COUNCIL OF EUROPE'S COMMITTEE OF EXPERTS ON THE
EVALUATION OF ANTI-MONEY LAUNDERING MEASURES
AND THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2025)26

Practice of Using Virtual Assets, Virtual Asset Service Providers in the Laundering of Criminal Property, Financing of Terrorism, and the Evasion of Sanctions

Typologies report

December 2025

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The Typologies Report on Money Laundering, Terrorism Financing and Proliferation Financing Risks and Trends Linked to Proceeds Obtained from Conflicts was adopted by the MONEYVAL Committee at its 70th Plenary Session (Strasbourg, December 2025).

Contents

Abbreviations and acronyms

AML	Anti-Money Laundering
CASP	Crypto Asset Service Provider
CFT	Countering the Financing of Terrorism
CPF	Counter-Proliferation Financing
EU	European Union
DPRK	Democratic People's Republic of Korea
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
ML	Money Laundering
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MLA	Mutual Legal Assistance
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
PF	Proliferation Financing
PPP	Public–Private Partnerships
VA	Virtual Assets
VASP	Virtual Asset Service Provider

Executive Summary

The refreshed edition of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) Typology Report builds upon the 2023 Typology Report on Money Laundering (ML) and Terrorist Financing (TF) risks in the World of Virtual Assets (VAs). We can see throughout the evolution of virtual asset technologies and the increasing complexity of associated financial crime risks, specifically in relation to targeted financial sanctions (TFS) evasion.

The Typology Report presents a horizontal review of regulatory and supervisory measures adopted by MONEYVAL jurisdictions; in doing so it highlights significant progress in regulation, supervision, and international cooperation in the field of VAs/VASPs.

Approximately 81% of jurisdictions now require virtual asset service providers (VASPs) to be licensed or registered, and over 90% have designated supervisory authorities. Nevertheless, at present, enforcement against unlicensed operators remains weak, and Travel Rule implementation is incomplete, with only 46% of jurisdictions having operationalised it at the time of the data collection.

Emerging typologies include the misuse of VAs for sanctions evasion, fraud, proliferation financing, and child exploitation. Jurisdictions such as the Isle of Man and Gibraltar provide case studies illustrating the risks of VA use in online gambling and the effectiveness of blockchain analytics in detecting illicit activity.

Data collection is a challenge in many areas, with jurisdictions lacking structured insights into cross-border VA flows.

Some members are adopting advanced supervisory technologies (block chain analytics) and public–private partnerships (PPPs) to enhance risk understanding and suspicious reporting quality.

There continues to be the need for deeper integration of TFS and proliferation financing risks into national assessments, improved quality of suspicious activity reporting from VASPs, and enhanced investigatory capabilities for all competent authorities and the private sector. Jurisdictions need continued capacity building, cross-border cooperation, and to develop tailored guidance to keep pace with the dynamic VA landscape and high paced industry of VASPs.

Prepared by a cross-jurisdictional team, with contributions from experts across seven jurisdictions, the report aims to support MONEYVAL members in strengthening their AML/CFT frameworks and mitigating emerging threats in the virtual asset domain.

Introduction

1. In May 2023 MONEYVAL adopted the first typologies report on money laundering and terrorist financing risks in the world of virtual assets. Recognising the fast-paced nature of developments in crypto and virtual asset technology, it was agreed to undertake a second edition of the typologies.

2. This second edition aims to take into account events on the world stage which have occurred since the first report was written, specifically in relation to how VAs can be used to circumvent TFS. It includes an updated horizontal review of the measures taken to regulate and supervise the virtual asset service provider (VASP) sector as well as identified risks around specific products. It also considers identified risks and features of the implementation of Recommendation 16 and the way it has been applied by jurisdictions to enhance payment transparency and security in cross-border transactions, aiming to combat financial crime more effectively with VAs.

3. The project was conducted by a dedicated working group composed of experts from Isle of Man (Team lead), Azerbaijan, Czech Republic, Estonia, Gibraltar, Guernsey and Romania, supported by the MONEYVAL Secretariat. The analysis is split into several topical areas:

- MONEYVAL Member's Compliance with FATF Standards
- Understanding ML/TF Risks Arising from the Misuse of VAs and VASPs for ML/TF.
- Supervision of VASPs in MONEYVAL Member States
- Law Enforcement and VASPs
- VASPs and Financial Sanctions
- Travel Rule Compliance

4. The primary source of data for these topical areas was a questionnaire answered by 25 MONEYVAL jurisdictions, which included data and case study requests. Results were then coupled with expert opinion from the various jurisdictions and private sector information leading to this comprehensive report.

Key Findings

1. Widespread but Uneven Risk Assessments

Most MONEYVAL jurisdictions have conducted risk assessments on VAs and VASPs, but the depth and quality vary. Many assessments lack specific analysis of TFS evasion risks.

2. Licensing and Registration Regimes Are Expanding

Approximately 81% of jurisdictions now require VASPs to be licensed or registered, marking a significant increase. However, enforcement and detection of unlicensed VASPs remain weak.

3. Supervisory Structures Are Mostly in Place

Over 90% of jurisdictions have designated supervisory authorities for VASPs, typically financial regulators or FIUs. However, guidance and outreach to VASPs are inconsistent.

4. Travel Rule Implementation Is Incomplete

Only about 46% of jurisdictions have implemented the FATF Travel Rule for VASPs. Many non-EU countries are awaiting alignment with EU regulations, and enforcement is limited.

5. TFS Compliance Is Legally Mandated but Operationally Challenging

Most jurisdictions require VASPs to comply with TFS obligations, but few have robust mechanisms to detect or penalize breaches. Sanctions evasion via VAs is a growing concern.

6. International Cooperation Is Strong

Jurisdictions report high levels of cross-border collaboration through FIUs, law enforcement, and supervisory networks. This is one of the most compliant areas across MONEYVAL members.

7. VA Use in Gaming and Other Sectors Presents Unique Risks

Some jurisdictions allow VA use in online gambling under strict conditions. Case studies show exposure to illicit activity, including links to child abuse material.

8. Data Collection Remains a Major Challenge

Many jurisdictions lack structured data on VAs activity, especially cross-border flows. Some are adopting blockchain analytics and enhanced reporting to address this.

9. Emerging Typologies Include Sanctions Evasion, Fraud, and Proliferation Financing

New threats include state-sponsored actors using VAs for proliferation financing, money mule networks, and fraud schemes exploiting the anonymity and speed of VAs.

10. Public–Private Partnerships (PPPs) Are Growing but Uneven

Some jurisdictions have launched PPPs to improve suspicious transaction reporting (STR) quality and typology development, but only 40% have active initiatives involving VASPs. PPPs are becoming critical in the fast-moving VAs space to allow the private sector effectively to enable the public sector to prevent VAs from being used for criminal purposes.

Topical Sections

1. MONEYVAL members' compliance with FATF Standards on VAs and VASPs

5. This section of the report is analysing the MONEYVAL members' compliance with FATF standards on VAs and VASPs. For this part of the report, in addition to the responses provided by the jurisdictions, the mutual evaluation and follow-up reports were analysed.

1.1 Risk Assessment Regulatory Framework (c.15.3–c.15.3)

6. Assessing and understanding ML/TF risks associated with VAs and VASPs is now a near-universal practice among MONEYVAL members. All responding jurisdictions have undertaken some form of risk assessment focusing on VAs, VASPs or both, either as part of their NRA or through dedicated sectoral studies. However, the depth and scope of these assessments vary significantly. In several cases the assessments are recent or still underway, and some were initially academic in nature (conducted before a domestic VASP sector emerged).

7. Notably, many early risk assessments lacked specific consideration of sanctions evasion and TFS risks. In addition to integrating VAs and VASPs in their NRAs, a small number of jurisdictions have undertaken dedicated sectoral risk assessments. For example, a jurisdiction conducted a stand-alone sectoral risk assessment focused on VASPs, analysing the specific ML/TF vulnerabilities of this sector in greater detail. Such targeted assessments are considered good practice, as they provide authorities with a deeper understanding of risks compared to the general NRA-level coverage. For instance, another jurisdiction's initial risk overview (2020–2021) assigned a high-risk rating to the VA sector but did not specifically include TFS evasion risks. This gap is common – a number of jurisdictions acknowledged their VA/VASP risk analysis did not incorporate sanctions-related vulnerabilities.

8. Overall, while every jurisdiction has recognized VA/VASP risks on paper, the quality of risk understanding remains uneven, with some reports using outdated information and others providing only superficial coverage of VA threats.

1.2 Regulatory Framework on licencing/registration (c.15.4)

9. In terms of regulatory framework, most MONEYVAL members now require VASPs to be licensed or registered in order to operate. None of the MONEYVAL member jurisdictions that responded to the questionnaire completely prohibits VAs and related services, and only one member prohibits activity of VASPs on its territory while allowing supervised entities to facilitate transactions for resident clients with foreign-licensed VASPs (see para 48).

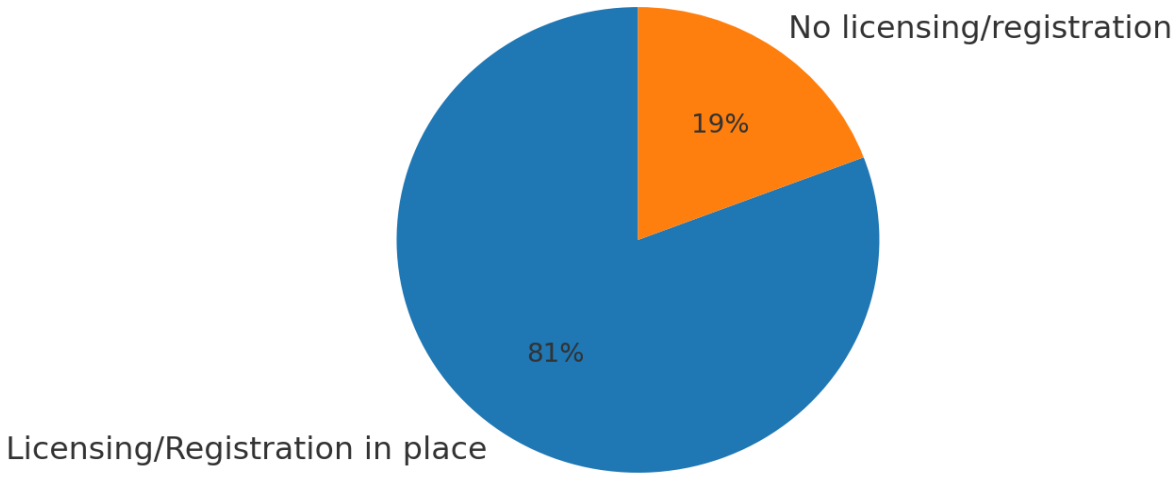

Figure 1- Proportion of MONEYVAL jurisdictions requiring VASPs to be licensed or registered

10. Approximately three-quarters of the surveyed jurisdictions (around 81%) have introduced a licensing or registration regime for VASPs, typically via recent legislative amendments. This marks a substantial increase compared to just a few years ago. Many jurisdictions have established their regimes in alignment with FATF standards and the European Union (EU) framework on VAs. For example, some members have maintained comprehensive VASP registers since 2021 under their designated supervisory authorities, while in other cases legislation requires all VASPs to obtain a license from the national regulator.

11. A few jurisdictions have taken alternative approaches: some have outright prohibited VASP activities rather than licensing them, and several others have not yet implemented their planned licensing frameworks. Where no bespoke regime exists, authorities generally still consider VASPs to fall under existing AML/CFT obligations, but the absence of a registration mechanism creates a regulatory blind spot. The cross-border nature of VASP operations remains a challenge even for those with licensing requirements – VASPs can offer services into a country without physical presence or easily evade local registration. To mitigate this, some members broadened the criteria for mandatory registration (for instance, requiring foreign VASPs that target local customers or advertise in the local language to register). Nonetheless, ensuring all active VASPs are captured by the regime is difficult in practice.

1.3 Identifying and combating unlicensed or unregistered VASPs (c.15.5)

12. Once a regulatory regime is in place, identifying and combating unlicensed or unregistered VASPs becomes crucial. Most jurisdictions have enacted legal prohibitions and penalties for conducting VASP business without a license (or failing to register), establishing the groundwork for enforcement. In practice, however, detection of "black market" VASP activity remains problematic.

13. Members reported that discovering unlicensed operators often relies on indirect methods – media and internet monitoring, market intelligence, or ad-hoc reports – rather than systematic audits. Jurisdictions with no active licensing system face an even greater knowledge gap; for example, a few jurisdictions conceded they had no data available on how many VASPs might be operating in their territory (illustrating the difficulty of quantifying a sector that is not formally supervised). Even where

registers exist, authorities must continuously evaluate if unregistered entities are still servicing local clients online. Overall, while the legal basis to shut down unlicensed VASPs is increasingly in place across MONEYVAL, the proactive identification of such illicit operators is a weak point. Several countries indicated that limited visibility and understanding of the VA ecosystem hampers their ability to find VASPs operating outside the law. This remains an area where further capacity-building and intelligence sharing are needed.

14. Some jurisdictions attempt to prevent 'offshore' VASPs from operating in their country and providing services to their residents. Offshore VASPs pose significant AML/CFT risks to jurisdictions due to their potential to operate beyond the reach of domestic regulatory and supervisory frameworks. These entities often provide services to residents without establishing a physical presence or obtaining local registration, creating regulatory blind spots that can be exploited by illicit actors.

1.4 Supervision (c.15.6)

15. Legal definitions of both VAs and VASPs are in place in almost all jurisdictions, generally embedded in AML/CFT legislation or aligned with the EU Markets in Crypto-Assets Regulation, to define sectors that are supervised. Supervision is conducted by a number of different styles of competent authorities as reported by MONEYVAL members.

16. The vast majority of MONEYVAL jurisdictions have designated one or more competent authorities to supervise VASPs for AML/CFT purposes. In over 90% of cases, a pre-existing national authority was assigned this role – typically the financial sector regulator, financial intelligence unit (FIU), or a specialised agency. For example, in some jurisdictions the central bank has been empowered to supervise VASP compliance (including TFS obligations), while in others AML/CFT oversight of VASPs has been vested in the FIU.

17. In certain cases, the designated supervisor is also the same body that maintains the VASP register, combining authorisation and supervision under one authority. A few members share oversight responsibilities among multiple institutions, with supervisory tasks divided between sectoral regulators, IT agencies, and the FIU. At present, only a couple of MONEYVAL members lack a clearly established VASP supervisor – notably those that have not yet implemented a regulatory regime and therefore have not appointed an authority to license or oversee VASPs. Generally, once VASPs are under oversight, supervisors are applying standard risk-based supervisory tools: conducting on-site/off-site inspections, requiring regular reports, and monitoring compliance in line with practices used for other financial institutions.

18. While many frameworks include both natural and legal persons, some restrict coverage to incorporated entities, and a few do not specify whether natural persons are captured.

1.5 Guidance (c.15.7)

19. Provision of guidelines, feedback and training to the VASP sector is an area where members' approaches diverge. Roughly half of the surveyed jurisdictions have issued some form of public guidance tailored to VASPs, whereas others rely on general AML/CFT guidance or are still developing VASP-specific materials. Many early-adopting regulators published directives or explanatory notes to help VASPs implement their AML obligations (often mirroring guidance given to banks or designated non-financial businesses and professions (DNFBPs)). For example, in some jurisdictions, the competent supervisory authority has published guidelines for risk assessment and implementation of AML/CFT measures applicable to entities under its supervision, including VASPs. In several cases, regional guidelines on ML/TF risk factors have also been used as a basis for providing sector-specific

customer due diligence (CDD) guidance for crypto service providers. On the other hand, some jurisdictions admit they have not yet issued any dedicated guidance for VASPs. In certain cases, FIUs or other authorities host general AML methodological guidelines and information relevant to the crypto sector, but no VASP-specific guideline has been promulgated to date. A similar situation is found in other members where the VASP regime is new or the sector is very small – guidance is planned or under development but not finalised. In terms of feedback, a few supervisors have engaged in outreach programs such as organising training sessions for VASPs, publishing typologies or red flag indicators for VAs, and consulting with private sector on emerging compliance issues. Overall, while baseline expectations for VASP compliance are usually communicated through law and regulation, only about half of MONEYVAL members supplement this with detailed practical guidance, especially on niche aspects like Travel Rule implementation or TFS screening.

20. As of 30th December 2025 The Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures will apply to EU Member States. This document sets out two sets of Guidelines, one of which is specific to Payment Service Providers (PSPs) and Crypto-Asset Service Providers (CASPs) and specifies what PSPs and CASPs should do to be able to comply with restrictive measures (sanctions) when performing transfers of funds or crypto-assets. The second set of guidelines (Travel Rule Guidelines.pdf) target both competent authorities and financial institutions.

1.6 Sanctions (c.15.8)

21. An effective sanctioning regime is in place in virtually all jurisdictions that regulate VASPs. Administrative and civil penalties for non-compliance with AML/CFT requirements by VASPs generally mirror those applicable to other financial institutions and DNFBPs. These typically include a range of punitive measures from written warnings and remedial orders to monetary fines (often substantial), suspension of activities, and revocation of licenses. For example, in some jurisdictions the AML law empowers the supervisory authority to impose sanctions for violations – ranging from warnings and fines up to significant amounts, to suspension or revocation of the VASP's license in serious cases.

22. Many countries have also enabled public enforcement actions (e.g. publishing the names of sanctioned VASPs) to enhance the dissuasiveness of penalties. Notably, most jurisdictions treat operating an unlicensed VASP as a punishable offense – either via administrative penalties or even criminal charges in some cases. Unauthorised provision of VA services is now explicitly prohibited under the laws of many MONEYVAL members. A few members provided concrete examples of enforcement: in one case, authorities took action against entities operating without a license, with individuals prosecuted for facilitating unlicensed VASP activity and even receiving suspended prison sentences – demonstrating that breaches are taken seriously by law enforcement. On the other hand, jurisdictions without a regulatory framework have no such sanctions to apply; until new laws come into effect, they cannot penalize VASP misconduct. Apart from those exceptions, all responding members report having "adequate powers" to apply coercive measures on VASPs that fail to meet their obligations.

23. It is worth noting that TFS obligations are covered under the supervisory and sanctioning frameworks as well. In jurisdictions where VASPs are supervised, the oversight explicitly extends to compliance with UN sanctions regimes (terrorism and proliferation financing sanctions). Supervisors indicated they can apply sanctions for TFS compliance failures just as for other AML/CFT breaches. For example, in some jurisdictions the designated supervisory authority monitors VASPs' compliance with the legal framework on TFS alongside AML/CFT controls. A number of countries have also included TFS-specific enforcement tools in their laws (such as orders to freeze assets, or penalties for dealing with designated persons, applicable to VASPs).

24. Overall, the sanctioning regime "on the books" appears robust across the region – the key challenge moving forward will be the effective and proportionate application of these powers, given that actual enforcement actions against VASPs have so far been limited (in line with the still-nascent size of the sector in many countries).

1.7 Preventive Measures, TFS Obligations and International Cooperation (c.15.9–c.15.11)

25. All MONEYVAL members that have brought VASPs into their AML/CFT regime require them to implement the full suite of preventive measures in line with FATF Recommendations 10–21. In practice, this means VASPs must conduct customer due diligence (CDD) on their clients, keep records, monitor transactions, file suspicious transaction reports (STRs) to the FIU, and so on, just as banks or other covered entities do. One particular element – the "Travel Rule" for virtual asset transfers (analogous to wire transfer rules in traditional finance) – has proven to be a compliance hurdle for some jurisdictions. The Travel Rule (FATF Recommendation 16/INR.15) requires VASPs to obtain, transmit and record originator and beneficiary information for VA transfers above a certain threshold, and to screen transactions for sanctioned parties. As of mid-2025, implementation of the Travel Rule among MONEYVAL members is mixed.

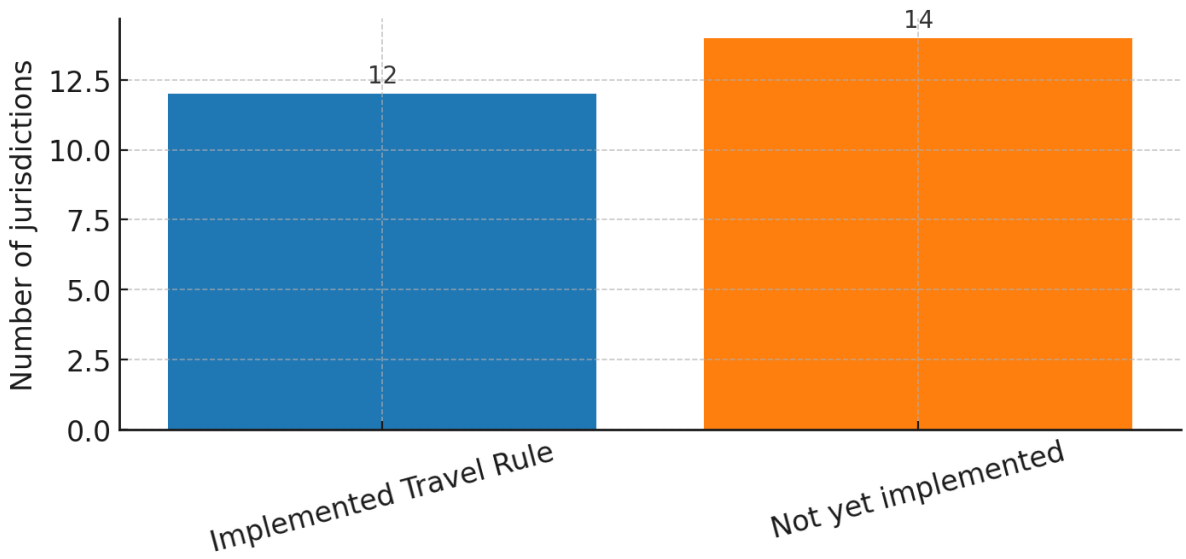

Figure 2 - Implementation of the Travel Rule among MONEYVAL member jurisdictions

26. Roughly half of the surveyed jurisdictions (approximately 46%) reported that they have already implemented or enforced Travel Rule requirements for VASPs. These include most of the early adopters and EU members that moved ahead of forthcoming EU regulations. The other half have not yet operationalised the Travel Rule – in some cases because the legal basis was only recently adopted, and in others because they are waiting to align with the new EU framework which entered into application on 30th December 2024. For example, in some jurisdictions AML/CFT laws have recently been amended to integrate the updated EU framework on fund transfers, ensuring that VASPs comply with Travel Rule obligations going forward. In other cases, legislation explicitly forbids domestic VASPs from transacting with unlicensed or non-compliant foreign VASPs – effectively an implementation of the Travel Rule principle of integrating only with VASPs that also meet information-sharing requirements. On the other hand, some jurisdictions (particularly those with very few VASPs or those still developing regulations) have not yet put the Travel Rule into practice. A number of authorities

noted that they plan to issue detailed guidance or regulations on Travel Rule implementation in the near future (often timed with EU framework). In summary, while basic CDD and reporting obligations are universally applied to VASPs, the Travel Rule is only partially implemented across MONEYVAL at present, with broader compliance expected as new regulations come into effect.

27. With regard to TFS (Recommendation 6, 7 and c.15.10), all jurisdictions affirmed that VASPs are subject to the same TFS obligations and enforcement mechanisms as other financial institutions. This means that VASPs must screen their customers and transactions against relevant UN sanctions lists (e.g. UNSCR 1267/1373 lists for terrorist financing, and proliferation financing lists) and freeze any assets of designated persons or entities. Supervisory authorities are actively checking VASPs' compliance with TFS requirements as part of their inspections.

28. A dozen member countries explicitly confirmed that their VASP supervisors include TFS checks in supervisory scope, and none indicated any exemption for VASPs. In practice, many VASPs in the region use automated screening tools or rely on outsourced solutions to manage sanctions screening, similar to how banks operate.

29. A few jurisdictions shared that they have not yet encountered cases of sanctions evasion via VASPs but remain vigilant. Importantly, no major gaps were reported in countries' legal frameworks for applying TFS to VAs – laws generally empower authorities to enforce asset freezing orders on VASPs and take action for non-compliance, as needed. For example, in some jurisdictions the FIU or competent authority can issue binding orders to freeze transactions, including those involving VAs, if a match with designated persons is identified. Some countries have also engaged VASPs in awareness-raising about sanctions risks (for instance, listing red flags of potential sanctions evasion through crypto).

30. Overall, MONEYVAL members appear to have integrated VASPs into their national TFS regimes comprehensively, ensuring that VASPs are obliged to promptly implement any new UN designations. Minor deficiencies in this area, where noted, tend to stem from broader issues in national TFS frameworks rather than VA-specific problems (e.g. delays in transposing UN designations into local lists, which would affect all sectors equally).

31. Finally, international cooperation (c.15.11) emerges as one of the strongest aspects of compliance among MONEYVAL members in the VA/VASP domain. Countries reported that their authorities are generally able to exchange information and provide assistance to foreign counterparts involving VAs, using the full range of existing international cooperation channels. This includes FIU-to-FIU exchanges (through the Egmont Group), law enforcement agencies (LEAs) cooperation via INTERPOL/Europol and bilateral MLA, and supervisory cooperation through MOUs or networks (e.g. the International Organization on Securities Commissions (IOSCO) fintech forum, AML/CFT supervisory colleges). A horizontal review of compliance indicated that members achieved the highest level of compliance on c.15.11, largely thanks to the broad powers already available under Recommendations 37–40 for international cooperation.

32. In practice, many MONEYVAL jurisdictions have already engaged in cross-border investigations or joint actions involving VAs/VASPs. Several respondents shared concrete success stories: for instance, in one case an FIU coordinated a joint investigation with international partners, leading to the sanctioning of a licensed VASP (VA exchange platform) for facilitating illicit transactions. In another example, close collaboration with a regional cybercrime division was highlighted as "essential" for investigating VA-related criminal cases.

33. Likewise, some members have participated in international task forces and information-sharing networks on VAs, helping to trace funds and identify perpetrators across borders. No jurisdiction reported any legal impediment to cooperating on VA matters; if anything, those without

established domestic VASP frameworks noted that they still rely on international assistance when cases arise (for example, seeking information from countries where major exchanges are domiciled).

34. A common challenge mentioned is the need for timely cooperation – rapidly freezing or seizing VAs often requires expeditious communication between countries. While some difficulties were acknowledged (such as differences in legal procedures or technical capabilities), overall, MONEYVAL members are leveraging international cooperation mechanisms effectively to compensate for the borderless nature of VAs. This strong international link is crucial: as one authority put it, regulated and supervised VASPs can be "a useful source of information" for investigations, but the global reach of crypto means no country can combat abuse of VAs in isolation. The survey responses underscore a clear commitment across the region to continue strengthening cooperation, through both formal channels and informal partnerships, to address emerging ML/TF risks in the VAs space.

2. Understanding of ML/TF risks arising from the misuse of VAs and VASPs for ML/TF

35. This section of the report analysis the understanding of ML/TF risks arising from the misuse of VAs and VASPs for ML/TF. It examines in more details how the risks are being identified, assessed and understood, including the challanges in data colletion.

2.1 Identifying and assessing the risks

36. The extent to which MONEYVAL members effectively identify and assess the risks associated with VAs and VASPs has advanced notably in recent years. A growing number of jurisdictions have now undertaken both national and sectoral risk assessments, with the latter increasingly used to complement broader national analyses by focusing in detail on the characteristics of the VASP sector. These improvements reflect the marked increase in the number of jurisdictions that have established supervisory frameworks governing VAs and VASPs (as set out in the analysis above), which in turn has enabled a more systematic identification and assessment of the associated risks.

Case Box 1 - VA and VASP risk assessment – Lithuania

Lithuania carried out its third national risk assessment (NRA), completed in October 2024, with an increased emphasis on assessing the risks posed by VAs and VASPs.

The study of the VASP sector included a mapping of the existing market and an analysis of its vulnerabilities. Twelve main risk scenarios were identified, covering the misuse of VAs for money laundering and terrorist financing purposes, as well as sector-specific typologies such as the use of mixers, NFT trading, fraud schemes, and vulnerabilities in crypto-ATM operations. The assessment was supported by supervisory insights, intelligence from the FIU, and comparative analysis with neighbouring jurisdictions.

The NRA concluded with key findings, risk ratings, and proposed mitigation measures. The overall risk of ML/TF associated with the VASP sector was assessed as heightened, requiring continued strengthening of supervision, early implementation of the FATF Travel Rule, and regular updating of the sectoral assessment.

37. Despite this broader coverage, a number of assessments lack depth and remain largely theoretical, often relying heavily on international typologies rather than detailed domestic analysis. Across jurisdictions, typologies are often drawn from international reports and sources, with few being rooted in domestic cases or intelligence, limiting the extent to which assessments capture the operational realities of how VAs and VASPs are actually being misused within national contexts. A

relatively common observation is also that these assessments focus primarily on VASPs themselves, giving less attention to the broad use of VAs in the wider financial system and economy. For example, the misuse of VAs in online gambling, in-game purchases, real estate transactions and other products/services may not be fully considered, representing a possible blind spot in a jurisdiction's understanding of VA-related risks. In some jurisdictions, the use of VAs in these contexts falls outside the scope of regulatory oversight altogether or is formally prohibited, resulting in little structured information available to assess their scale, materiality or risk profile. Whilst progress has therefore been made in strengthening the understanding of risks arising from the misuse of VAs and VASPs, the assessments conducted in some jurisdictions remain preliminary in nature and will require further development before they can be considered a mature and comprehensive analysis.

Case Box 2 - Use of VAs in Gaming – Isle of Man

The Isle of Man Gambling Supervision Commission (GSC) permits the use of VAs for online gambling, subject to appropriate approval and the application of additional licensing conditions. As an example, the GSC considers the use of VAs to represent higher inherent risk, increasing the licence holder's risk score and leading to more frequent regulatory inspections under its risk-based supervisory methodology. The GSC also collects data from its regulated entities specifically on VA transactions, including the number and value of deposits and withdrawals per jurisdiction.

In 2022, a gambling licence holder, which was permitted to use VAs (with the relevant imposed licence conditions), demonstrated to the GSC the use of blockchain analytics to monitor VA transactions in detail. On three separate occasions, alerts had been received from the entity's chosen blockchain analytics system in relation to three different customers, notifying the licence holder that the wallet addresses used to deposit had been transactionally linked to VA wallets used on websites connected to child abuse material. In its investigation, the licence holder determined that all three addresses originated from the same illicit website use, and on further review, it was established that two of the chains overlapped and shared an address in common. As a result, the licence holder terminated the relationships and appropriate disclosures were made.

This case illustrates how VA use in online gambling can create channels of exposure to high risk/illicit activity. It also highlights the importance of supervisory oversight, and the need for jurisdictions to reflect the risks of such VA activity in NRAs rather than focusing on VASPs alone.

2.2 Challenges in Data Collection

38. A solid information base is critical for developing meaningful VA and VASP risk assessments; yet, in some jurisdictions this remains largely limited. Authorities often lack formal data that would allow them to assess the scale and nature of activity in a systematic way, particularly in relation to cross-border flows. This gap reflects, in part, the relative infancy of regulatory frameworks in some jurisdictions, where supervisory authorities are still developing and amending reporting requirements and data-collection practices capable of generating reliable insights. As set out above, in the absence of such inputs, assessments tend to rely heavily on qualitative judgements or international typologies, reducing their ability to effectively capture the specificities of VA-related activity within domestic economies.

39. This challenge is compounded by the fact that a number of MONEYVAL members have not yet implemented dedicated regulatory frameworks to supervise VA and VASP activities. The absence of such regimes creates structural weaknesses that illicit actors can exploit as a means of facilitating financial crime. At the same time, some jurisdictions with established frameworks rely solely on the observation that no VASPs are currently registered in order to justify low risk ratings, overlooking the

principle that the absence of domestic regulated VASPs does not, in itself, guarantee there is no wider VA activity giving rise to potential risk.

40. Some jurisdictions have begun to address gaps in data collection by integrating technological solutions into their supervisory and risk assessment frameworks. Supervisory technology and enhanced regulatory returns, for example, have been introduced to provide more granular insights into VASP activity, including customer profiles, transaction volumes and geographic exposure. In parallel, the adoption of blockchain analytics technology has allowed jurisdictions to assess connections with known sources of higher-risk activity on the blockchain. These tools, when combined with structured reporting from supervised entities, create a more robust evidential base for national and sectoral risk assessments and enable authorities to move beyond largely qualitative judgements towards data-driven analysis.

Case Box 3 - Use of technology and data collection – Gibraltar

The Gibraltar Financial Services Commission (GFSC), as the designated supervisory authority for VASPs, has implemented a series of VASP-specific questions within its annual supervisory returns. Each VASP is required to submit an extensive regulatory data set, including (but not limited to) data pertaining to:

1. the composition of its new and existing customer base, including categories of clients and their geographic distribution;

2. transaction values and volumes, including their geographic exposure;

3. reporting mechanisms and disclosures; and

4. materiality and risk indicators.

In parallel, the GFSC has integrated blockchain analytics into its supervisory approach. Using its selected analytics system, the GFSC is able to assess transactional exposure at wallet, entity and jurisdictional levels. These tools are also leveraged as an additional means of facilitating the identification of potential unauthorised VASP activity.

In addition to feeding into the GFSC's supervisory approach, these data sources support the assessment of national and sectoral risk and enhance the authority's ability to identify trends, anomalies or shifts in risk across the industry.

2.3 Scope of Assessments

41. Most VA and VASP risk assessments undertaken by MONEYVAL members to date have focused primarily on quantifying money laundering (ML) and terrorist financing (TF) risks. These dimensions are generally well reflected in national and sectoral analyses, often supported by suspicious transaction report data, supervisory findings and case examples. By contrast, far fewer jurisdictions have incorporated a systematic assessment of risks relating to TFS evasion or proliferation financing (PF). The limited treatment of these risks is notable, especially considering that the growing use of VAs by sanctioned actors and proliferating states has been well documented internationally.

42. Sanctions evasion through VAs has emerged as a concrete and growing threat. In practice, sanctioned entities and individuals exploit the attractive speed and borderless nature of VA services to shift value outside of the traditional financial system, often abusing peer-to-peer transactions, VASPs with limited controls, or layers of self-hosted wallets. The use of anonymising products and services, including mixers and privacy-enhancing coins, has been internationally recognised as a means of further evasion detection. These methods allow sanctioned actors to obscure the origin and

destination of funds, undermining the effectiveness of TFS regimes. This underscores the relevance of TFS and PF risks in relation to VAs and VASPs. In a number of jurisdictions, however, they remain largely unassessed, or acknowledged only briefly, without the same depth of analysis or typology development that is applied to ML and TF. As the VA/VASP landscape continues to shift and develop over time, addressing these areas will be critical in developing a comprehensive understanding of risks that keeps pace with international typology developments.

Case Box 4 - Sanctions evasion typologies – Estonia

In May 2023, the Estonian Financial Intelligence Unit (EFIU) published a dedicated report entitled "*Overview of evasion of sanctions through VAs*". The report identifies three primary typologies through which VAs are considered to be used to evade TFS, namely:

1. direct peer-to-peer transactions;
2. the use of layers of intermediaries; and
3. the use of an escrow system of intermediaries.

By mapping out these techniques, the FIU demonstrated how sanctioned individuals and entities can use VAs to bypass restrictions and re-enter the formal financial system. The report further highlights a series of potential risk indicators of sanctions evasion, together with key factors that VASPs should consider in order to ensure effective compliance checks and the appropriate mitigation of risk.

2.4 Emerging VA & VASP Typologies

43. The rapid evolution of the VA ecosystem in recent years has been accompanied by a parallel increase in its exploitation for illicit purposes. International evidence demonstrates that illicit actors are quick to adapt to innovations in this space. The ability to recognise and integrate these emerging risks into national assessments is therefore crucial to ensure that frameworks remain up-to-date and effective.

44. As set out above, PF risks represent one of the most significant developments. State-sponsored actors have increasingly turned to VAs as a means of acquiring and moving funds associated with the development of weapons of mass destruction. The activities of the Democratic People's Republic of Korea (DPRK) provide the most prominent example, with cyber units repeatedly stealing large volumes of cryptocurrency from exchanges and platforms and laundering them through obfuscation tools. As noted earlier, however, a significant proportion of MONEYVAL members are yet to incorporate an analysis of these risks into structured national or sectoral assessments, leaving gaps in the regional understanding of exposure.

45. Money mules are also becoming more prominent in the VA context. Traditional mule networks (which involve individuals transferring or withdrawing illicit funds on behalf of criminal organisations), are increasingly being adapted to VAs. Individuals (often recruited through social media, job advertisements, or online forums) are persuaded to open exchange accounts or facilitate peer-to-peer transfers, lending criminals access to regulated platforms while obscuring the true beneficial owner. These arrangements complicate customer due diligence and transaction monitoring, and they illustrate the convergence between VA misuse and more established financial crime techniques.

46. Fraud cases linked to VAs are also generally reported to be increasing. Common schemes include investment scams, Ponzi structures, and romance frauds where victims are persuaded to purchase VAs and transfer them to fraudsters. International reports suggest that these typologies are

becoming increasingly prevalent, with criminals exploiting the irreversible nature of VA transfers and the speed with which funds can be moved across borders. The rise of fraud also creates secondary laundering risks, as stolen or fraudulently acquired funds are layered through complex webs of wallets and service providers before re-entering the financial system.

47. The increase in illicit activity associated with VAs is enabled, more generally, by a growing ecosystem of tools designed to enhance anonymity. Mixers, tumblers and anonymity-enhancing assets are routinely used to conceal the origin of illicit funds and disrupt tracing efforts. DeFi protocols and cross-chain bridges add an additional layer of complexity, enabling rapid movement between different assets and blockchains in ways that circumvent traditional compliance controls. These technologies are not inherently illicit, but their misuse by criminals and sanctioned actors poses acute challenges for authorities. While some jurisdictions have responded by restricting or prohibiting the provision of certain anonymity-enhancing services/products by regulated VASPs, the risk of their misuse by illicit actors remains high.

48. Taken together, these developments highlight the speed with which VA-related typologies evolve and the difficulties jurisdictions face in keeping pace. For MONEYVAL members, the challenge is twofold: ensuring that national assessments adequately capture emerging risks and developing supervisory and investigative capabilities able to address the increasingly complex tools being deployed by illicit actors.

Case Box 5 - Proliferation financing risk assessment – Gibraltar

In August 2025, Gibraltar published the third iteration of its NRA, which includes a detailed assessment of the proliferation financing risks faced by the jurisdiction. The assessment focuses on the potential misuse of both traditional financial channels and emerging technologies (including VAs and VASPs) for the purposes of facilitating the proliferation of weapons of mass destruction.

The assessment explores the risks posed by VASPs in relation to cyber-enabled proliferation financing, and focuses on the materiality, scale and context of Gibraltar's VA/VASP activities, including trends in both regulatory compliance and suspicious transaction reporting. The report concludes that while the threat is low (due primarily to Gibraltar's lack of geographic proximity or trade/financial ties to proliferating states, coupled with the absence of any known domestic cases or exposure to PF-related activity), the risk of proliferation financing within Gibraltar's finance centre cannot be discarded. The findings of the PF assessment were incorporated into Gibraltar's supervisory strategy, including the integration of targeted outreach.

2.5 Capacity Building & Public-Private Engagement

49. The development of expertise in both the public and private sectors is key to effectively understand and mitigate the risks associated with VAs and VASPs, given their reliance on relatively novel technology. Among the submitted responses, MONEYVAL member jurisdictions referred to a wide range of training and technical assistance initiatives targeting both public and private sector stakeholders. These initiatives ranged significantly in topic, format and intensity, reflecting the multifaceted nature of VA-related risks.

50. In relation to the public sector, FIUs, supervisory authorities, LEAs and prosecutors have increasingly recognised the need to strengthen institutional capacity across supervision, analysis, investigation and enforcement in respect of VA-related activity. Reported training programmes included introductory courses on blockchain fundamentals, specialised modules on the use of blockchain analytics tools, and targeted sessions on emerging typologies such as mixers, privacy coins,

and decentralised finance (DeFi). In several cases, these training sessions were provided in cooperation with international bodies, as well as private sector institutions.

51. In parallel, outreach to the private sector has been a growing focus of MONEYVAL members. Supervisors and FIUs have convened workshops and seminars for obliged entities to raise awareness of VA-related risks and red flags. These engagements have often been designed not only to improve compliance capacity but also to ensure that reporting entities recognise their role in identifying suspicious patterns and transactions. This has been undertaken in tandem with the development of practical handbooks or sectoral guidance notes, complementing outreach efforts. Overall, these initiatives aim to increase risk awareness, although the level of maturity varies across MONEYVAL members.

Case Box 6 - FIU Engagement with VASPs – Gibraltar

As part of a concerted effort to improve STR quality through an outreach and engagement program called Project Nexus, the Gibraltar Financial Intelligence Unit (GFIU) engaged directly with the VASP sector to strengthen mutual understanding of ML/TF and other criminality risks. The GFIU delivered targeted training to one VASP (identified as the top submitter of STRs) while also inviting the entity to demonstrate how their monitoring systems operate, how suspicious activity is identified with crypto tracing tools, what triggers internal reporting, and how cases are escalated.

This collaborative approach allowed both the GFIU and the entity to share knowledge on typologies, clarify expectations, and build stronger working relationships. The initiative has enhanced the quality of STRs submitted, encouraged early identification of suspicious activity, and reinforced Project Nexus' sustainable framework for ongoing public–private sector cooperation.

52. Beyond discrete training programmes, several MONEYVAL members highlighted the growing role of public-private partnerships (PPPs) as a powerful mechanism for capacity building and risk analysis. PPPs provide a structured forum through which regulators, FIUs, LEAs and industry can share data, typologies and practical experience in real time. In doing so, they leverage pooled resources in the expertise developed within both the private and public sectors to foster a robust shared understanding of risk. In some jurisdictions, PPPs have evolved into standing working groups dedicated to VAs, with outputs feeding directly into national and sectoral risk assessments. Jurisdictions with active PPPs report better coordination and more actionable intelligence and, although VASP inclusion in PPPs is still limited, it is growing, especially in jurisdictions with mature FinTech sectors.

53. However, the limited jurisdictional adoption (40%) and lower private sector representation suggest that further outreach, capacity building, and trust-building are needed to scale PPPs globally and make them more inclusive.

54. In summary, MONEYVAL members have made notable progress in identifying and assessing the risks associated with VAs and VASPs, underpinned by the expansion of supervisory frameworks and the increasing use of effective national and sectoral risk assessments. At the same time, the horizontal review highlights areas where further development would strengthen collective resilience, including the depth of data collection, the scope of risk coverage, and the integration of emerging and domestic typologies into formal assessments. Good practices, such as the use of blockchain analytics, dedicated proliferation financing assessments, and structured public–private partnerships, demonstrate that innovative and effective approaches are already being implemented. Building on these foundations will enable MONEYVAL members to continue advancing their understanding of VA-related risks and to ensure that supervisory and risk assessment frameworks keep pace with the rapidly evolving VA ecosystem.

Case Box 7 - Use of PPPs – Malta

The Financial Intelligence Analysis Unit (FIAU) of Malta has established its Financial Intelligence Report Partnership (FINREP) with the primary aim of creating a structured platform for the FIAU and the private sector to collectively identify new ML and TF typologies, as well as to conduct joint analysis projects designed to proactively uncover suspicious activity.

In 2024, FINREP launched a specific project involving 42 obliged entities (including VASPs) aimed at determining whether the terrorist financing risk rating produced by the Maltese NRA accurately reflected the jurisdiction's lower TF exposure, or whether it was the result of under-reporting. The project has resulted in a number of key outcomes, including:

1. in-depth analysis of specific cases;
2. intelligence sharing with foreign counterparts; and
3. the drafting of a best-practice guidance document to be circulated to industry stakeholders following completion.

Case Box 8 - VASPs, E-Gaming & PPPs – Isle of Man

In May 2025, the Isle of Man (IOM) Financial Intelligence Unit (FIU) published an '*Online Gambling: Red Flags and Typologies'* document covering Money Laundering, Terrorist Financing and Proliferation Financing.

The same month, the IOM published a '*National Statement on e-Gaming and Financial Crime'* document. This specifically addressed emerging risks related to organised crime groups from East and Southeast Asia operating in e-Gaming-related businesses.

As a result, both publications have led to an increased focus of the public and private sectors working collaboratively to mitigate risks.

Whilst work continued on the *Gambling National Risk Assessment*, the jurisdiction also began to create a new IOM Financial Crime Partnership (IOMFCP) group that could work together on risks related to IOM e-Gaming and associated businesses. A purely sectoral approach was considered and a new group established, uniting representatives from IOM licensed e-Gaming operators, an IOM trust and company service providers (TCSP) specialised in accommodating e-Gaming business, e-Gaming software suppliers, banks, a Money Transmission Services, an IOM VASP, an IOM e-Gaming set up company, as well as representatives from the Gambling Supervision Commission, the Financial Services Authority, the IOM Constabulary and the FIU (which includes the IOMFCP Secretariat).

The e-Gaming Risk Group has commenced a meeting cycle and is preparing future strategic projects that will assist in the mitigation of risks related to the IOM e-gaming industry.

2.6 Summary of PPP Initiatives Across Jurisdictions

Jurisdictions Reporting Active PPPs Involving VASPs:

Jurisdiction	Initiative Name / Description	Stakeholders Involved	Outcomes / Lessons Learned
Cyprus	Pilot PPP coordinated by FIU (MOKAS)	FIU, Police, Central Bank, Banks	Strategic analysis report on complex ML typologies; plans to expand to VASPs
Czechia	PPP with VASPs (2017–2020), now under AML/CFT Coordination Group	FIU, VASPs, Czech Banking Association	Improved STR quality and sectoral awareness
Estonia	Estonian Financial Intelligence Task Force (EFIT)	FIU, 5 largest banks, open to LEA input	77% useful STRs via EFIT; improved reporting quality
Georgia	Interagency Working Group led by Prosecutor General	Prosecutor's Office, LEAs, FIU, Supervisors, VASPs	Unified AML/CFT practices; typology sharing; extended-format meetings
Gibraltar	Exploring VASP PPP following success of FLINT (banking sector PPP)	FIU, VASP sector (planned)	Positive initial feedback; launch expected by end of 2025
Hungary	Supervisory working group initiated by National Bank of Hungary (MNB) and Financial Intelligence Unit of Hungary (HFIU)	MNB, HFIU, Ministry of Justice, Ministry of Economy	MoU being drafted to coordinate AML/CFT supervision of crypto-asset service providers (CASPs)[1]
Isle of Man	Isle of Man Financial Crime Partnership (IOMFCP)	FIU, LEAs, regulators, banking, insurance, TCSPs	Tactical briefings; improved asset restraint processes; VASPs included in key areas
Lithuania	Center of Excellence in AML; FinTech Action Plan (2023–2028)	FIU, LEAs, Supervisors, FinTechs	Unified AML/CFT approach; timely threat sharing; FinTech sector engagement
Malta	FINREP PPP; Operation HAFI (2024)	FIAU, 22 VASPs, 12 financial institutions, 8 banks	STRs on HAMAS-linked wallets; intelligence shared with foreign FIUs

1. Crypto-asset service providers (CASPs) as per definition in MiCA Regulation.

Jurisdiction	Initiative Name / Description	Stakeholders Involved	Outcomes / Lessons Learned
Slovakia	Interdepartmental working group coordinated by National Bank of Slovakia (NBS)	NBS, Police, Prosecutor General's Office	Unified approach to crypto-asset regulation and criminal activity

3. Supervision of VASPs in MONEYVAL Member States

55. This section of the report outlines the different approaches taken by members to license or register domestic VASPs, and to implement a risk-based supervisory framework for the VASP sector.

3.1 General information

56. Before analysing the licensing and supervision of VASPs across MONEYVAL member states, it is important to first highlight the key regulatory developments at the EU level, specifically the adoption of the Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA Regulation)[2] and Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (TFR Regulation).[3] These instruments have introduced high regulatory standards for VASPs and established robust mechanisms for implementing the Travel Rule across EU jurisdictions.

57. Within the MONEYVAL membership, the regulatory landscape must be assessed by distinguishing between:

- EU Member States: All EU countries are required to implement the MiCA and TFR Regulations into their national legal frameworks, thereby ensuring a harmonised and strengthened regulatory foundation for VASPs across the EU. Among Member States, it is important to distinguish between those that followed the regulatory framework as set out in the MiCA Regulation and those that opted to go beyond its requirements—particularly in areas such as the definition of VAs and VASPs;
- Non-EU Member States: Among these jurisdictions, two distinct approaches can be observed. Some states are actively seeking to align their regulatory frameworks with the MiCA Regulation, while others continue to rely solely on the FATF Recommendations as the basis for their domestic regulation of VASPs.

58. This typological distinction is critical for the structure of this report. In particular, the licensing and supervisory frameworks of EU Member States, as well as those of non-EU countries aligning with the EU regulatory model, are currently undergoing (for EU) or is undergoing (non-EU countries) significant conceptual reforms. Therefore, it is recommended that a comprehensive update of the analysis is conducted in the coming years, once the MiCA and TFR Regulations have been fully implemented, the MiCA grandfathering periods have expired, and supervisory practices have stabilised.

2. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, Regulation - 2023/1114 - EN - EUR-Lex .
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, Regulation - 2023/1113 - EN - EUR-Lex .

3.2 Different types of VAs and VASPs

59. MONEYVAL members used different approaches when introducing a definition of the terms VAs and VASPs into their legislation, which has a cascading effect both on technical compliance and effectiveness issues. In the Glossary to the FATF Methodology VAs is defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

60. While MONEYVAL members mostly adhere to this definition of VAs, there are minor differences in approaches. From the responses received, it can be observed that EU countries[4] adapted their regulatory framework to the MiCA Regulation. While some EU countries define VAs purely based on the MiCA Regulation, including its limitations (e.g. NFTs, DeFi, utility tokens), others went beyond and extended the definition to limitations set. Additionally, some non-EU countries also expressed willingness to align their legal framework with the MiCA Regulation. However, the level of alignment varies.

61. A Virtual Asset Service Provider (VASP) is any natural or legal person that provides as a business one or more of the following activities or operations, for or on behalf of another natural or legal person:

i. exchange between VAs and FIAT currencies;
ii. exchange between one or more forms of VAs;
iii. transfer of VAs;
iv. safekeeping and/or administration of VAs or instruments enabling control over VAs; and
v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

62. The term VASP is technology neutral, it could include crypto currency businesses, NFT trading sites, ATM operators, wallet custodians and decentralised exchanges. The recent overhaul of EU legislation regarding VAs and AML/CFT/CPF (e.g. MiCA Regulation, TFR, amendment to AML directive due to AML package) closed the majority of legacy gaps between the definition of VASP (respectively defined as Crypto Asset Service Providers (CASP) in MICA), at the FATF and EU level. For example, participation in and provision of services in relation to coin issuance, the provision of VA transfer services, and services of exchange between VAs are now covered by MiCA. The analysis indicated that, in most non-EU jurisdictions as well, the scope of definitions provided by the FATF is generally respected. Some countries permit VASP activities to be carried out by natural persons, whereas others have chosen to limit the status of VASPs exclusively to legal entities.

63. Stablecoins have recently become one of the important topics within the AML/CFT framework associated with VA and VASP. Stablecoins represent a form of VA that may be particularly attractive to criminals, as they combine the enforcement challenges typical of VA with the relative price stability. Under the new EU regulatory framework, stablecoins are classified into two distinct categories:

- E-Money Tokens (EMTs): single-fiat stablecoins (e.g. euro-pegged)
- Asset-Referenced Tokens (ARTs): tokens pegged to a basket of fiat currencies, commodities or crypto-assets.

64. Issuers of both EMTs and ARTs, as well as any CASPs involved in activities related to these tokens, are governed by the MiCA Regulation.

4. Only responses from EU countries were received, no EEA only country responded.

65. The analysis indicates that, in the vast majority of non-EU jurisdictions, stablecoins are generally covered under the definition of VA. These jurisdictions typically do not apply any specific regulatory provisions to stablecoins beyond the standard AML/CFT rules applicable to VA and VASPs.

66. Another important topic within the AML/CFT framework is decentralised finance (DeFi). Some jurisdictions report that DeFi arrangements are considered to fall under the definition of VASPs. In contrast, many jurisdictions indicate that DeFi is currently unregulated within their national frameworks. EU Member States generally base their approach on the MiCA Regulation. According to Recital 22 of the MiCA Regulation, "*Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation*." According to the analysis, the principal regulatory challenge concerning DeFi is to establish clear criteria for the types and levels of control or involvement through which an individual or entity should be regarded as a VASP or, under the MiCA Regulation, as a CASP.

Case Box 9 – Stable Coins - Andorra

Issuance of stablecoins would be subject to the "specially activity regime" of Article 26 of Law 24/2022. Some additional regulatory requirements, as established in Article 26.1 of said law, would include the following:

(i) *The issuance of digital asset pegged to a traditional financial or digital instrument is reserved exclusively to banking entities, investment firms and collective investment funds management firms.*

(ii) The issuance of a fiat-pegged digital asset is reserved exclusively to banking entities, non-banking specialised credit institutions and payment entities.

(iii) The custody of the reserve funds (in fiat money) that stablecoins issuers use will have to be deposited in an Andorran banking entity.

(iv) No other natural or physical person other than the ones indicated above can issue or provide any ancillary services to stablecoins pegged to fiat money or financial instruments.

(v) The issuance of any digital asset pegged to other digital assets different from fiat money or financial instruments can only be made by a legal person having a business address in Andorra.

(vi) The issuance of a digital asset that can be considered as an algorithmic stablecoin is reserved exclusively to banking entities, investment firms and collective investment funds management firms.

(vii) Stablecoin issuers will have to submit, when applying for a license, some additional documents, including the governance rules related to the collateralised assets (including roles, responsibilities, administration of the depositary accounts, custody, distributions and mechanisms to guarantee liquidity) and the stabilisation mechanism for the digital asset.

(viii) On an annual basis (during the first trimester of each year), the stablecoin issuer will have to present an activity report to the AFA demonstrating that they continue to meet all the criteria that led to the granting of the license.

(ix) Stablecoin issuers will have to monthly publish on their website and submit to the AFA the number of circulating tokens, as well as the value and composition of the collateralised funds.

Case Box 10 – Stable Coins - Estonia

Estonia's Market in Crypto-Assets Act, which entered into force on 1 July 2024, implements the EU's MiCA Regulation framework domestically and treats fiat-pegged tokens as two distinct categories:

- Asset-Referenced Tokens (ARTs): tokens pegged to a basket of fiat currencies, commodities or crypto-assets.
- E-Money Tokens (EMTs): single-fiat stablecoins (e.g. euro-pegged) analogous to e-money under the E-Money Directive.

Both ART and EMT issuers (and any CASP dealing in them) must obtain a CASP licence from the Estonian FSA, maintain a registered office in Estonia, and comply with MiCA's issuance rules (white-paper approval for ARTs; notification for EMTs), governance standards, capital/reserve requirements, disclosure obligations and consumer-protection measures.

Stablecoins in Estonia are not exempt from AML/CFT or customer due diligence (CDD) rules. Under the MLTFPA, as amended in 2019, all crypto asset service providers – including those issuing or trading ARTs and EMTs – must:

- Perform customer due diligence (KYC) and ongoing monitoring.
- Identify and verify beneficial owners.
- Screen transactions and report suspicious activity to the FIU.

These obligations apply on a risk-based basis and mirror those for other VAs.

While AML/CFT/CDD is universal regarding all crypto-assets, MiCA/CMA impose additional obligatory layers on stablecoins:

- ART issuers must hold diversified liquid reserves, meet higher capital buffers, conduct periodic stress-testing, and obtain formal FSA approval of their white paper.

EMT issuers (e-money tokens) follow an e-money-style regime: safeguarding client funds, maintaining minimum own-funds and governance standards akin to electronic-money institutions (but under the FSA's CASP licence rather than via the separate E-Money Directive alone).

3.3 Regulatory framework

67. A risk mitigating measure for VASP activity is the application of market entry controls and of adequate risk-based supervision for AML/CFT purposes to the sector. Due to the new EU regulatory framework, there were major regulatory changes in EU Member States and, to some degree, in other countries that decided to align themselves more closely to the EU's regime (this process is still ongoing). As mentioned above, this not only closed legacy gaps in some countries but significantly increased regulatory requirements due to the MiCA Regulation. None of the MONEYVAL member jurisdictions that responded to the questionnaire completely prohibits VAs and related services, and only one member prohibits activity of VASPs on its territory while allowing supervised entities to facilitate transactions for resident clients with foreign-licensed VASPs.

3.4 Licensing or registration regime

68. FATF Recommendation 15 allows countries to choose between licensing or registration of VASPs, providing that at a minimum, VASPs would be required to be licensed or registered in the jurisdiction(s) where they are created. In cases where the VASP is a natural person, it should be required to be licensed or registered in the jurisdiction where its place of business is located. To

comply with this requirement, most MONEYVAL members have introduced some form of licensing or registration or notification regime for VASPs.

69. For EU members, the MiCA Regulation goes beyond FATF standards for licensing or registration and introduces complex licensing requiring fit-and-proper assessments, internal control mechanisms for AML/CFT/CPF, risk assessment framework for the management of AML/CFT/CPF and many other non-AML/CFT/CPF related requirements (e.g. prudential, ICT/cybersecurity, client-asset protection). Transitional grandfathering periods are currently in place and licensing process is ongoing: data received shows that many entities try to use transitional grandfathering periods to the maximum extent possible and apply for the license just before the deadline, which places significant burdens on licensing authorities as they have to assess most of the applications at once within tight deadlines (hundreds of applications in some cases).

70. EU countries generally expect, at least in the short term, a decrease in the number of supervised entities due to significant requirement of the MiCA Regulation. This, together with the consolidation of VASP ecosystem, was observed in several countries even before the MiCA regulation came to force. This trend seems to be caused by the strenghtening of regulatory requirements and the remedying of existing so-called sunrise issues. The decrease in number of supervised entities was already evident from some preliminary data provided. Only one EU country indicated that it expects an increase in the number of supervised entities in the short term.

71. Some jurisdictions have laws regulating the use of specific technology. For example, in one member, there is a separation between Digital Ledger Technology (DLT) Providers and other VASP activities. There are different regulatory regimes for the DLT Providers authorised and supervised by one regulatory authority, and a different requirement for the other VASP activities.

72. The previously limited possibility for natural persons to be registered or licensed as a VASP has been further narrowed under the MiCA Regulation, as neither CASPs nor issuers of crypto-assets can be natural persons. Despite this, some EU countries allow natural persons to be licensed as VASPs, but with severe limitations to provide only VA services not regulated by the MiCA Regulation.

73. The MiCA Regulation also sets high fit-and-proper standards for members of the management body as well as shareholders and members (whether direct or indirect) that have qualifying holdings, as they have to be of good repute and, in particular, not been convicted of ML/TF offences. This contributes to unifying the previously fragmented requirements.

Case box 11 - Current statistics from licensing and lessons learnt - Czechia

The Czechia legislation adopting MiCA introduces a transitional period during which VASPs that provided crypto-asset services defined by MiCA must apply for a new CASP license with the Czechia National Bank by 31 July 2025; otherwise, their former license would become void.

The Czechia National Bank has previous experience with re-licensing and consolidating several financial sectors, so it has been preparing intensively for this process by taking several measures:

- Communicating with the private sector and estimating the number of license applications.
- Reallocating and training additional personnel to assess applications. Experienced supervisors were temporarily reassigned from other supervisory areas.
- Enhancing cooperation with the FIU to gather any negative information for fit-and-proper assessments. This cooperation considered logistical challenges such as high

expected workload and the relatively short timeframe for application assessments. Additionally, ad hoc meetings were planned in case negative information emerged.
- Introducing a tiering system for applications after preliminary review to streamline the assessment process based on quality and completeness.

During the transitional period, 188 entities previously licensed as VASPs applied for a CASP license.

As of the end of October 2025, there were 236 applications in total, with preliminary results as follows:

- 0 licenses granted
- 13 applications assessed as legally invalid
- 79 applications rejected (with several administrative appeals)
- 144 applications still under evaluation.

Preliminary results indicate that a significant number of CASP license applications under MiCA do not meet the requirements.

Lessons learned:

- Communication with the private sector and accurate estimation of expected applications are key to preventing supervisory overload.
- Reallocation of additional resources may be necessary to ensure adequate market entry rules in line with MiCA.
- Streamlined communication with other authorities is crucial to maintain proper information flow within the short evaluation timeframes envisioned by MiCA.

3.5 AML/CFT supervision or monitoring

Designating the supervisory authority

74. The FATF Recommendations allow a wide margin of flexibility for the authorities to choose the supervisory model that is most suitable for them, taking into account the risk and materiality of the VASP sector, and the specific institutional setup of public authorities. MONEYVAL members have implemented different approaches to supervision – which means that the licensing or registration authority is not always the same authority that conducts the AML/CFT supervision of VASPs. MONEYVAL members mostly entrust supervision of VASPs to FIU, central banks or other financial supervisors, and the supervision is either carried out solely by one of these supervisors or jointly. Whichever approach the jurisdiction is taking, in the case of VASP, it should be effective in supervising the sector and minimising the ML/TF risks.

Powers of supervisors to adequately monitor the sector and resources

75. MONEYVAL members implement the supervision and monitoring obligations in varied ways. Some jurisdictions opted to apply the same AML/CFT obligations to VASPs as for FIs and DNFBPs, with the same powers for performing the supervisory function available in relation to VASPs. As such, any new potential VASP would be subject to the same risk-based supervision model and tools as other obliged entities.

76. There is evidence of significant training and capacity building of supervisors in the VASP sector across MONEYVAL members. This might be a result of significant focus on VAs in the AML/CFT area in recent years. Additionally, the MiCA Regulation places high expectations on supervisors, including strict deadlines, so intense preparation was needed.

77. The previously identified trend of integrating IT specialists, including specialists on VA tracing, into supervisory teams appears not only to continue but also to strengthen. However, it was observed that not all supervisors of MONEYVAL members have necessary tools for effective supervision of VASPs (e.g. VA tracing tools), likely due to the significant cost of these tools which hinders effectiveness of supervision, especially regarding Travel Rule obligations. Therefore, there seems to be scope for improving supervisory resources.

Applying a risk-based approach to supervision of VASPs

78. Most countries have conducted national or sectoral risk assessments for VAs and VASPs, identifying the sector as high or emerging risk for ML/TF. Risk assessments start to consider factors such as transaction anonymity, cross-border flows, customer profiles, and typologies of misuse (e.g. fraud, sanctions evasion) and are less reliant on high-level general findings. This increase in quality of risk assessment should improve supervision more in line with risk-based approach. Many authorities use or are adopting blockchain analytics tools for transaction monitoring and risk profiling. Regarding individual VASPs or particular VA products, services, or activities, more advanced supervisors take into account the level of risk associated with the VASPs' products and services, business models, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location, countries of operation, their level of compliance with AML/CFT measures, as well as the risks associated with specific VA products that undermine transparency.

Detecting cross-border flows

79. For EU Member states, the TFR operationalises the Travel Rule, requiring VASPs to collect, verify, and transmit detailed originator and beneficiary information for all crypto-asset transfers. This ensures a harmonised and enforceable approach to monitor such transactions across the EU.

80. In contrast, implementation of the Travel Rule in non-EU jurisdictions remains limited and, in many cases, is still under development. While some MONEYVAL countries have introduced annual or periodic questionnaires to gather data on cross-border inflows and outflows of VAs, these mechanisms largely rely on self-reported information from VASPs. Such data is not always independently verified through blockchain analytics or other technical means, which can limit its reliability and effectiveness.

81. A notable trend across both EU and non-EU countries is the increasing engagement with virtual asset experts and the adoption of blockchain analytics tools. Supervisory authorities and obliged entities are investing in specialised training and capacity-building, often in collaboration with external providers, to enhance their ability to detect, monitor, and analyse cross-border virtual asset flows and related risks.

Sanctions

82. The availability and effectiveness of sanctions for VASP supervisors in MONEYVAL member jurisdictions varies considerably, both in terms of the scope and the amounts of sanctions that can be imposed. While some members have established a comprehensive and dissuasive sanctioning framework, others still face significant limitations. In several jurisdictions, supervisors are empowered to impose a broad range of administrative and pecuniary sanctions—including warnings, fines, license suspension or revocation, and public statements—on VASPs and their management for non-compliance with AML/CFT and TFS obligations. However, in other cases, the available sanctions are more limited: supervisors may lack the authority to restrict or suspend a VASPs' license, or to impose non-monetary penalties such as management bans or remedial directives. As a result, not all members are able to apply a full suite of effective, proportionate, and dissuasive sanctions to the VASP sector.

83. The ability to sanction unregistered or unauthorised VASPs also differs across jurisdictions. In some countries, supervisors or LEAs have explicit powers to penalise both legal and natural persons for conducting VASP activities without proper registration or authorisation, including the authority to prohibit business activities, impose fines, or refer cases for criminal prosecution. In other jurisdictions, such enforcement is less clear-cut, with gaps in the legal framework or ambiguity over which authority is responsible for taking action. Administrative and criminal courts may also play a role, particularly where complaints are made or where unauthorised activity is identified.

84. Enforcement in practice remains uneven. While there are examples of significant enforcement actions against VASPs for AML/CFT violations, the actual use of sanctions—especially non-monetary and TFS-related measures—remains limited in many jurisdictions. The detection and sanctioning of unregistered VASPs is particularly challenging. Responsibility for detecting and sanctioning unregistered or unlicensed VASP activity is often fragmented. In some countries, the task is clearly assigned to a specific authority (typically the supervisor), with established procedures for investigation and enforcement. In others, responsibility is diffuse or ambiguous, leading to gaps in enforcement. A common scenario is that, in the absence of clear procedures or powers, supervisors may treat unregistered VASPs as engaging in illegal activity and expect the police or other LEAs to intervene, whereas LEAs may lack the expertise or mandate and expect supervisors to take the lead. This diffusion of responsibility can result in inaction and regulatory arbitrage.

VAs in the Gaming Industry

85. The analysis revealed that, in most MONEYVAL member states, VAs are not currently used in the gaming industry, or the respective jurisdictions have no available information regarding such use. In jurisdictions where VAs are not used in gaming, several cases were identified where indirect restrictions on VA-based payments were applied—typically through limitations on permitted payment methods, which are often restricted to fiat transactions and, in some cases, exclusively to cashless payments.

86. In other jurisdictions, the use of VAs is not possible due to the fact that, under national legislation, they not recognised as a means of payment or legal tender. In jurisdictions where VAs are used in gaming, national legislation generally requires gaming operators to obtain specific authorisation prior to accepting payments in VAs.

VAs in the Real estate Sector

87. Only a limited number of MONEYVAL member states have a specific regulatory framework governing the purchase of real estate using VAs. The questionnaire responses indicate that real estate purchases involving VAs are recognised among respondents, although not in significant volumes. In the case of jurisdictions that have restricted the use of VA in real estate transactions, such limitations are typically implemented through limitations on permitted payment methods, which are often restricted to cashless transactions.

Case Box 12 – Real Estate Sector – Andorra

VAs are not officially accepted as a direct payment method in notarial real estate purchase and sale transactions within Andorra.

Although Law 24/2022 regulates digital assets, they cannot be used in official real estate transactions before a notary.

This means that transactions must be carried out in euros and with bank traceability.

If cryptocurrencies have been converted into euros, the buyer must prove the origin of those funds and their traceability.

4. Law Enforcement and VASPs

88. This chapter examines the evolving capabilities and approaches of MONEYVAL jurisdictions in investigating money laundering (ML) and terrorist financing (TF) involving VAs, and in applying interim measures to disrupt illicit financial flows. Building on the findings of the 2023 report, the 2025 assessment reflects both progress and persistent challenges in the operational and regulatory response to VA-related financial crime.

4.1 Law Enforcement

89. Investigations involving VAs continue to present a complex set of challenges. Jurisdictions report ongoing difficulties, including:

(i) limited expertise among law enforcement and supervisory authorities in tracing and analysing VA transactions;
(ii) legal uncertainty regarding the applicability of interim measures to VAs, particularly in cross-border contexts;
(iii) gaps in access to or deployment of blockchain analytics tools;
(iv) inconsistent cooperation with foreign jurisdictions and VASPs, which delays the freezing and seizure of assets; and
(v) the emergence of unregulated or decentralised VASP models that fall outside traditional supervisory frameworks.

90. At the same time, the underlying technology, particularly blockchain, remains an asset for investigators. The immutable nature of blockchain records offers a reliable trail for tracing transactions, provided that appropriate tools and expertise are in place. Jurisdictions that have invested in blockchain analytics and capacity-building report improved outcomes in tracing and recovering VAs.

91. The regulation and supervision of VASPs continues to be a cornerstone of effective financial crime prevention in the VA space. Regulated VASPs serve as key sources of financial intelligence, particularly through the submission of suspicious transaction reports (STRs). However, the quality of STRs submitted by VASPs remains uneven. The 2025 report highlights concern around automated reporting, defensive STRs, and the outsourcing of AML/CFT functions, which collectively undermine the utility of STRs for investigative purposes.

92. The rapid evolution of the VA sector, including the rise of privacy-enhancing technologies, decentralised finance (DeFi), and cross-chain asset movement, necessitates ongoing adaptation. Jurisdictions are increasingly recognising the need for continuous training, inter-agency coordination, and structured public-private partnerships to keep pace with technological developments and emerging typologies.

93. This chapter draws on responses from jurisdictions and provides a comparative analysis of investigative powers, legal frameworks, operational tools, STR quality, and international cooperation mechanisms. It aims to identify good practices, highlight areas for improvement, and support jurisdictions in strengthening their response to ML/TF involving VAs.

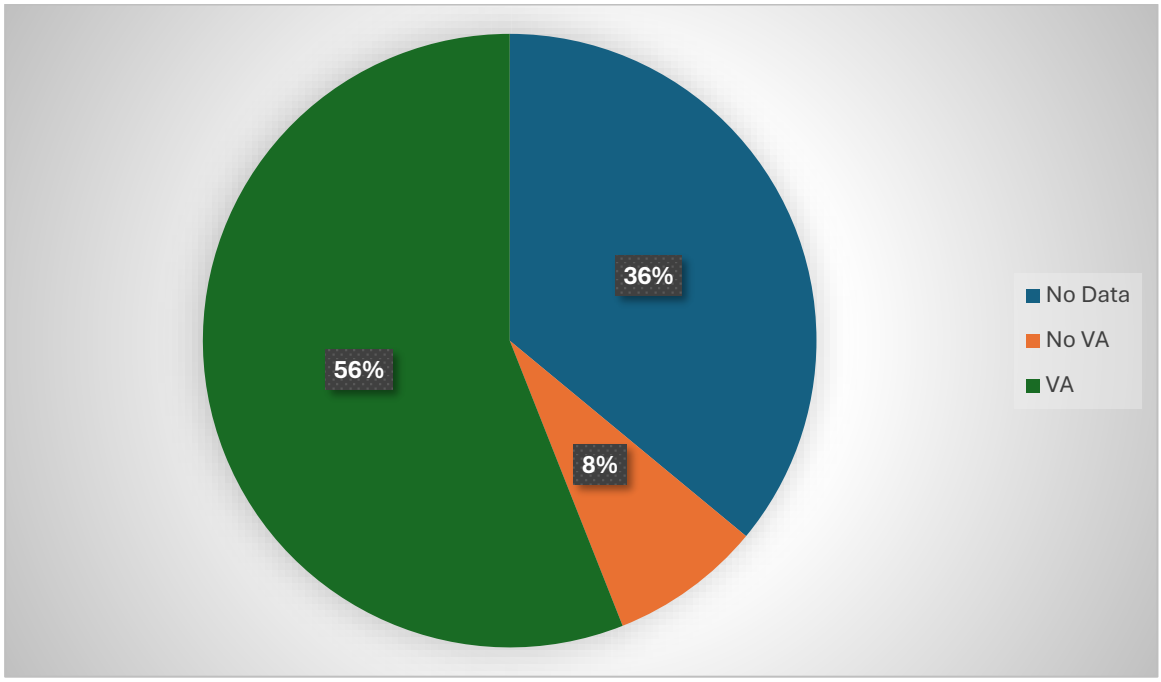

Figure 3- Number of respondents with VASPs as the source of their STRs and/or SARs

94. Chart *"Number of respondents with VASPs as the Source of their STRs and/or SARs"*:

- 56% of respondents indicated that VAs were the source of their STRs/SARs;
- 36% reported no data on this topic;
- 8% stated that VASPs were not the source of their STRs/SARs.

95. This suggests that a majority of jurisdictions are seeing suspicious reporting activity linked to VASPs, while a significant portion either lacks data or does not associate VASPs with such reports.

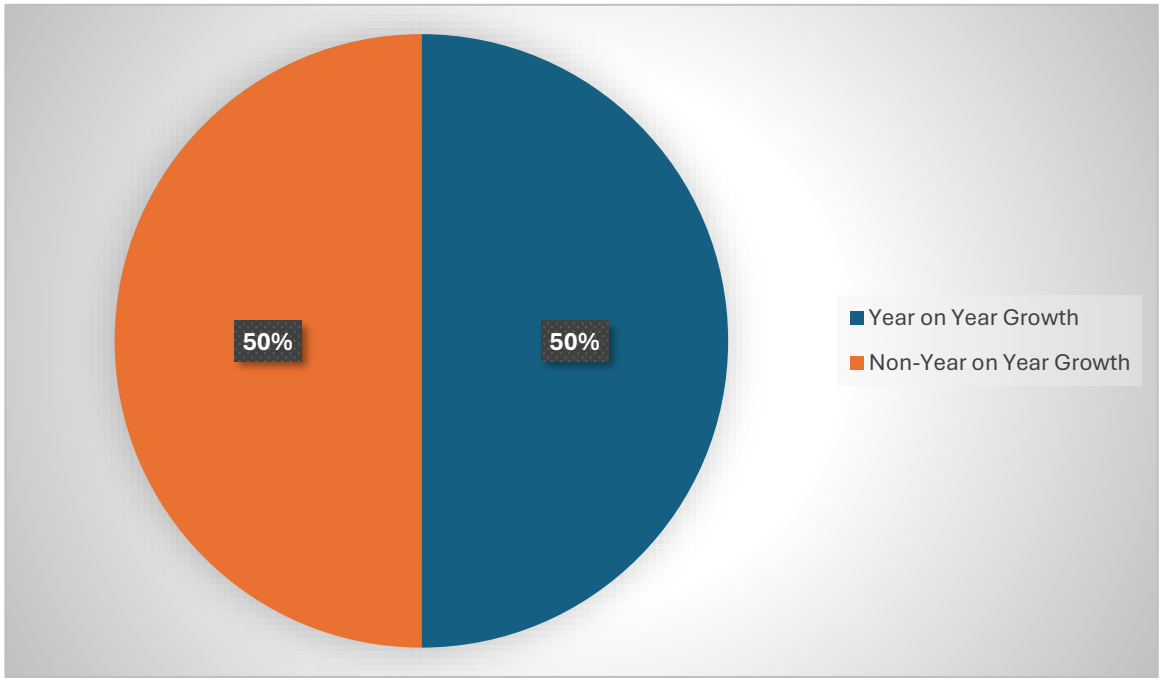

Figure 4 - Number of Respondents who saw Year on Year Growth in VASPs as the Source of their STRs and/or SARs

96. Chart "*Number of Respondents who saw Year-on-Year Growth in VASPs as the Source of their STRs and/or SARs*":

- 50% of respondents reported year-on-year growth in VASPs as sources of STRs/SARs.
- 50% reported no year-on-year growth.

97. This split suggests that jurisdictions are evenly divided on whether they are seeing increasing suspicious reporting activity linked to VASPs over time.

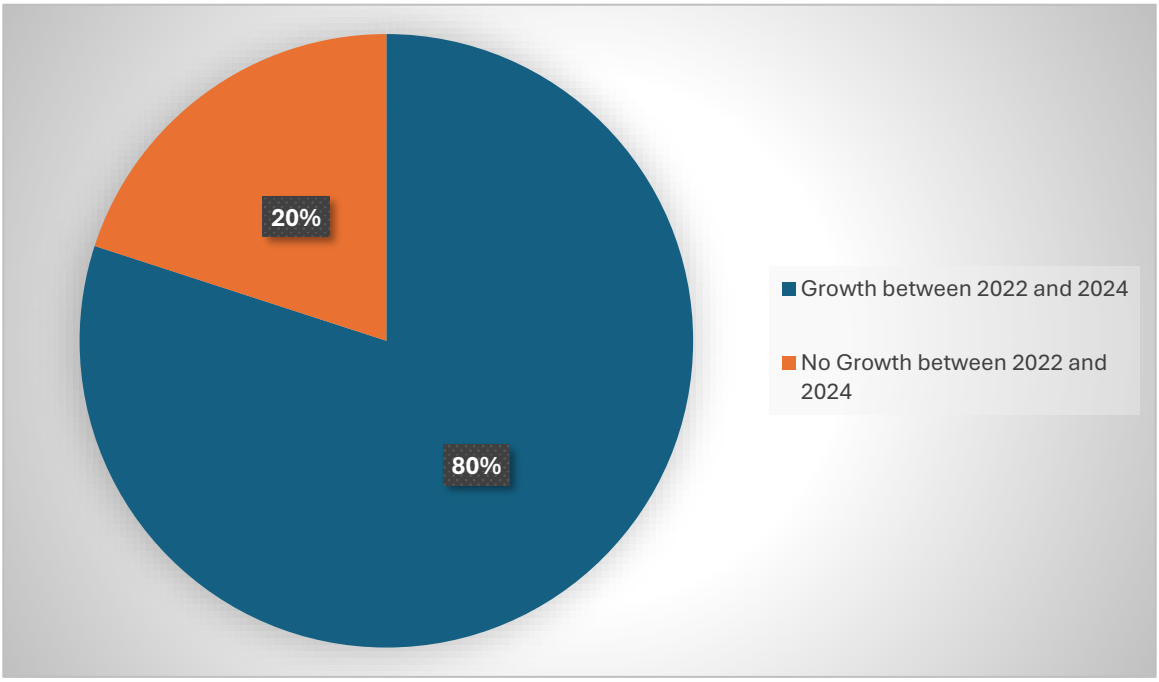

Figure 5 - Number of Respondents who saw Growth in VASPs as the Source of their STRs and/or SARs from 2022 and 2024

98. Chart "*Number of Respondents who saw Growth in VASPs as the Source of their STRs and/or SARs from 2022 and 2024*":

- 80% of respondents observed growth in VASPs as sources of STRs/SARs between 2022 and 2024.
- 20% reported no growth during that period.

99. This suggests a strong upward trend in suspicious reporting activity linked to VASPs across jurisdictions over the two-year span.

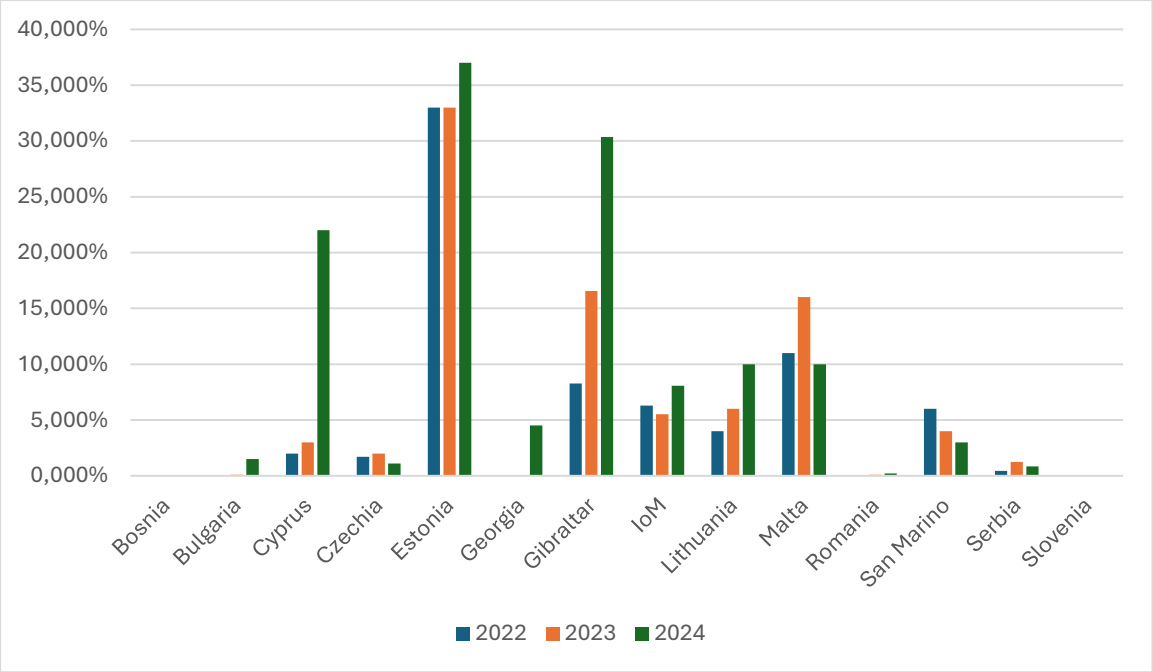

Figure 6 - % of STRs and/or SARs Received who's source was VASPs

100. Figure 6:

- Estonia consistently leads with the highest percentage of reports, rising from ~35% in 2022 to nearly 40% in 2024.
- Cyprus shows a sharp growth in 2024 (~25%), as did Gibraltar (~30%)
- Malta demonstrates steady growth, peaking near 20% in 2023 and 2024.
- The data reflects regional variation in VASP-related suspicious reporting, with some jurisdictions showing clear upward trends while others remaining static or low.

101. It is accepted by the project team that numbers of STRs and/or SARs should not be used in isolation when comparing jurisdictions, especially considering the different levels of materiality that the sector has in different jurisdictions.

Table 1 - Table with respondents who declared data on VASPs as the Source of STRs and/or SARs from 2022 – 2024

Jurisdiction	**2022**	**2023**	**2024**
Bosnia	0.001%	0.001%	0.003%
Bulgaria	0.1%	0.1%	1.5%
Cyprus	2%	3%	22%
Czechia	1.7%	2%	1.1%
Estonia	33%	33%	37%
Georgia	0%	0.0%	4.5%
Gibraltar	8.3%	16.6%	30.3%

IoM	6.3%	5.5%	8.1%
Lithuania	4.0%	6.0%	10.0%
Malta	11%	16%	10%
Romania	0.1%	0.1%	0.2%
San Marino	6.0%	4.0%	3.0%
Serbia	0.5%	1.2%	0.8%
Slovenia	0.0%	0.0%	0.01%

102. Based on the above charts, the consolidated conclusion can be made regarding jurisdictional engagement with Virtual Asset Service Providers (VASPs) in the context of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs):

A. Engagement with VA-related ML Investigations

- 60% of jurisdictions (15 out of 25) have actively investigated VAs in relation to Money Laundering (ML).
- The remaining 40% either have no data or have never investigated such cases.
- This indicates a majority awareness and operational engagement, though a significant minority still lacks either experience or data.

B. VASPs as a Source of STRs/SARs

- 56% of jurisdictions reported receiving STRs/SARs from VASPs.
- 36% had no data, and 8% reported no VASP-related reports.
- This indicates awareness and operational engagement by the majority, though a significant minority still lacks either experience or data.

C. Year-on-Year Growth Trends

- An even split: 50% of jurisdictions observed year-on-year growth in VASP-related STRs/SARs, while 50% did not.
- This reflects divergent experiences, possibly due to differences in market maturity, regulatory frameworks, or VASP activity levels.

D. Growth Between 2022 and 2024

- A strong 80% of jurisdictions reported growth in VASP-related STRs/SARs over the two-year period.
- Only 20% saw no growth, indicating a clear upward trend in VASP-related suspicious activity reporting.

E. Jurisdictional Breakdown

- Estonia, Cyprus, and Malta show the highest percentages of STRs/SARs from VASPs, with Estonia peaking near 40% in 2024.

Overall Conclusion

103. There is a clear and growing engagement with VASPs across jurisdictions, especially in relation to money laundering investigations and suspicious reporting. However, the data also reveals

gaps in experience and reporting, with some jurisdictions lacking sufficient data. The trend from 2022 to 2024 shows strong growth, reinforcing the need for tailored policies, SOPs, and capacity building, particularly in jurisdictions with low or no engagement

4.2 Quality of STRs Submitted by VASPs

104. An overview of the quality of STRs submitted by VASPs in jurisdictions where the number of reports is significantly higher – namely Hungary, Lithuania, and Malta – indicates recurring concerns.

105. Several jurisdictions highlighted the following issues:

A. Automated STR generation

- In Lithuania, and Malta, STRs are frequently generated by technological tools used by VASPs to monitor wallet activity. These tools often flag wallet addresses based on links to other addresses associated with adverse information, sometimes several hops down a transaction chain. While these tools are useful for identifying potentially suspicious activity, they cannot replace human-led analysis based on behavioural traits and typologies.
- The lack of human intervention in STR selection has led to a high volume of low-quality reports, with practitioners suggesting that fewer, more targeted STRs would yield better financial intelligence.

B. Defensive reporting

- Jurisdictions such as Malta reported that a significant portion of STRs were submitted defensively, often triggered by the inability to complete customer due diligence (CDD).
- In some cases, STRs were filed even when no transaction had occurred, undermining the value of the reports.

C. Outsourcing of AML/CFT obligations

- Malta and Lithuania noted that some VASPs outsource their CDD and transaction monitoring functions. This practice has hindered the development of internal expertise in detecting suspicious transactions.
- In response, certain jurisdictions have introduced restrictions on outsourcing specific AML/CFT obligations, particularly those related to transaction monitoring and suspicion analysis.

D. IT-to-Compliance conversion

- Malta highlighted a trend where VASP compliance teams are composed of individuals with strong technical knowledge of blockchain and VAs tools but limited understanding of AML/CFT principles. This mismatch has contributed to poor STR quality, as technical proficiency alone does not ensure effective suspicion detection.

E. Jurisdictional reporting challenges

- VASPs operating across multiple jurisdictions often struggle to determine where to report a suspicion, especially when the jurisdictional nexus of a transaction is unclear. Malta reported instances of both duplicate reporting and misdirected STRs due to this issue.

D. Improving STR Quality

- Jurisdictions stressed the importance of outreach and capacity-building initiatives to improve the quality of STRs submitted by VASPs. Recommended measures include: (i) disseminating

typologies and ML/TF trends specific to VASPs and VAs; (ii) collecting and analysing data on STR quality and sharing insights with the private sector; (iii) organising informal discussion sessions between FIUs, supervisors, and VASP operators to foster mutual understanding and improve detection capabilities.

4.3 Underlying Predicate Offences

106. A limited number of jurisdictions provided data on predicate offences identified through STRs involving VASPs. Nonetheless, several common trends and typologies were observed, consistent with those highlighted in the 2023 report:

- **Money laundering** remains the most frequently cited predicate offence, followed by cybercrime, fraud, and terrorist financing. Jurisdictions such as North Macedonia and Slovakia reported cases of investment fraud, where victims were deceived into transferring VAs to fraudulent schemes, often under the guise of high-return investment opportunities. These cases typically involve social engineering tactics, including impersonation and phishing, to gain access to wallets or persuade victims to initiate transfers.
- **Child exploitation** was reported as a key predicate offence in Bosnia and Herzegovina, where blockchain analysis tools were used to trace transactions linked to wallets associated with child abuse material. STRs were triggered when VASPs identified suspicious links between client wallets and known illicit addresses.
- **Sanctions evasion** was noted by several jurisdictions, including Andorra, Estonia, Georgia, and Moldova. These jurisdictions highlighted the potential for VAs to be used as alternative payment mechanisms by sanctioned entities seeking to bypass restrictions on traditional financial systems. Estonia, for example, reported cooperation with OFAC in a case involving a sanctioned VASP.
- **Range of offences, including corruption, organised crime, tax crimes, and human trafficking** were reported by other jurisdictions, though these were less frequently mentioned. This suggests that while VAs and VASPs are increasingly relevant in financial crime investigations, their role as primary enablers of predicate offences remains limited to jurisdictions with more advanced supervisory and investigative capabilities.

107. Overall, the data indicates that money laundering, investment fraud, child exploitation, and sanctions evasion remain key typologies. Continued development of blockchain analytics, typology sharing, and inter-agency cooperation will be essential to improving detection and reporting of these offences.

4.4 Investigatory Capabilities

108. Drawing from questionnaire responses, it appears that in most jurisdictions, investigatory responsibilities for ML/TF cases are not determined by the modus operandi (e.g. use of legal entities, cash, or VAs), but rather by the predicate offence. This reflects a continuation of the trend observed in the 2023 report.

109. Typically, jurisdictions assign cases to specialised units based on the nature of the underlying offence, such as corruption, organised crime, or economic crime, rather than the tools or technologies used in the commission of the offence. For example, Andorra and Bulgaria reported that their cybercrime or technological crime units are involved in VA-related investigations, but these units are not exclusively dedicated to VAs.

110. In smaller jurisdictions, such as Guernsey and Gibraltar, a centralised law enforcement authority or asset recovery unit is responsible for investigating all criminal offences, including those involving VAs. These jurisdictions tend to rely on generalist structures with cross-functional capabilities, rather than creating dedicated units.

111. A few jurisdictions have opted to establish specialised units focused on VAs or technology-enabled crime. These include:

- Albania, where the Cyber Crime Unit supports investigations involving VAs.
- Estonia, where the Police and Border Guard Board hosts a central Asset Recovery Office and Cybercrime Bureau. Georgia, where the Prosecutor's Office has developed guidelines for VA seizure and freezing.
- Hungary, which has created a national cybercrime and asset recovery backbone to support regional police units.

112. Overall, while some jurisdictions are beginning to adapt their structures to better address the challenges posed by VAs, the majority continue to rely on existing frameworks. The investigation of ML/TF cases involving VASPs or VAs is generally entrusted to law enforcement agencies based on their pre-existing mandates, with limited differentiation based on typology or technological complexity.

Collection of Intelligence and Evidence from VASPs

113. Most MONEYVAL jurisdictions continue to rely on their FIUs and LEAs to collect intelligence and evidence from VASPs, with the legal basis for such collection typically rooted in AML/CFT legislation and criminal procedure codes. However, the effectiveness of these mechanisms remains closely tied to the jurisdiction's regulatory approach to VASPs, particularly the extent to which VASP activities are designated under national law.

114. Several jurisdictions reported that their FIUs can request information from VASPs as part of their operational and strategic analysis functions. This includes access to customer due diligence records, transaction histories, wallet addresses, and internal alerts. In jurisdictions such as Bulgaria, Estonia, and Malta, domestic VASPs are considered obliged entities, and FIUs can compel disclosure under AML/CFT laws. In cases involving foreign VASPs, FIUs often rely on international cooperation channels, such as the Egmont Secure Web or FIU.Net, to obtain relevant information. However, challenges persist when dealing with unregistered VASPs or those operating in jurisdictions with limited cooperation frameworks.

115. A minority of jurisdictions, including the Isle of Man and Malta, have broader powers allowing FIUs or LEAs to request information from any person or entity, regardless of their designation as a reporting entity. These powers are particularly relevant in cases involving decentralised platforms or non-custodial wallet providers, where traditional regulatory oversight may not apply.

116. The issue of decentralised finance (DeFi) remains a concern. While FATF guidance clarifies that the Recommendations do not apply to the underlying software, jurisdictions continue to grapple with identifying controllers or operators of DeFi arrangements who may fall within the definition of a VASP. Several jurisdictions noted that the lack of identifiable persons behind DeFi platforms complicates intelligence collection and enforcement actions.

117. For the collection of evidence, jurisdictions generally rely on powers granted under criminal law. These include search and seizure orders, production orders, and court-authorised freezing measures. In many cases, LEAs must obtain judicial approval before accessing data held by VASPs. Jurisdictions such as Georgia and Lithuania reported the use of specialised procedures for seizing VAs, including transferring assets to government-controlled wallets or using multi-signature wallets to ensure secure custody.

118. Cross-border cooperation remains a critical component of evidence collection. Jurisdictions frequently cited the use of Mutual Legal Assistance Treaties (MLATs), European Investigation Orders (EIOs), and direct engagement with foreign FIUs or VASPs. However, the responsiveness of foreign VASPs varies significantly, with some requiring formal legal requests and others cooperating voluntarily. The lack of harmonised procedures across jurisdictions was identified as a barrier to timely intelligence and evidence collection.

119. Jurisdictions also highlighted the operational challenges posed by VASPs with no physical presence or unclear jurisdictional ties. In such cases, LEAs often rely on open-source intelligence, blockchain analytics tools, and cooperation with third-party service providers to trace transactions and identify suspects.

120. In summary, while legal mechanisms for collecting intelligence and evidence from VASPs are generally in place across MONEYVAL jurisdictions, their effectiveness is contingent on the scope of VASP regulation, the availability of international cooperation channels, and the technical capacity of FIUs and LEAs. The emergence of DeFi and privacy-enhancing technologies continues to pose challenges, underscoring the need for ongoing policy development and capacity building.

Special Investigatory Tools

121. As noted in the introduction to this chapter, blockchain technology offers inherent advantages for financial investigations, particularly due to its transparency and immutability. While private blockchain networks exist, most mainstream VAs operate on public blockchains, allowing FIUs and LEAs to independently access transaction data without relying solely on reporting entities. However, meaningful analysis of such data requires specialised tools and technical expertise.

122. Responses from MONEYVAL jurisdictions indicate a growing but uneven adoption of blockchain analytical tools. Nearly all jurisdictions reported using either public blockchain explorers or commercial forensic platforms. These tools enable investigators to trace transactions, cluster wallet addresses, identify counterparties, and detect links to illicit activity. Nonetheless, several jurisdictions noted that they still rely heavily on open-source intelligence due to limited access to commercial tools or budgetary constraints.

123. Among the jurisdictions that have acquired commercial blockchain analytics platforms, the most cited features sought during procurement included:

- Clustering and attribution capabilities: the ability to group wallet addresses and transactions to identify intermediaries and potential malicious actors.
- User-friendly interfaces: tools that do not require deep technical knowledge of blockchain or virtual asset ecosystems.
- Exportable and readable outputs: support for generating reports and visualisations suitable for evidentiary use or intelligence sharing.
- Reliable and up-to-date data: continuous updates to reflect emerging typologies, new tokens, and evolving risk indicators.
- Cost-effectiveness: balancing functionality with affordability, particularly for smaller jurisdictions.

124. Some jurisdictions, such as Bulgaria, Estonia, and Georgia, have developed detailed protocols for the seizure and analysis of VAs, including the use of multi-signature wallets and secure custody procedures. Others, such as Malta and the Isle of Man, have leveraged public-private partnerships to enhance investigative capacity and share typologies across sectors.

125. Despite these advancements, several jurisdictions acknowledged gaps in their technical capabilities. In some cases, FIUs and LEAs outsource blockchain analysis to private sector experts, akin

to the use of forensic specialists in traditional investigations. This approach has proven effective in complex cases involving mixers, privacy coins, or cross-chain obfuscation techniques. Bosnia highlighted a great example of jurisdictional cooperation: in situations where they needed a deeper analysis or verification of VA transactions, the Republic of Serbia, whose competent institutions use the IT tool, came to their aid and performed checks using this tool, which significantly contributed to their investigations.

126. The use of blockchain analytics tools has also facilitated cooperation with foreign jurisdictions. For example, Estonia and Malta reported successful asset freezes and intelligence sharing with counterparts in the United States and other EU Member States, often initiated through Egmont Secure Web or mutual legal assistance frameworks.

127. In summary, while the adoption of special investigatory tools for virtual asset analysis is increasing across MONEYVAL jurisdictions, disparities remain in access, expertise, and integration into broader investigative workflows. Continued investment in training, tool acquisition, and inter-agency cooperation will be essential to ensure effective detection and prosecution of ML/TF involving VAs.

4.5 Freezing and Seizure of VAs

128. MONEYVAL members were asked to describe the mechanisms available for imposing interim measures on VAs, including freezing and seizure procedures. A significant number of jurisdictions provided detailed insights into their legal and operational frameworks, revealing a diverse landscape of practices and challenges.

129. Of the respondents, six jurisdictions either provided no information on how they would freeze and seize VAs or reported that they either did not have any experience, regulatory framework or processes in place to seize VAs. Two of these jurisdictions are looking at appointing a third-party provider to hold any seized VAs.

130. Most jurisdictions indicated that freezing and seizure of VAs typically involves cooperation with VASPs that hold custody of the assets. In such cases, LEAs or prosecutors issue formal orders—either judicial or administrative—requiring the VASP to freeze the assets in question. Several jurisdictions, including Bulgaria, Georgia, and Malta, reported the use of official or government-controlled wallets to transfer and securely hold seized VAs. These wallets are often managed by designated law enforcement or asset recovery units and may include multi-signature or hardware wallet configurations to ensure integrity and security.

131. Where VAs are not held by a VASP, the ability to seize assets depends on whether LEAs can obtain access to the wallet keys. Jurisdictions such as Serbia and Lithuania reported cases where seed phrases or hardware wallets were discovered during searches and subsequently used to transfer assets to government-controlled wallets. In such instances, seizure is treated similarly to physical evidence and is subject to chain-of-custody protocols.

132. A recurring challenge highlighted by MONEYVAL members is the extraterritorial nature of many VAs. Assets may be held by VASPs located in foreign jurisdictions, or on decentralised platforms with no identifiable operator. In these cases, LEAs rely on international cooperation mechanisms, such as Mutual Legal Assistance (MLA) requests or European Investigation Orders (EIOs), to pursue freezing or seizure. However, several jurisdictions expressed concern about the timeliness and effectiveness of these channels, noting that delays can result in the dissipation of assets.

133. Some jurisdictions reported success in engaging directly with foreign VASPs, requesting voluntary cooperation to freeze or hold assets pending formal legal requests. While this approach has yielded positive outcomes in certain cases, its success is highly dependent on the VASP's internal

policies and willingness to cooperate. Others noted that some VASPs require court orders issued in their jurisdiction, adding further complexity to cross-border enforcement.

134. FIUs in several jurisdictions have the power to impose temporary freezing measures at the pre-trial stage. These postponement powers allow for the suspension of transactions or the freezing of accounts for a limited period, providing a critical window for LEAs to initiate formal seizure procedures. Jurisdictions such as Cyprus, Estonia, and Hungary reported using these powers effectively to prevent asset flight in high-risk cases.

135. The practical implementation of freezing and seizure measures varies widely. Some jurisdictions have developed detailed protocols, including the use of blockchain analytics tools to trace assets, secure transfer procedures, and asset management frameworks. Others are still in the process of developing such capabilities or rely on ad hoc arrangements.

136. The importance of international cooperation was repeatedly emphasised. Jurisdictions cited examples of successful collaboration with foreign FIUs, law enforcement agencies, and VASPs, often facilitated through platforms such as the Egmont Secure Web, INTERPOL, or Europol. These partnerships have proven essential in tracing and recovering assets across borders.

137. In conclusion, while MONEYVAL members have made notable progress in developing mechanisms for freezing and seizing VAs, challenges remain, particularly in cases involving decentralised platforms or foreign VASPs. Continued investment in legal frameworks, technical capacity, and international cooperation will be essential to ensure effective enforcement in this evolving domain. The Guide on Seizing Cryptocurrencies developed under the iPROCEEDS-2 project remains a valuable resource for jurisdictions seeking to enhance their capabilities in this area.

4.6 Training and Upskilling

138. The rapid evolution of VAs and VASPs has necessitated significant investment in training and upskilling for law enforcement agencies (LEAs), FIUs, prosecutors, and supervisory authorities across MONEYVAL jurisdictions. The complexity of VA-related investigations, the technical nature of blockchain analytics, and the emergence of new regulatory requirements (such as the Travel Rule and TFS) have all driven demand for specialist knowledge and practical skills.

139. Training and upskilling are recognised as critical enablers for effective supervision, investigation, and enforcement in the VA/VASP sector. While significant progress has been made, ongoing investment is required to keep pace with technological change, regulatory developments, and the evolving threat landscape. Peer learning, international cooperation, and practical, hands-on training are emerging as best practices across the region.

Training Key Findings

140. *Widespread Training Initiatives*: Nearly all jurisdictions reported that their LEAs and FIUs have participated in training on VAs and VASPs between 2022 and 2024. Training has been delivered by a mix of international organisations (e.g., Council of Europe, Europol, CEPOL, INTERPOL, OSCE, UNODC), private sector vendors, and national authorities.

141. *Focus Areas:* Training topics include blockchain analysis, tracing and seizure of VAs, investigation of crypto-related money laundering and cybercrime, use of open-source and commercial blockchain analytics tools, and the application of AML/CFT obligations to VASPs. Increasingly, sessions also address TFS enforcement and the Travel Rule, though coverage remains uneven.

142. *Specialist Units and Knowledge Transfer*: Several jurisdictions have established specialist cybercrime or financial crime units within police or prosecution services, with dedicated staff

receiving advanced training in VA investigations. In some cases, IT professionals have transitioned into compliance or supervisory roles, highlighting the sector's technical demands.

143. *FIU Training:* FIUs have also invested in upskilling, with staff attending international conferences, workshops, and vendor-led certification courses. Many FIUs now routinely participate in joint training with LEAs and supervisors.

144. *Peer Learning and International Cooperation*: Cross-border workshops, regional working groups, and joint exercises (e.g., EMPACT, Egmont Group, FATF, Basel Institute) have played a key role in disseminating good practices and building networks for operational cooperation.

Training Comparative Insights

145. *Coverage of TFS and Travel Rule*: While most jurisdictions have included TFS and Travel Rule topics in at least some training events, only a minority report systematic, in-depth coverage. For example, Bulgaria, Gibraltar, and Malta specifically mention targeted sessions on TFS and the Travel Rule, while others (e.g., Andorra, Montenegro, Slovakia) note only brief or incidental coverage.

146. *Variation in Depth and Frequency*: The frequency and depth of training varies widely. Some countries (e.g., Lithuania, Bulgaria, Cyprus, Isle of Man) report dozens of events, including advanced workshops and vendor certifications, while others (e.g., Moldova, North Macedonia) have more limited activity, often due to the absence of a domestic VASP sector.

147. *Tools Training*: Training increasingly includes hands-on use of blockchain analytics tools, with some jurisdictions investing in multi-year licenses and structured certification pathways for investigators and analysts.

Training Challenges and Gaps

148. *Resource Constraints*: Not all supervisors and LEAs are comprehensively resourced in terms of staffing and knowledge. Smaller jurisdictions, or those at an early stage of VASP regulation, often rely on external support or ad hoc training.

149. *Keeping Pace with Change*: The rapid evolution of VA typologies, obfuscation techniques, and regulatory requirements means that ongoing, iterative training is essential. Several jurisdictions highlight the need for continuous professional development and regular updates to training curricula.

150. *Quality and Relevance*: There is a risk that training remains too academic or generic, rather than tailored to the specific operational challenges faced by LEAs and supervisors. Peer learning, case studies, and practical exercises are increasingly recognised as best practice.

4.7 Statistics on Investigations, Seizure, Freezing, and Confiscation of VAs

151. Of the twenty-five respondents, sixty percent provided responses that evidenced they had investigated cases involving VA.

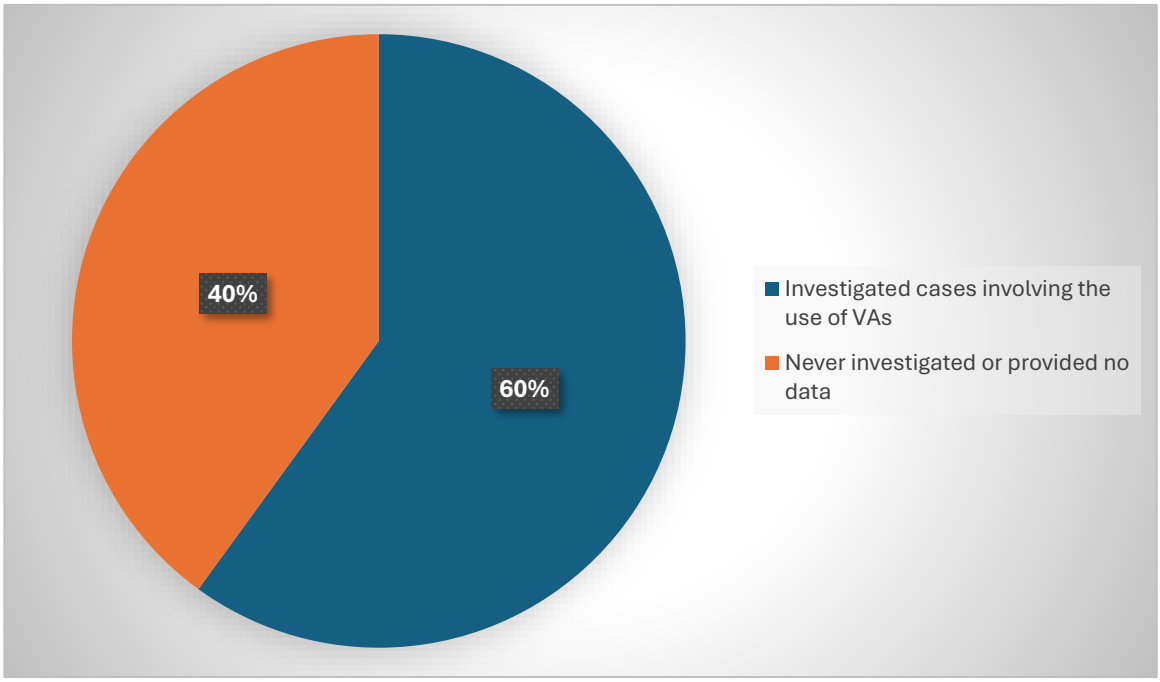

Figure 7 - Jurisdictions investigating VA-related ML

152. This data shows little change from 2023 when, from an albeit smaller sample, 38% of responding MONEYVAL members had not investigated cases involving VA and 62% had investigated cases involving VA.

4.8. Case Studies

Case Box 13 - Illegal Migration Scheme Paid in Cryptocurrencies – Moldova

An organised criminal group led by "G.I." used Moldova as a transit zone for Ukrainian citizens seeking to reach the EU. The group leveraged social media to recruit migrants and coordinated payments and logistics using VAs.

Modus Operandi:

1. **Recruitment:** Ukrainian citizens affected by conflict were targeted via social media.
2. **Payment:** Migrants paid fees of $2,000–$2,500 per person, transferred in cryptocurrency (USDT) to a VA account.
3. **Logistics:** After payment, migrants were instructed to travel to Odessa, then guided to cross the Moldovan border illegally. They were picked up in Moldova, temporarily housed in Chișinău, and then assisted in leaving for EU states.
4. **Scale:** Total cryptocurrency received: 1,167,784.64 USDT (approx. $1.17 million) deposited into the group's Binance account during the period.

Distinctive Features:

- Use of encrypted communications and strict operational security.
- High level of conspiracy and cross-border coordination.
- Payments exclusively in VAs to avoid detection.

Case Box 14 - Unauthorised Financial Activity and Investment Fraud – Hungary

The Hungarian FIU (HFIU) received several Suspicious Activity Reports (SARs) about an individual who received approximately EUR 6.25 million to his payment account, with references to "loan agreements" and "crypto." Funds were transferred to and from various VASPs and payment accounts.

Key Elements:

- The individual provided "investment services" by purchasing VAs for customers' wallets, but customers had no access to their wallets.
- The individual engaged in trading activities with the VAs, without proper authorization.
- The HFIU determined this was unauthorised financial activity—a criminal act.

Actions Taken:

- The case was referred to the competent investigative authority, which launched a criminal investigation.
- The financial supervisory authority banned the individual from continuing the activity as an interim measure.
- Bilateral meetings were held to support the investigation.

4.9 Mixers, Tumblers and Privacy Enhancing VAs

153. Mixers and tumblers are privacy-enhancing tools used in the virtual asset ecosystem to obscure the origin, destination, and ownership of funds. These services aggregate VAs from multiple users, shuffle them through complex transaction chains, and redistribute them in a manner that breaks the traceable link between sender and receiver. While not inherently illegal, their use is strongly associated with illicit activity, including money laundering, sanctions evasion, and darknet market transactions.

154. Jurisdictions such as Estonia and Georgia have identified mixers and privacy coins as high-risk typologies. Estonia's Financial Intelligence Unit published guidance outlining how mixers are used in sanctions evasion, including techniques like chain-hopping and escrow structures. Georgia explicitly prohibits VASPs from offering services involving anonymity-enhanced assets. These tools are also linked to ransomware payments and fraud schemes, where criminals exploit their obfuscation capabilities to frustrate law enforcement tracing efforts.

155. The misuse of mixers and tumblers undermines the transparency of blockchain transactions and poses significant challenges for regulators and investigators. As such, several MONEYVAL jurisdictions have begun integrating these typologies into national risk assessments and supervisory

strategies, recognising their role in facilitating financial crime within the VA space. For instance, Gibraltar identifies privacy-enhancing assets and mixing services as high-risk and outside its regulatory appetite, and Bulgaria included mixers and privacy coins in its 2023 sectoral ML/TF risk assessment for VAs/VASPs, referencing international typologies.

156. Privacy-enhancing mechanisms can be implemented in all other typologies linked to VAs and VASPs; they add a further level of complication and obscurity. These findings complement the earlier findings in this report:

a) Stakeholder Distribution Chart: highlights the need for deeper engagement with VASPs, especially around high-risk asset types.
b) Reported Outcomes Chart: typology development and improved STR quality are key outcomes of PPPs, which are essential for identifying risks linked to privacy-enhancing assets.
c) PPP Presence Chart: with only 40% of jurisdictions having active PPPs, there's a clear opportunity to expand collaboration to address emerging threats like mixers and privacy coins.

5. VASPs and Targeted Financial Sanctions

157. Several public sources highlight the use of VAs for circumventing TFS. These have largely been a biproduct of the regime utilising stable coins to try and mitigate hyperinflation.[5] This section of the report outlines the measures taken by members related to VAs/VASPs and TFS.

5.1 Oversight of VAs/VASPs on TFS compliance and available sanctions

158. Among the 26 jurisdictions that responded, two indicated the absence of a legislative framework for VASP registration and licensing. Therefore, these two jurisdictions lacked an established authority to oversee VASP compliance with targeted financial sanctions (TFS). These jurisdictions cannot conduct any oversight over VAs/VASPs and are unable to impose any sanctions. Moreover, the jurisdictions who reported to have regulations in place to conduct the oversight address quite differently the sanctioning of VASPs for the failure to enforce the TFS-related measures. In most cases, there are certain legal instruments which allow to impose administrative or criminal penalties as well as to revoke or suspend the license for the violation of TFS regime. These are often the same legal instruments regardless of the type of firm they are being applied to.

5.2 Training on VAs/VASPs and TFS

159. There are several countries which have no registered VASPs at the time of querying, and for this reason there is no training provided. Some jurisdictions have published practical guides addressing TFS compliance. Some entities offered several online courses, including on the topic of TFS, while some jurisdictions offered training in a physical format.

160. The importance of training extends beyond VASPs themselves. As VAs become increasingly integrated into financial systems and criminal typologies, it is essential that supervisory authorities,

5. For example, the March 2025 RUSI Round Table Report "*Sanctions in the Virtual Asset Industry*" highlights the use of Virtual Assets and circumventing TFS on Iran, see: Sanctions in the Virtual Asset Industry: SIFMANet Roundtable Report. The 2025 Crypto Crime Report by Chainalysis further builds on this: "*Sanctioned jurisdictions and entities received $15.8 billion in cryptocurrency in 2024, accounting for about 39% of all illicit crypto transactions. In total, OFAC issued 13 designations that included cryptocurrency addresses — slightly fewer than in 2023 — but still the second highest in the last seven years.*", see: 2025 Crypto Crime Trends from Chainalysis.

financial intelligence units (FIUs), LEAs, and other public sector bodies receive targeted education on the risks and regulatory expectations surrounding VAs. This includes understanding the technological features of VAs, the typologies of misuse (e.g. sanctions evasion, fraud, proliferation financing), and the tools available for blockchain analytics and transaction tracing.

161. Training should also be extended to sectors indirectly exposed to virtual asset risks, such as gambling regulators, tax authorities, and customs enforcement, especially in jurisdictions where VAs are used in gaming, real estate, or cross-border commerce. Without a broad base of institutional knowledge, jurisdictions risk overlooking emerging threats or failing to enforce compliance effectively.

162. Moreover, cross-sectoral training fosters collaboration and improves the quality of suspicious transaction reporting (STRs), particularly when public–private partnerships (PPPs) are in place. Jurisdictions that have invested in multi-stakeholder training—covering both technical and regulatory dimensions—report stronger investigatory outcomes and more proactive risk mitigation strategies.

163. In summary, while VASP-specific training is vital, a holistic approach to capacity building across all relevant sectors is necessary to ensure robust enforcement of TFS obligations and keep pace with the evolving virtual asset landscape.

5.3 Guidance for VASPs on TFS

164. The approach to publishing TFS-related guidance for VASPs varies widely. Only a few countries have not published any materials on the topic, while most responding jurisdictions have issued guidance or recommendations for the virtual asset (VA) sector. Not all documents are available in English, which may pose challenges for non-native English-speaking service providers.

165. Many jurisdictions publish whole jurisdiction guidance and ask sectors to tailor the guidance to their individual circumstances.

5.4 STRs related to VAs and circumvention of TFS

166. Only a few countries provided numbers of reports related to VAs and circumvention of TFS, and these numbers remain relatively small. Only one jurisdiction demonstrated a large number of received reports regarding circumvention of TFS where the *modus operandi* included VA.

5.5 E-Gaming and Online Gambling

167. Only a few jurisdictions recognise VAs as an acceptable payment solution for the online gaming sector. In those that do, the use of VAs is typically subject to regulatory oversight, including the enforcement of TFS compliance measures.

168. The integration of VAs into online gaming platforms introduces significant risks of abuse, particularly in relation to sanctions evasion. Criminal actors and sanctioned entities may exploit the relative anonymity, speed, and global reach of VAs to move funds through gaming platforms that accept such assets. For example, sanctioned individuals may deposit VAs into gaming accounts, use in-game transactions to obscure the origin of funds, and then withdraw them as fiat or other assets, effectively laundering the proceeds and bypassing financial restrictions.

169. Gaming firms that accept VAs are therefore exposed to the risk of becoming conduits for sanctions circumvention. This is especially true where customer due diligence (CDD) and transaction monitoring controls are weak, or where blockchain analytics tools are not employed to screen wallet

addresses against sanctions lists. The use of privacy-enhancing technologies, such as mixers or anonymising wallets, further complicates detection and enforcement.

170. To mitigate these risks, jurisdictions that permit VA use in gaming typically impose enhanced licensing conditions, require regular reporting of VA transactions, and mandate the use of blockchain analytics tools. Supervisory authorities may also increase the frequency of inspections and require firms to demonstrate robust TFS screening procedures.

171. Ultimately, the effective regulation of VA use in gaming requires a coordinated approach involving regulators, financial intelligence units, and the gaming industry itself, supported by strong public–private partnerships and continuous training on emerging typologies and compliance expectations.

5.6 Risk Assessment on VAs/VASPs including TFS evasion

172. Only some jurisdictions responded that they had addressed the TFS related risks in their risk assessments. Several jurisdictions did not reflect these topics in their previous NRAs, but most likely are going to cover it in the upcoming risk assessments and NRAs.

173. An appropriate TFS-related risk assessment identifies where exposure to sanctions-evasion risk resides - by sector, product/service and customer segment. This enables proportionate allocation of controls (e.g., enhanced due diligence, screening of transactions) to identify, mitigate and report certain cases.

5.7 DeFi services regulation in terms of TFS

174. In most responded jurisdictions, there is either a lack of decentralised finance (DeFi) regulation or there are no known DeFi service providers. Some jurisdictions highlighted that if they would have DeFi types of service providers, then the local VASP-related regulation would be applied to them. In this case, it would mean the automatic enforcement of AML/CFT and TFS compliance.

175. Decentralized platforms can facilitate financial transactions without traditional intermediaries, making it more challenging to identify and restrict sanctioned individuals or entities. As the usage of DeFi ecosystems grows rapidly and enables cross-border, pseudonymous transactions, the risk of misuse for sanctions evasion and proliferation financing increases significantly.

176. Regulatory measures to mitigate TFS risks within DeFi are essential to prevent decentralized financial systems from being misused for sanctions evasion, terrorism financing, or other illicit activities.

177. As DeFi operates without traditional intermediaries, the lack of clearly defined accountability can undermine the effective implementation of asset-freezing and sanctions-screening obligations. Introducing proportionate and technology-neutral regulations helps address these compliance gaps, enhance transparency, and ensure that DeFi developments remain consistent with international AML/CFT and TFS requirements.

5.8 LEAs enforcing TFS

178. The legislative frameworks governing the approach of Law Enforcement Authorities (LEAs) to the investigation of TFS-related offences vary significantly across jurisdictions. In some jurisdictions, breaches of TFS obligations are treated as criminal offences and investigated by specialized law enforcement agencies, while in others, such violations are addressed through

administrative measures and regulatory actions. Developing clear and harmonized frameworks that define the scope of TFS violations, outline investigative responsibilities, and specify the roles of competent authorities would strengthen the effectiveness and proportionality of enforcement measures.

179. Enhancing inter-agency cooperation, improving information sharing, and investing in capacity building among law enforcement and supervisory bodies would further support the timely detection, investigation, and resolution of TFS breaches, thereby reinforcing overall compliance and alignment with international standards.

Expedited processes for intelligence gathering in TFS-related investigations

180. Expedited processes for obtaining information from Virtual Asset Service Providers (VASPs) in TFS-related cases are vital for ensuring timely and effective sanctions enforcement. In most jurisdictions, the collection of such information is governed by national criminal or administrative procedure laws, which require all entities, including VASPs, to provide relevant data to competent authorities upon request.

181. These frameworks allow authorities to quickly access transaction records, customer details, and other pertinent information, thereby facilitating the prompt identification, freezing, and investigation of assets linked to designated persons or entities in line with TFS requirements.

Specific procedures for TFS enforcement in case of extraterritorial element.

182. International cooperation in the enforcement of TFS generally follows the same foundational principles and legal frameworks as cooperation in other financial crime matters, such as money laundering or terrorist financing. This includes reliance on established mechanisms such as Mutual Legal Assistance Treaties (MLATs), the Egmont Secure Web for FIU-to-FIU communication, and regional instruments like European Investigation Orders (EIOs).

183. While the procedural basis remains consistent, the urgency and geopolitical sensitivity of TFS cases, particularly those involving sanctioned states or entities, often demand faster response times and more proactive engagement. In practice, this means that effective TFS enforcement relies heavily on timely intelligence sharing, the use of blockchain analytics to trace virtual asset flows, and the willingness of jurisdictions to act swiftly on freezing or seizure requests.

Additional steps required for TFS-related measures regarding the freezing and seizing obligation

184. Clear and harmonized guidance would help financial institutions and other obliged entities act swiftly and accurately when identifying and freezing assets associated with designated persons or entities. Enhancing the legal and procedural foundations in this area would significantly strengthen the effectiveness, consistency, and timeliness of TFS implementation across jurisdictions.

LEA and FIU trainings covering TFS

185. TFS-related trainings are vital for enabling competent authorities to detect and respond effectively to the sanctions' circumvention cases involving virtual assets. Such trainings strengthen the practical use of blockchain analytics tools, improve understanding of emerging evasion methods, and support the timely implementation of freezing and reporting obligations.

186. It was highlighted that the LEAs as well as Financial Supervisory Bodies of some countries did participate in the training events which covered the topic of TFS enforcement. TFS-related training modules are usually implemented into the blockchain analytical software users' trainings.

Blockchain investigation tools with TFS screening capability

187. It may be useful to note that the choice of blockchain analytics tools often depends on cost, available features, and national procurement processes. Some jurisdictions also combine multiple tools to enhance coverage, as no single provider offers full visibility across all blockchains.

188. Jurisdictions may benefit from ensuring that the selection and use of blockchain analytics tools align with their risk profiles and the types of virtual asset activities present in their markets, as recommended by the FATF risk-based approach.

Case Box 15 – Circumvention of TFS – Estonia

The investigation case described below is related to the circumvention of TFS.

Company G was registered in Estonia and held a license to provide virtual-asset / cryptocurrency-related services. However, it mostly operated from another country and involved customers from high-risk jurisdictions. Conducted oversight and inspections by FIU of Estonia uncovered the following serious deficiencies:

- Weak or insufficient risk management, internal controls, and procedures.
- In over 90% of cases, failures in the KYC procedure.
- Failures by the company to systematically report suspicious transactions (as required under AML/CTF laws) to the FIU.
- Discovery that part of the funds passing through Company G were linked to crime or wallets used by criminals.

Due to the detected issues, the FIU of Estonia concluded that the deficiencies were systematic and sustained. As a result, Company G's license to offer virtual-currency services in Estonia was revoked.

Subsequently, a criminal case was initiated, with the former board members accused of continuing to provide virtual-asset services without a valid license in Estonia (after the license was revoked).

In December 2024, Harju County Court convicted the former board members of Company G of aiding the unauthorised provision of financial services (i.e. assisting in operating without a license). The Court held that their involvement was via omission (i.e. doing nothing, allowing the company's operations to continue) in the period after the license was revoked.

Case Box 16 – Lessons Learned – Gibraltar

In Gibraltar, the lessons learned from the difficulties with direct and indirect sanctions exposure concepts in relation to Bitcoin (BTC) and "change", as well as other issues with VAs that "taint" the asset, have led to policy decisions to bring criminal charges against VASPs when their clients carry out transactions with a sanctioned entity.

Gibraltar is also moving to implement a dedicated civil penalties regime for sanctions breaches through amendments to the Sanctions Act 2019, designed to complement rather than replace existing criminal and regulatory powers. The framework will broadly follow the United Kingdom's civil enforcement model, empowering a designated authority to impose proportionate monetary penalties of up to a maximum of £1 million or 50% of the value of the funds or economic resources involved, alongside a graduated range of other outcomes including warnings, regulatory referrals and publication of enforcement action. Civil penalties will be imposed on the balance of probabilities, supported by clear rules on representations, internal review and appeal to the Supreme Court, thereby providing a more flexible and responsive means of addressing sanctions breaches and systems failings while reserving criminal prosecution for the most serious and culpable misconduct.

Case Box 17 – International Cooperation – Ukraine

One example of successful international cooperation was the investigation of a scheme to circumvent sanctions and launder funds through a well-known cryptocurrency exchange (Crypto Exchange A) linked to sanctioned public figures. Cooperation between the FIU of Ukraine, foreign financial intelligence units, reporting entities (banks), as well as the use of open sources intelligence (OSINT) and blockchain analysis made it possible to detect the transfer of over USD 140 million from a crypto exchange subject to sanctions (Crypto Exchange B) to Crypto Exchange A after the introduction of TFS.

The exchange of financial information via Egmont Secure Web (ESW) channels between the FIUs and the use of blockchain intelligence analytical tools played a key role in detecting the transactions, allowing links to be established with darknet platforms, North Korean hacker groups and Iranian exchange offices.

This case is an example of the effective implementation of TFS in practice and demonstrates the importance of the rapid exchange of information between the FIUs, in particular regarding suspicious transactions in VAs.

6. Travel Rule Compliance

189. The Travel Rule is part of the preventive measures applied to VASPs and financial institutions. This section of the report examines how MONEYVAL jurisdictions comply with the so-called "*Travel Rule*" obligations, which requires the collection, transmission, and availability of originator and beneficiary information in virtual asset transfers, ensuring that this data can be provided to competent authorities when requested.

6.1 General information

190. Travel Rule obligations mirror the standards already applied to traditional wire transfers, extending them to VAs transactions in order to promote traceability and strengthen the safeguards against misuse. The framework also sets thresholds for occasional transactions and includes provisions on cross-border cooperation, which together shape how jurisdictions and service providers are expected to apply the rule in practice.

6.2 Definition of the Travel Rule and core obligations

191. The Travel Rule is addressed in paragraph 7(b) of the FATF Recommendations Interpretive Note under Recommendation 15. It links VASPs to Recommendation 16 requirements for originator and beneficiary information on virtual-asset transfers. Under this requirement, countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Beneficiary providers are also required to obtain and retain the originator's details together with accurate beneficiary information, and to make this data available to authorities when requested. The broader framework further requires ongoing monitoring of the availability of this information and the application of TFS, including freezing actions or prohibitions on dealings with designated persons and entities. Financial institutions that process virtual asset transfers on behalf of customers are subject to the same obligations, ensuring consistency between traditional financial intermediaries and VASPs.

192. Although these requirements are central, the framework also sets a threshold of USD/EUR 1 000 for occasional transactions, which has a practical impact on how firms implement customer due diligence and related transfer requirements. In addition, the provisions on international cooperation highlight the importance of supervisors and authorities exchanging information promptly and constructively across borders, reinforcing the effective implementation and enforcement of the Travel Rule.

6.3 Travel Rule implementation and challenges

193. When comparing these international obligations with what MONEYVAL members reported, a few recurring themes stand out. The most frequently cited elements across the questionnaires are training, guidance, and regulation. Several supervisors have conducted outreach events and training sessions where the Travel Rule was introduced, often alongside TFS. These initiatives help build awareness, yet they remain uneven. Some jurisdictions only began including dedicated Travel Rule modules after the EU Funds Transfer Regulation entered into application at the end of 2024.

194. At the same time, most jurisdictions formally acknowledge the Travel Rule in their AML and CFT frameworks, but its practical enforcement is still at an early stage. While legal bases, supervisory

responsibilities, and some tools are in place, effective and consistent implementation is slowed by gaps in training, limited guidance, weak monitoring of cross-border transfers, and a lack of Travel Rule–specific reporting. Explicit requirements, whether in law, regulation, or supervisory codes, are confirmed in the majority of jurisdictions. In EU Member States, these obligations arise directly from Regulation 2023/1113, while among non-EU jurisdictions, some have introduced dedicated Travel Rule codes or amended their national anti-money laundering legislation to ensure coverage of virtual asset transfers.

195. Guidance and training on the Travel Rule are becoming increasingly common, with many supervisors providing seminars, webinars, or e-learning programmes specifically focused on this requirement. In non-EU jurisdictions, compliance is only partial, as provisions have been planned but are not yet fully in force, often because they are awaiting alignment with EU crypto-asset regulations or tied to scheduled implementation dates. Non-implementation is limited to a very small minority, usually in jurisdictions where the broader regulatory regime for VASPs is not yet operational.

196. Turning to practical supervision, some jurisdictions report testing Travel Rule solutions as part of licensing processes or on-site inspections. Others describe record-keeping conditions or address-whitelisting requirements that indirectly support compliance, though such measures are far from universal. A small number of responses refer to lessons learned from practical cases, such as gaps in sanctions screening at providers; however, overall explicit feedback loops feeding back into policy adjustments remain scarce.

197. In addition to these measures, authorities also highlight the use of blockchain analytics tools by financial intelligence units and LEAs. These tools can screen sanctioned wallets, trace flows, and verify originator and beneficiary details. While this strengthens investigative capacity, it often works as a downstream control. True Travel Rule implementation requires upstream, automated information exchange between providers, which remains limited.

198. Enforcement mechanisms are formally established in many legal frameworks, where breaches of sanctions obligations or missing transfer data are classified as serious offences. However, actual cases of sanctions imposed specifically for Travel Rule violations are almost absent. References to un-hosted wallets also appear only occasionally, with some jurisdictions introducing risk-based controls such as verification and enhanced monitoring instead of outright bans. Statistical evidence is weak. VA–related suspicious transaction reports represent only a small portion of total filings, and none of the submissions clearly identify Travel Rule failures as triggers. This suggests either very early implementation or underdeveloped detection and reporting pipelines, or that jurisdictions are utilising other parallel legal frameworks to supervise and impose sanctions on those breaching Travel Rule obligations.

199. Cross-border monitoring is similarly inconsistent. Some supervisors already apply value-transfer obligations to VA transfers and are preparing structured monitoring under the EU regulation, while others continue to rely on firm-level vigilance and ad-hoc reporting. International cooperation channels such as the Egmont Secure Web, INTERPOL, and EUROPOL are regularly used, underlining the dependence on cross-border information exchange to make the Travel Rule operational in practice.

200. In conclusion, MONEYVAL jurisdictions show solid progress in setting up the legal and supervisory infrastructure for the Travel Rule. Training programmes, public registers, sanctioning powers, and investigative tools are gradually taking shape. Yet, the decisive test of consistent, end-to-end compliance in daily provider operations remains ahead. To bridge the gap, jurisdictions will need to publish more detailed guidance, collect specific Travel Rule metrics, expand training beyond awareness into practice, and develop structured mechanisms for cross-border data exchange. Until

these steps are in place, compliance with the Travel Rule will remain more of a legal formality than a fully functional safeguard.

Case Box 18: Travel Rule implementation – Latvia

Latvia applies the EU Transfer of Funds Regulation (2023/1113) for Travel Rule compliance and the Markets in Crypto-assets Regulation (2023/1114) for licensing and prudential requirements. From 30 December 2024, the licensing of CASPs was transferred from the State Revenue Service to Latvijas Banka, with AML/CFT supervision to be completed by June 2025.

CASPs are treated as financial institutions under the AML/CFT Law. Latvijas Banka has issued AML licensing guidance and an AML Handbook that includes provisions on TFS and customer due diligence. A new chapter covering CASP-specific requirements, including Travel Rule implementation, is in preparation. Supervisory arrangements include quarterly reporting on crypto-asset transfers and planned use of blockchain analytics for monitoring both on-chain and off-chain transactions, including those linked to self-hosted wallets.

In 2024, CASPs filed six suspicious transaction reports, representing 0.11% of the national total. Issues noted in reporting include transfers involving unhosted wallets. Sanctioning measures are set out in Section 78 of the AML/CFT Law, enabling supervisory authorities to issue warnings, fines, or licence suspensions, while the FIU is empowered to impose freezing orders. TFS are applied under the Law on International and National Sanctions.

At the end of 2024, 23 CASPs were operating in Latvia. This number is expected to change in 2025 following the entry into force of EU regulations.

Case Box 19: Travel Rule implementation – Gibraltar

Gibraltar has incorporated the FATF Travel Rule into its regime for VAs and service providers through the Proceeds of Crime Act 2015 and the Transfer of Virtual Assets Regulations 2021. These define "virtual asset" and "virtual asset service provider" and place transfer activities under AML/CFT/CPF oversight. The Gibraltar Financial Services Commission (GFSC) is the responsible authority, licensing DLT Providers under the Financial Services Act 2019 and registering other VASP activities. Its supervisory powers include inspections, information requests, directions, financial penalties, suspension or withdrawal of licences, and enforcement of TFS under the Sanctions Act 2019.

Implementation is carried out through guidance and supervision. In October 2024, the GFSC issued revised AML/CFT/CPF Guidance Notes with a chapter on Travel Rule compliance and TFS. Training activities have included sessions with Travel Rule content, such as a 2024 webinar. In late 2024, the GFSC conducted a thematic review on the Travel Rule and considered expanding the Financial Crime Supervisory Return to include data on self-hosted wallets and non-compliant transfers.

Supervision is supported by data and technology. All VASPs must submit an annual Financial Crime Supervisory Return, which is analysed through a dashboard to identify anomalies and cross-border patterns. Different IT tools are used by the GFSC for address screening and exposure analysis, as well as for sanctions-screening functions.

Operational data indicates an increasing proportion of suspicious transaction reports from the VASP sector, rising from 8.26% in 2022 to 30.34% in 2024. The GFSC maintains a public register of authorised entities and has applied enforcement measures, including licence cancellation, with related information shared through international supervisory cooperation. Gibraltar is also consulting on

additional guidance for Travel Rule compliance, developing a unified licensing framework for VASPs, and exploring a public–private partnership for supervisory information-sharing.

Annex I: Links to VASP Registers and/or Licencing/ Registration Requirements by Jurisdiction

Albania	https://amf.gov.al/#
Andorra	https://www.afa.ad/en/entitats-supervisades/digital-assets/participants-actors-relacionats-amb-els-actius-digitals/participants-or-actors-related-to-digital-assets?set_language=en
Azerbaijan	https://sandbox.cbar.az/az/registry
Bosnia and Herzegovina	https://www.secrs.gov.ba/Ucesnici/PruzaociUsluga.aspx
Bulgaria	https://www.fsc.bg/registri-i-spravki/registar-po-paragraf-5-al-3-ot-zakona-za-pazarite-na-kriptoaktivi/
Cyprus	https://www.cysec.gov.cy/en-GB/entities/crypto-asset-services-providers-casps/casp-register/, https://www.cysec.gov.cy/en-GB/entities/crypto-asset-services-providers-casps/eea-casps/
Czechia	https://jerrs.cnb.cz/apljerrsdad/JERRS.WEB07.INTRO_PAGE?p_lang=cz, https://fau.gov.cz/povolovaci-rizeni-pro-nft
Estonia	https://mtr.ttja.ee/tegevusluba?m=97 https://fi.ee/en/investment-market/crypto-asset-service-provider-casp/investment-market/crypto-asset-service-provider-casp
Georgia	https://nbg.gov.ge/en/page/virtual-asset-service-providers-vasps
Gibraltar	https://www.fsc.gi/FSC/distributed-ledger-technology-providers
Guernsey	https://www.gfsc.gg/industry-sectors/lending-credit-and-finance/regulated-entities
Hungary	https://intezmenykereso.mnb.hu
Isle of Man	https://www.iomfsa.im/register-search/
Latvia	https://uzraudziba.bank.lv/en/market/crypto-asset-market/crypto-asset-service-providers/
Lithuania	https://www.registrucentras.lt/jar/sarasai/vvko.php https://www.registrucentras.lt/jar/sarasai/dvvpo.php
Malta	https://www.mfsa.mt/financial-services-register/
Moldova	Not available

Monaco	Not available
Montenegro	Not available
North Macedonia	Not available
Romania	Not available
San Marino	https://www.sanmarinoinnovation.com/dlt / https://www.bcsm.sm/hubfs/Regolamenti/Regolamento%20n.%202024-03/Reg.2024-03%20Agg.%20I.pdf?hsLang=en
Serbia	https://nbs.rs/en/ciljevi-i-funkcije/nadzor-nad-finansijskim-institucijama/digital-imo/reg_di/index.html https://www.sec.gov.rs/index.php/en/public-registers-of-information/register-of-service-providers-related-to-digital-tokens
Slovakia	https://subjekty.nbs.sk/sk/?s=1414
Slovenia	https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.gov.si%2Fassets%2Forgani-v-sestavi%2FUPPD%2FDokumenti%2FSeznam-ponudnikov-storitev-virtualnih-valut%2FSeznam-ponudnikov-storitev-virtualnih-valut%2FSeznam-ponudnikov-storitev-virtualnih-valut-.docx&wdOrigin=BROWSELINK
Ukraine	Not available

Annex II: Links to Websites Providing Guidance for VASPs by Jurisdiction

Albania	https://amf.gov.al
Andorra	https://www.uifand.ad/en
Azerbaijan	Not provided
Bosnia and Herzegovina	https://www.secrs.gov.ba
Bulgaria	https://www.dans.bg
Cyprus	https://www.cysec.gov.cy/en-GB/home/
Czechia	https://fau.gov.cz/metodicke-pokyny
Estonia	https://www.fiu.ee
Georgia	https://nbg.gov.ge https://www.fms.gov.ge/ka
Gibraltar	https://www.fsc.gi/guidance_notes
Gurnsey	https://www.gfsc.gg
Hungary	https://www.mnb.hu/web/fooldal
Isle of Man	https://www.iomfsa.im
Latvia	https://www.vid.gov.lv/lv https://www.bank.lv
Lithuania	https://fntt.lrv.lt/lt/
Malta	https://fiaumalta.org
Moldova	Not available
Monaco	Not available
Montenegro	https://scmn.me/me/
North Macedonia	Not available
Romania	https://www.onpcsb.ro
San Marino	https://www.aif.sm
Serbia	https://www.nbs.rs/sr_RS/indeks/ https://www.sec.gov.rs/index.php/en/
Slovakia	https://www.minv.sk
Slovenia	https://www.bsi.si/sl
Ukraine	Not available

www.coe.int/MONEYVAL

December 2025

MONEYVAL

Typologies Report

Practice of Using Virtual Assets, Virtual Asset Service Providers in the Laundering of Criminal Property, Financing of Terrorism, and the Evasion of Sanctions

This Typology Report presents a horizontal review of regulatory and supervisory measures adopted by MONEYVAL jurisdictions; in doing so it highlights significant progress in regulation, supervision, and international cooperation in the field of VAs/VASPs.

Typologies report