers VA transfers that are conducted directly between users, without the use or involvement of a VASP or other obliged entity (e.g., VA transfers between two unhosted wallets whose users are acting on their own behalf). It does not deal with P2P exchanges or marketplaces, which facilitate transactions between users and may be captured as VASPs under the FATF Standards.

[38] FATF (2021) Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs, para.79.

[39] One blockchain analytics company has identified an outflow of funds from unhosted wallets to sanctioned entities.

[40] FATF (2021) Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paragraph 106, and "VA transfers to/from unhosted wallets"

transactions. However, even amongst jurisdictions with more advanced VASP regulations, most respondents (39 of 62) have not yet evaluated the specific risks related to unhosted wallets or P2P transactions. Many jurisdictions have encountered significant data gaps related to the size of the overall P2P ecosystem and the volume of illicit transactions, which makes it difficult for countries to effectively assess the domestic or global risks posed by P2P transactions. This appears further complicated by significant differences between jurisdictions and userbases in the use of unhosted wallet - including P2P - transactions . Both the FATF and individual jurisdictions need to continue to monitor developments in this emerging area and share jurisdiction approaches to mitigating any identified risks.

47. In addition to monitoring and assessing risks, certain regulators and VASPs are implementing measures to manage the potential risks posed by transactions with unhosted wallets, in line with the FATF's 2021 Guidance[41]. In some jurisdictions, VASPs are required to collect information about transactions to unhosted wallets to determine the level of due diligence for that particular transaction. Some regulators have included factors related to unhosted wallets as potential indicators of suspicious transactions. Discussions with the private sector indicate that some VASPs are independently categorising transactions with unhosted wallets as higher risk than transactions involving VASPs and taking enhanced due diligence measures even in the absence of a regulatory requirement to do so.

Non-Fungible Tokens (NFTs)

48. NFTs continue to pose risks for ML/TF, although some jurisdictions have seen a decrease in risk level in this area following the market boom in 2021. In February 2023, the FATF issued a report on *ML/TF in the Art and Antiquities Market*. This report highlighted the vulnerabilities of NFTs related to illicit finance and potential mitigating measures, and shared case studies of NFT misuse for ML purposes.

49. How NFTs are regulated differs between jurisdictions and depending on the type of NFT. While some NFTs may be captured under VA definitions, others may be considered and regulated as works of art or collectibles. One jurisdiction shared that they have revised supervisory guidelines to clarify whether or not a specific NFT constitutes a VA under their regime. NFTs could also emerge as tokenised versions of physical good, like real estate or precious metals. As with DeFi, authorities need to take a functional approach and look beyond the marketing associated with NFTs to determine if the product or service in question qualifies as a VA, VASP, a financial institution, or a designated non-financial business or profession.

50. Looking at survey responses, most jurisdictions that are more advanced in regulating VASPs (i.e., those that have implemented the Travel Rule) are regulating NFTs as VAs where appropriate (e.g., where NFTs are used for payment or investment purposes[42]) (40 of 62 respondents). A minority of advanced jurisdictions do not apply their AML/CFT framework to NFTs at all (22 of 62 respondents). No jurisdictions reported that NFTs were regulated as art or cultural objects.

[41] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.

[42] FATF (2021) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* clarifies that NFTs may fall under the VA definition if they are to be used for payment or investment purposes in practice.

Other market developments (stablecoins[43] etc.)

51. As the liquidity of stablecoins increases in parallel with the growth of DeFi markets, the FATF will continue to assess related ML/TF risks and challenges mitigating these risks. As noted above, mass-adoption of VAs, including stablecoins,[44] could potentially decrease the use of AML/CFT-obliged entities to transfer or custody VAs in the future.

52. Traditional financial institutions and institutional investors are increasingly participating in the virtual assets market[45]. Market participants are exploring how incumbent players and VASPs can cooperate to mitigate the ML/TF risks by incorporating years of experiences and practices from the traditional financial system. The FATF will continue to monitor market development and explore the potential role for such cooperation.

[43] So-called 'stablecoins' are not a legal or technical category and the use of this term is not intended to endorse any stability claims. Under the revised FATF Standards, a stablecoin will either be considered a virtual asset or a traditional financial asset depending on its exact nature: FATF (2020) *Report to the G20 on So-called Stablecoins*.

[44] As noted in the FATF's report to G20, stablecoins share many of the same ML/TF risks as some VAs. However, certain stablecoin projects could have greater potential for mass-adoption, which could heighten ML/TF risks. As such, while the potential for mass-adoption is a factor relevant to all VAs, it is a particularly relevant factor to consider in assessing the ML/TF risks of stablecoins.

[45] OECD (May 2022) "Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness". Available at: www.oecd.org/publications/institutionalisation-of-crypto-assets-and-defi-tradfi-interconnectedness-5d9dddbe-en.htm

SECTION FOUR:
Recommendations for the Public and Private Sectors

Recommendations for the Public Sector

Risk assessment, mitigation, and licensing/registration

53. Jurisdictions that have not yet assessed the risks of VAs and VASPs should make use of available resources, including the FATF's 2021 guidance and the Community Workspace on Virtual Assets[46], to identify the risks, and put in place risk mitigation measures, including measures to combat identified regulatory and supervisory challenges.

54. Both jurisdictions that permit VAs and VASPs and those that prohibit them should commence or continue monitoring or supervising their VASP population and enforcing against non-compliance, including sanctioning illicit VASPs.

55. In light of increasing TF and PF threats related to VAs, jurisdictions should take immediate action to mitigate these risks, including by ensuring full implementation of R.15 and adopting other risk-based measures (e.g., enhancing cybersecurity).

56. Jurisdictions should assess illicit finance risks of DeFi arrangements, consider how DeFi arrangements fit into their AML/CFT frameworks, and share their experiences, practices and remaining challenges with the FATF's global network to mitigate the risk of DeFi arrangements.

57. Jurisdictions are encouraged to assess and monitor the risks associated with unhosted wallets, including P2P transactions, and share their experiences, including on data collection and risk assessment methodologies and findings, as well as practice in mitigating risks.

Implementation of the Travel Rule

58. Jurisdictions that have not yet introduced legislation/regulation to implement the Travel Rule should urgently do so.

[46] The Community Workspace on Virtual Assets is available to government officials of the FATF Global Network only. To request access, authorities should contact their lead ministry or authority in their country's delegation to the FATF, or their FSRB's Secretariat.

59. Jurisdictions that have introduced the Travel Rule should rapidly operationalise it, including through effective supervision and enforcement against non-compliance.

60. To facilitate counterparty due diligence in line with R.16 as well as R.13, jurisdictions are strongly encouraged to maintain and publicise information on VASPs that are registered or licensed in their jurisdiction.

61. Jurisdictions could consider engaging with their VASP sector to promote the adoption of Travel Rule compliance tools that meet all the FATF requirements. This could include optionally engaging with tool providers to identify possible shortcomings and impress the importance of full compliance.

Recommendations for the Private Sector

62. VASPs and Travel Rule compliance tool providers should:

- review their Travel Rule compliance tools to ensure they fully comply with the FATF requirements, and should rapidly address any shortcomings; and
- improve the interoperability of their Travel Rule compliance tools globally, whether through technological advancements that allow interoperability between tools or by developing relationships that permit transactions to be made through a chain of interoperable tools.

63. In light of increasing TF and PF threats related to VAs, including the theft of VAs by DPRK, the private sector and particularly VASPs should ensure they have appropriate risk identification and mitigation measures in line with R.15 in place and should adopt other risk-based measures (e.g., cyber security measures).

64. The private sectors should continue to monitor and assess the risks across the VA ecosystem, including related to DeFi and unhosted wallets, including P2P transactions, and take steps to mitigate these risks and to consult with regulators as necessary to ensure a common risk understanding.

SECTION FIVE:
Next Steps for the FATF and VACG

65. In line with the Roadmap to improve R.15 implementation, the FATF and VACG will continue to conduct outreach and provide assistance to low-capacity jurisdictions to encourage compliance with R.15, including:

- Making use of FATF's internal online platforms to share material related to R.15, including available training and presentations; examples of legislation/regulation, guidance and risk assessments; information on other jurisdictions' approaches.
- Providing technical assistance where possible with a specific focus on areas identified as challenging, e.g., risk assessment, licensing and registration, implementation of the Travel Rule.
- Organising forums, workshops or webinars as possible to share experience and build capacity.
- Collaborating with international partners (including technical assistance providers and Standards-setting bodies) to support broader efforts to improve R.15 implementation.

66. In the first half of 2024, the FATF will publish a table showing which steps FATF member jurisdictions and other jurisdictions with materially important VA activity have taken towards implementing R.15 (e.g., undertaking a risk assessment, enacting legislation to regulate VASPs, conducting a supervisory inspection, etc.). The FATF and VACG will also produce another Targeted Update report in 2024 on jurisdictions' progress implementing R.15, and regulatory policies and responses to emerging virtual asset risks and developments, such as DeFi and P2P transactions.

67. The FATF and VACG will continue to monitor updates in the VA ecosystem as more jurisdictions implement and enforce R.15, including the Travel Rule, and will share information and engage in dialogue with the private sector.

68. In order to ensure that FATF Standards remain relevant in light of rapid changes and evolving risks in this space, including related to DeFi and unhosted wallets, including P2P transactions, the FATF and VACG will continue to monitor market developments, including activities by sanctioned actors, for developments that may necessitate further FATF work. To that end, the FATF and VACG will continue sharing findings, experiences, challenges and leading practices among VACG members and with the FATF global network.

Annex A. Prohibition or licensing/registration? IMF findings on the rationale for VASP regulation

The Rationale for Comprehensive VASP Regulation (IMF)

Extract from the IMF's report on Elements of Effective Policies for Crypto Assets:

Comprehensive regulations are preferred to blanket bans. Comprehensive regulations should address the specific features of crypto assets that generate externalities, such as those that enable high degrees of anonymity (which could facilitate illicit transactions) or lead to environmental burden (for example, when proof-of-work consensus mechanisms are used). Additionally, regulation, as it relates to consumer protection, is needed to address internalities—cases where consumers do not fully take into account the costs of using or holding crypto assets (e.g., volatility in value, possible losses due to cyber-attacks).[1] Issuing warnings and increasing the availability of information can also be helpful, but it might not be sufficient to address externalities and internalities. Moreover, it can provide legitimacy to the market, facilitating closer links with wider financial services that could generate systemic risks without adequately addressing them.

Blanket bans that make all crypto asset activities (e.g., trading and mining) illegal may stifle innovation and drive illicit activities underground. The crypto ecosystem is undergoing rapid change. There is much uncertainty about the extent to which this change will ultimately materialize as productive innovation. Allowing the system to develop (with proper regulation) will allow policy makers to learn about these potential benefits and better mitigate risks (including financial integrity risks), while bans may inadvertently increase the risk exposure.

Bans can be costly to enforce and increase the incentives for circumvention due to the inherent borderless nature of crypto assets, resulting in potentially heightened financial integrity risks, and can also create inefficiencies. A decision to ban should be informed by an assessment of money laundering and terrorist financing (ML/TF) risks, and other considerations, such as large capital outflows and other public policy aims. Regulations imply that certain forms of crypto assets will still be available in the legal marketplace, and thus the degree of substitutability of illegal versus legal assets is likely to be much larger relative to blanket bans of crypto assets.

When substitute assets are not widely available in legal markets, users may be more motivated to access illegal markets and willing to pay higher prices for these assets, due to the stronger incentives to obtain them. A higher willingness to pay for illegal assets increases the profits to those providing such assets, thus raising the incentives for

circumvention. Higher incentives for circumvention imply higher enforcement costs. Moreover, as incentives to circumvent bans are stronger, private sector actors devote more resources to circumvention—an activity that does not produce any socially valuable good or service—and therefore efficiency is negatively affected.

Crypto assets that escape bans may generate additional negative externalities (e.g., more crypto asset activity may become linked to the dark web). Moreover, once crypto assets migrate to illegal markets, the ability of targeted regulation to shape their characteristics and guide the types of innovation that occur is lost. Innovation is path dependent, and thus regulations that affect current features can have important long-run effects.

Targeted restriction could be justified to manage specific risks. Where countries experience large capital outflows, significant currency substitution, an unacceptable level of ML/TF risk, and/or risks to consumers and markets, targeted restrictions might be useful. These restrictions might be targeted to certain products (e.g., privacy tokens), activities (e.g., payments in Ukraine), financial promotions (e.g., in Singapore, Spain, U.K.), or products (e.g., crypto derivatives in Japan and the U.K.). Additionally, broader bans could be considered but only over a shorter time horizon. Also, targeted restrictions might be warranted in the short run while countries increase internal capacity (including knowledge and awareness) in anticipation of regulation.

Even when a temporary imposition of restrictions is contemplated, such restrictions should be considered as part of a larger policy framework. Restrictions should not substitute for robust macroeconomic policies and credible institutional frameworks, which are the first line of defense against the macroeconomic and financial risks posed by crypto assets.

[1] Internalities are the costs, often long-term, that an individual may incur as a result of their actions, which are not taken into account by the individual when deciding to take those actions (Reimer and Houmanfar 2017).

Source: IMF (February 2023), *Elements of Effective Policies for Crypto Assets*, Box 3: The Rationale for Comprehensive Regulations, available at: www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092.