MONEY LAUNDERING AND TERRORIST FINANCING RISKS IN THE WORLD OF VIRTUAL ASSETS

www.coe.int/moneyval

TYPOLOGIES REPORT

2023

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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 and terrorist financing risks in the world of virtual assets was adopted by the MONEYVAL Committee at its 65th Plenary Session (Strasbourg, 26 May 2023).

French version:
Les risques de blanchiment des capitaux et de financement du terrorisme dans le monde des actifs virtuels

Cover design: Council of Europe
Photo: Shutterstock

Table of Contents

List of Abbreviations

AML/CFT	Anti-Money Laundering/Combatting the Financing of Terrorism
AMLD	Anti-Money Laundering Directive
ATM	Automated Teller Machine
CDD	Customer Due Diligence
CEPOL	European Union Agency for Law Enforcement Training
CoE	Council of Europe
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
DNFBP	Designated Non-Financial Businesses and Professions
EAG	Eurasian Group on Combating Money Laundering and Financing of Terrorism
ECOFEL	Egmont Centre of FIU Excellence and Leadership
EDD	Enhanced Due Diligence
EGMONT	Egmont Group of Financial Intelligence Units
EEA	European Economic Area
EU	European Union
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FUR	Follow-Up Report
IT	Information Technology
LEA	Law Enforcement Authority
MER	Mutual Evaluation Report
MLA	Mutual Legal Assistance
ML/TF	Money Laundering/Terrorist Financing
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures
NFT	Non Fungible Token
NPO	Non-Profit Organisation
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBA	Risk Based Approach
SAR	Suspicious Activity Report
SNRA	EU Supranational Risk Assessment
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
VA	Virtual Asset
VASP	Virtual Asset Service Provider

1. Introduction

This report aims to present in an integrated manner an overview of the money laundering and financing of terrorism risks in the world of virtual assets and their service providers in MONEYVAL members. The report includes a horizontal analysis of MONEYVAL members' level of compliance with Recommendation 15, an overview of the measures taken to regulate and supervise the virtual asset service providers (VASP) sector as well as some features of the identified risks that criminals use VASPs and virtual assets (VA) to launder proceeds of crime (i.e., exchanges, exchange offices, aggregators, and other cryptocurrency platforms including e-gaming, sports betting and NFTs).

The report was prepared by a team led by the Project Leader Mr David Baker (Isle of Man) with the support of experts from Gibraltar, Malta, Principality of Monaco, Slovak Republic and Slovenia. Estonia and the Cybercrime Division of the Council of Europe reviewed the draft report.

In the preparation of the report the project team:

a) Prepared and distributed a questionnaire to which 15[1] MONEYVAL members contributed.
b) Performed a literature review of published reports and documents, including those from the Financial Action Task Force, the EGMONT Group, CoE and private sector.
c) Conducted two project team meetings and one extended typology meeting[2] where all MONEYVAL members and observers were invited to comment on and discuss the report.

The study integrates and analyses data obtained from MONEYVAL members across multiple issues relating to: 1) how members regulated the activity of issuance of VAs and operation of VASPs; 2) whether the LEAs have adequate powers and tools to investigate, locate and impose interim measures in respect of VAs, 3) the types of VA platforms used for financial support of criminal activity; 4) examples of cases investigated by the relevant authorities with a description of criminal schemes involving the virtual asset elements that have been identified; and 5) other data relevant to the goals of the study.

Taking the above into account, the report is structured into four sections; Horizontal review of compliance with R.15; assessment of VA and VASP risks; RBA supervision of the VASP sector; Law enforcement and operational issues.

[1] Albania, Andorra, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Germany, Gibraltar, Hungary, Isle of Man, Latvia, Lithuania, Malta, Serbia, Slovak Republic, Slovenia.
[2] The Typologies meeting took place on 22 March 2023.

2. Key Findings

- MONEYVAL members are at varying stages in their implementation of Recommendation 15. Most members require major or moderate improvements. Better results were achieved in areas where the VASPs were included as reporting entities in the national AML/CFT Law. Some members have made better progress than others.
- The VA and VASPs risk assessment at national level often starts with an inventory of the registered entities in the jurisdiction and determining the materiality of the sector. Members reported that it was challenging to accurately determine the materiality of the sector.
- When assessing the risk, different entities pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, business models and the strength of the entity's compliance program. In more advanced jurisdictions the risk analysis also considers the results of the supervisory actions.
- The use of technology when identifying and assessing risks in this sector appears to be a good practice. To better understand and mitigate the risk, some countries purchased blockchain risk evaluation tools and the supervisor trained employees in Blockchain analysis.
- Licensing, registration and regulation remain a challenge, mainly due to the capacity of the designated supervisor to fully understand the risks and the particularities of the sector.
- The difference between registering for the purposes of AML / CFT oversight and being licensed can have a significant impact in the prevention of crime and the management of an industry. Some members report that registration is still not enough, as less reputable firms use the registration as a stamp of legitimacy, and their customers rarely understand the difference between registration and regulation.
- MONEYVAL members report difficulties in detecting unlicensed/unregistered VASPs in practice.
- In supervising the VASP sector most of the MONEYVAL members are at the beginning of implementation. Not all supervisors are comprehensively resourced in terms of staffing and knowledge, and the RBA is rarely tailored on a sector specific risk assessment.
- The collection of statistics relating to VAs and VASPs would improve the assessment of risk, particularly in the jurisdictions that need to identify domestic unregistered VASPs or external VASPs operating in the jurisdiction.
- Monitoring of cross border transactions is still a problematic issue (e.g., issue with the application of travel rule).
- The majority of MONEYVAL members are receiving a negligible amount of STRs from VASPs. It is evident that the regulation and supervision of VASPs has a positive impact on STR reporting awareness and volumes.
- Concerns with the quality of VASP reports are noted. Contributing factors include (i) the overreliance on technological tools to detect potential suspicious transactions which can assist in identifying red flags but cannot completely replace human analysis and expertise; (ii) defensive STRs being reported; (iii) outsourcing of AML/CFT obligations including transaction monitoring; (iv) lack of AML/CFT expertise; and (v)

misunderstanding of reporting obligations in situations where VASPs operate in multiple jurisdictions.

- Fraud and child sexual exploitation were highlighted as prevalent predicate offences identified by VASPs
- ML/TF investigation responsibility is most often not determined on the basis of the cases' *modus operandi* (e.g., whether it involves VAs), but rather on the type of underlying crime. Smaller countries tend to have one central LEA responsible for all ML/TF investigations.
- Sourcing of financial intelligence is heavily dependent on the designation of VASPs as reporting entities. Members mostly reported that the legal powers to collect evidence throughout ML/TF investigations also cover information held by VASPs and VAs.
- There are difficulties in gathering evidence from VASPs located in foreign jurisdictions, and MLA channels are not efficient in ensuring timely seizure of VAs located abroad.
- The majority of FIUs and LEAs are lacking appropriate technological tools and expertise to effectively analyse and investigate VA related ML/TF cases. It is however evident that there is investment in training and cooperation with VASPs to build expertise.
- The ability to seize and freeze VAs is dependent on the presence of a VASP intermediary and/or the possession of the private keys providing controls over the VAs.
- Only a small fraction of ML/TF investigations involve proceeds of crime that are VAs. This indicates difficulties in detecting and investigating VA related ML/TF cases. The value of frozen and confiscated proceeds of crime that are VAs is negligible.

3. MONEYVAL members' compliance with FATF Standards on VAs and VASPs: a state of play

The global AML/CFT Standards for VAs and VASPs are set out in FATF Recommendation 15[3]. The FATF has published documents that are aimed at helping jurisdictions and private sector to comply with the new AML/CFT requirements for VAs and VASPs[4].

Due to the peculiarities of the sector and the (relatively) recent adoption of the standard, the vast majority of MONEYVAL members have not yet fully implemented these requirements. Of the 23 jurisdictions that have been assessed since June 2021 for their compliance with R.15, the majority require major or moderate improvements. In particular, further improvements are needed on assessing ML/TF risks, supervision and the application of AML/CFT preventative measures. The section below provides a detailed analysis on the compliance of MONEYVAL members with specific obligations outlined in each relevant criterion of R.15.

The following MERs and FURs of 23 member jurisdictions (that are only assessed by MONEYVAL[5]) as of April 2023 have been analysed: Albania, Andorra, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Gibraltar, Holy See (including Vatican City State), Hungary, Isle of Man, Liechtenstein, Lithuania, Malta, Republic of Moldova, Principality of Monaco, Poland, San Marino, Serbia, Slovak Republic, Slovenia and Ukraine. Two members (Latvia and Armenia) have not been assessed against the new requirements of R.15 in the follow-up process.

One MONEYVAL member – the Holy See (including Vatican City State) - has prohibited VAs. For the purposes of this horizontal review their compliance with criteria 15.1, 15.2, 15.3(a), 15.3(b), 15.5 and 15.11 has been reflected in the analysis. As criterions 15.4, c.15.6 – 10 are not applicable to this jurisdiction, the tables of horizontal review reflect a N/A as assigned sub-rating.

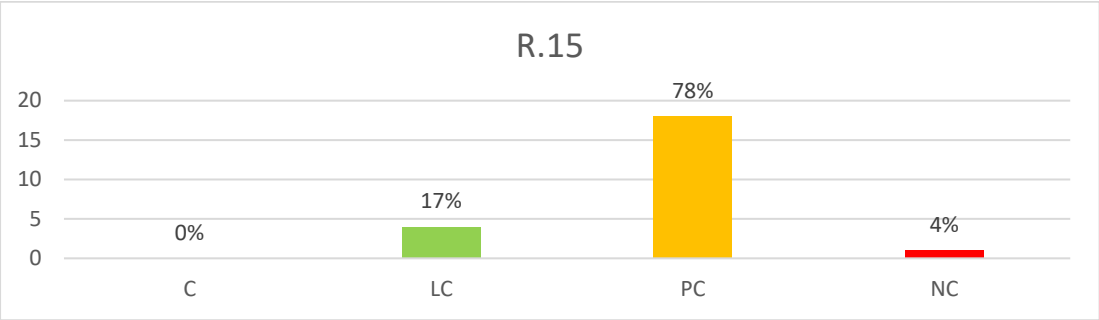
Around 80% of the assessed members do not comply or only partly comply with the requirements of R.15. None fully complies with FATF's requirements in relation to VAs and VASPs.

[3] Criterions 15.1 and 15.2 have not been assessed in detail as they do not exclusively cover obligations in relation to VAs and VASPs.

[4] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (October 2021) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>; Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020) <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html
>; Targeted Update on Implementation of FATF's Standards on VAs and VASPs (June 2022) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html >

[5] Compliance of Israel, Germany and United Kingdom with the requirements of R.15 have not been taken into account for the purposes of this horizontal review.

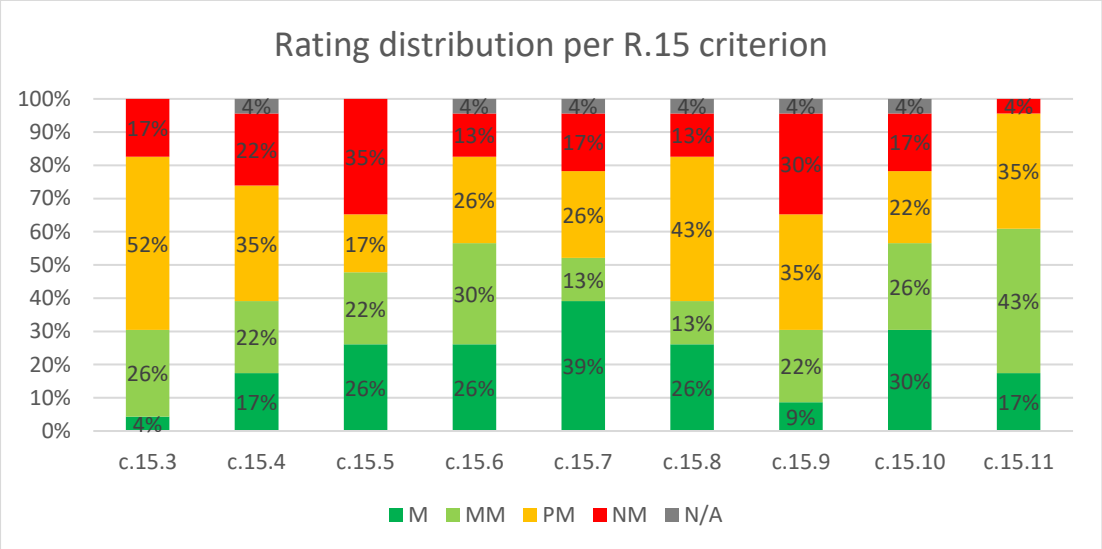
Chart 1 – Compliance with R.15 among assessed MONEYVAL Members



* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

While the deficiencies vary in each jurisdiction, the horizontal analysis indicates that better results were achieved in respect of those criteria where the domestic legal setting is so that the introduction of VASPs as reporting entities in the AML/CFT Law would automatically lead to the introduction of: supervision and monitoring, obligation for the supervisors to issue guidance, inclusion of obligations in relation to targeted financial sanctions and international cooperation. The requirements regarding undertaking specific risk assessments and the implementation of preventive measures (mostly due to travel rules issues and sources / destinations not being able to be monitored) appeared to be – even at technical level – more challenging.

Chart 2 - Comparison of levels of compliance across different criteria of R.15



* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

When analysing the results of compliance of MONEYVAL members with R.15 it must be noted that the first two sub-criterions are not directly related to the issue of VA and VASPs, nonetheless they still may influence the overall rating of technical compliance either positively or negatively.

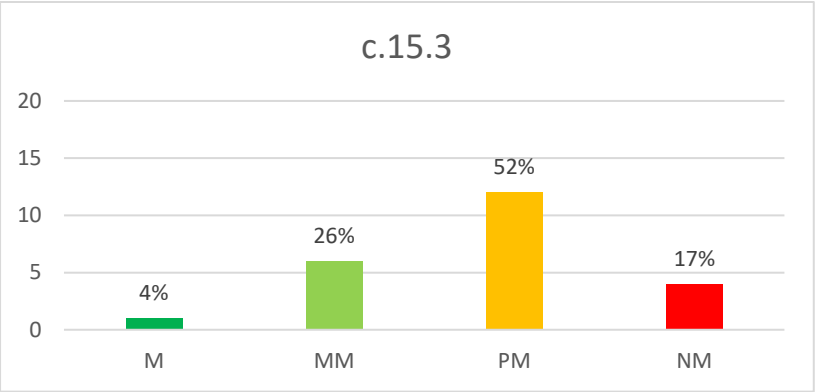
3.1. Assessing and understanding risks – seems like a risky business (c.15.3)

Assessing the specific VA related risks proved to be one of the most problematic areas with only 30% of members reaching a higher level of compliance. When conducted, the risk assessments are equally stand-alone or included in the NRAs. The requirements for the VASPs themselves to

identify, assess and manage the risks, are often addressed through the extension of the AML/CFT obligations already in place for the FIs and DNFBPs.

An interesting observation on the compliance of MONEYVAL members with c.15.3 is that the risk assessment was not comprehensive, and the information used to conduct the risk assessment (qualitative and quantitative) was not up to date. The countries that have either just started regulating VAs and VASPs or have a small VASP sector tended to have more academic risk assessments that heavily relied on information (publications) from international organisations.

Chart 3 – Compliance with c.15.3

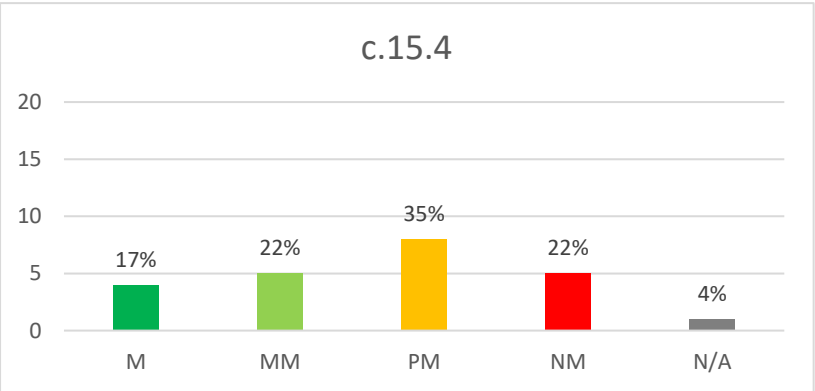


* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.2. Licensing and registration – still a challenge (c.15.4)

Of the assessed members, around 39% obtained a higher rating for the obligation to register or license VASPs. Nevertheless, even when such a requirement was in place, difficulties occurred in its application, as due to their nature, VASPs can operate in different jurisdictions without being registered and physically present. Solutions to address this challenge included identifying VASPs promoting themselves in the official language of the country or who provided services that are available to residents. Local intermediaries seeking clients or visiting resident potential clients might be a trigger for registration requirements. Some members failed to extend the registration or licensing regimes to natural persons that conduct VASP activities for business.

Chart 4 – Compliance with c.15.4

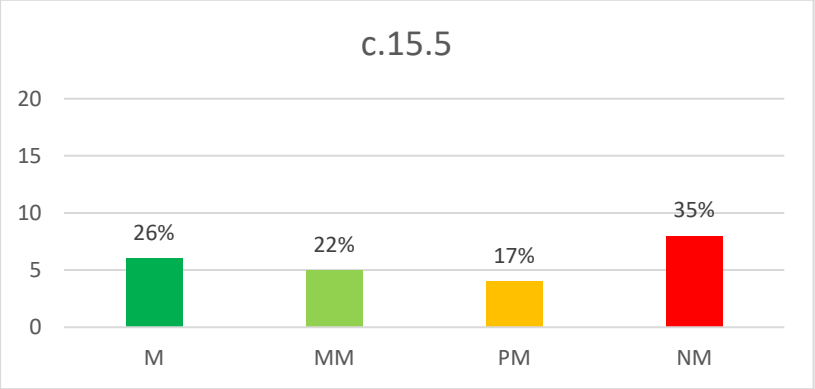


* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.3. Identification of un-licensed or un-registered VASPs – a drop of effectiveness into the technical compliance (c.15.5)

The identification of unregistered or unlicensed VASPs is done mostly through media monitoring including blogs in the fintech realm and by third-party reports. Another avenue used to identify unregistered VASPs is through on-site inspections by the registration authority. The first step to achieve compliance on this front is to adopt provisions prohibiting unregistered or unlicensed VASPs accompanied by a meaningful sanctioning regime for non-compliance cases. A lack of visibility and limited understanding on how VASPs can operate in their jurisdictions is an issue for detecting unlicensed activities. Also, where licensing/registration regimes were not extended to natural persons, authorities are not required to detect if such unlicensed/unregistered business is occurring.

Chart 5 – Compliance with c.15.5

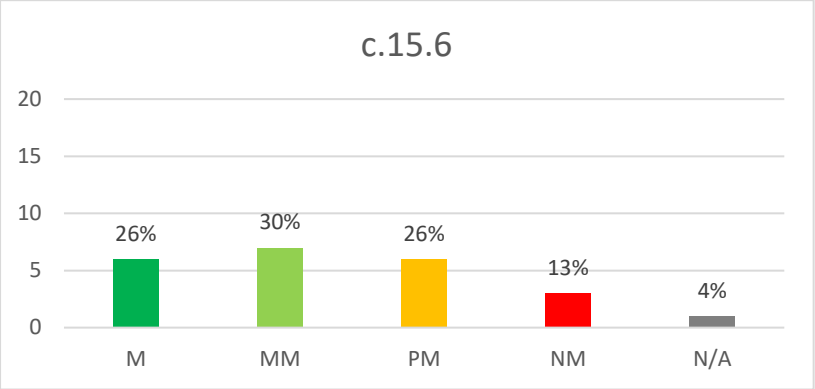


* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.4. Supervision and monitoring – it pays off to go with the flow (c.15.6)

The allocation of supervision and monitoring powers appears to be one of the requirements with the higher level of compliance in the overall context of R.15. In many cases the responsibility to supervise VASPs was given to an already established supervisory body, usually the Financial Service Authority, FIU or other experienced competent authority, which appears to be a good solution. One of the main challenges in supervising the VASPs is the allocation of staff which rarely is commensurate with the materiality of the sector. Another challenge identified relates to staff's level of knowledge and skills on how VAs function, and the application of the risk-based supervision, which cannot be achieved in the absence of a high level of compliance with the first criterion analysed above (15.3). Simply applying the same methods of supervision between sectors does not work.

Chart 6 – Compliance with c.15.6



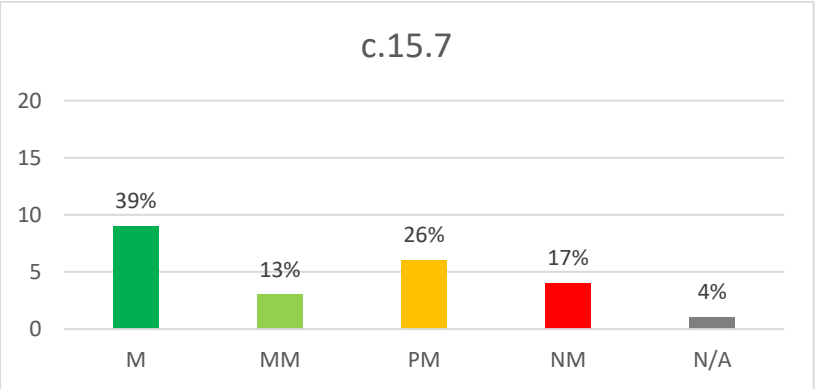
* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.5. Guidelines and feedback – what comes around goes around (c.15.7)

Another rather positive finding related to the capability of competent authorities and supervisors to develop guidelines, and provide feedback, to assist VASPs in applying AML/CFT measures to combat ML/TF, in particular, for detecting and reporting suspicious transactions to the FIU. When including the VASPs amongst the reporting entities, all requirements pertaining to guidelines and feedback would apply. In addition, countries who fully met the requirement issued specific instructions and recommendations applicable for the VASPs sector.

The sector is driven by enthusiastic members, who are generally sourced from a technical background due to the close ties between VAs and the information technology sector. This results in compliance team members often having an IT background and expertise rather than a compliance one. For this reason, feedback is very important to elevate the level of compliance with the AML/CFT requirements.

Chart 7 – Compliance with c.15.7



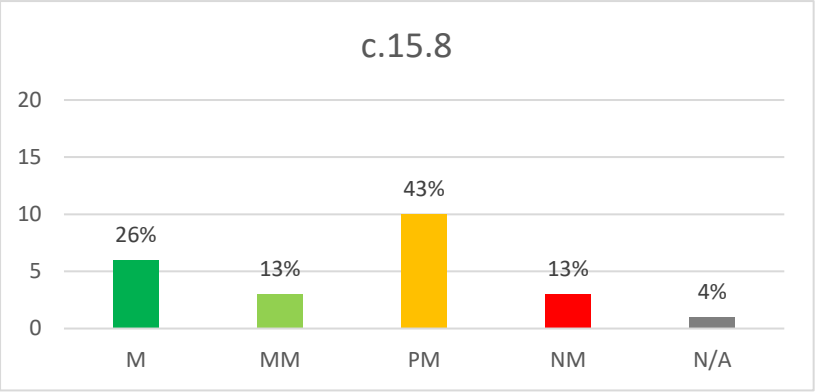
* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.6. The sanctioning regime in case of failure to comply – the stick and the carrot (c.15.8)

The sanctioning regime follows the same approach as the supervisory arrangements namely through the inclusion of VASPs in the list of reporting entities that extends supervisory powers

to this sector. This approach places this criterion amongst those with higher level of compliance. The issues in complying with this criterion are the limited scope (e.g., inability to remove license) and the range of sanctions that were not proportionate nor dissuasive.

Chart 8 – Compliance with c.15.8



* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

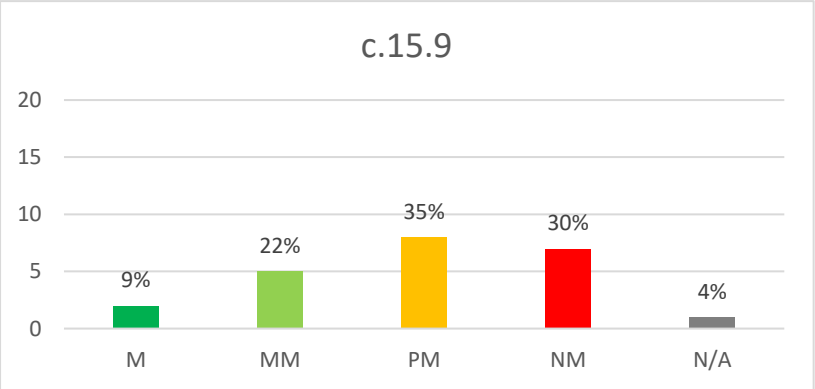
3.7. Applying preventive measures to VASPs (c.15.9)

Although it might appear that the preventive measures requirements can be easily implemented through the mere inclusion of the VASPs amongst the reporting entities, together with FIs and DNFBPs, the ratings show limited compliance, with only 9 % of the members achieving a met rating and 22% mostly met.

Some of these difficulties to reach a higher level of compliance for applying preventive measures are due to systemic deficiencies which are likewise applicable to FIs and DNFBPs (e.g., CDD, EDD, reporting regime, recordkeeping etc.).

Further separate issues relate to the requirements for the travel rule and the provision of information on the beneficiaries of transfers.

Chart 9 – Compliance with c.15.9

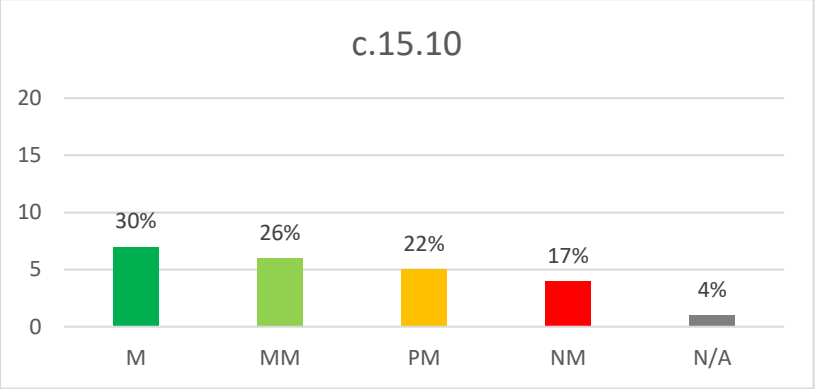


* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.8. Targeted financial sanctions are…targeted (c.15.10)

Compliance is achieved through the application of the same rules and mechanisms used for FIs and/or DNFBPs. A deficiency observed in members that are not compliant with this criterion is that the TFS obligations are not extended to VASPs.

Chart 10 – Compliance with c.15.10

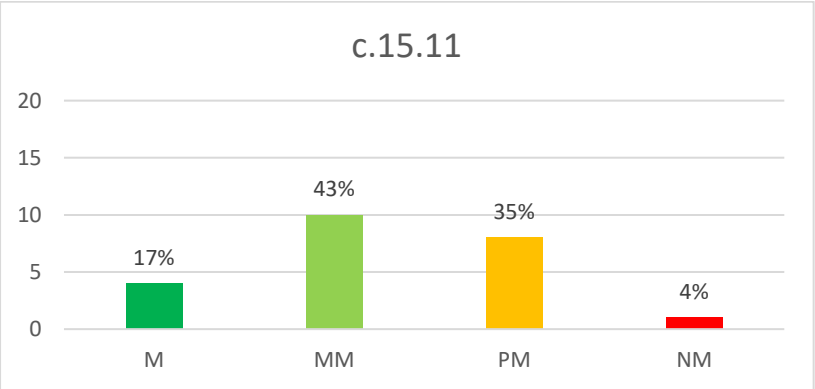


* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

3.9. International cooperation – the strong link (c.15.11)

The highest level of compliance with R.15 is to be found in relation to the capacity of authorities to provide the widest range of international cooperation to foreign counterparts when it comes to VAs. The positive outcome is based on authorities' wide powers to exchange information, regardless of the type of assets involved. The deficiencies that are identified in relation to c.15.11 relate to more systemic issues and are cascading from R.36-R.40.

Chart 11 – Compliance with c.15.11



* Table shows sub-ratings of 23 MONEYVAL members achieved in mutual evaluation and follow-up process.
** Some numbers (%) have been rounded up or rounded down.

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

As described under the horizontal review of R.15 above, not all members have assessed the ML/TF risk posed by VAs and VASPs, or if such risk assessment has been conducted in many cases it lacks depth.

Case Box 1: VA and VASP risk assessment - Andorra

Andorra carried out its second NRA, completed in December 2020, benefitting from a two-level study (both national and sectoral) and an independent risk assessment of both the NPOs and of the VAs sector.

The study of the VAs sector included a section devoted to the main definitions applicable (including the definition of "virtual asset", "virtual asset service provider", "digital currencies", "virtual currencies", as well as "cryptocurrencies"). The risks detected in relation to VAs and VASPs, include: (i) anonymity; (ii) the cross-border nature of transactions, (iii) the lack of homogeneous regulations on a global scale; and (iv) the need for further training and upskilling on the topic of VAs and VASPs.

The NRA also looked at the risk through the prism of the applicable international standards, including the FATF Recommendation 15, its Interpretative note, the content of the 5th AML Directive, as well as some other considerations.

A separate section covered the presence of VAs and VASPs in the Principality of Andorra. This section covers not only the applicable legal framework, but also the impact on other economic sectors. Existing public-private initiatives using blockchain technology in Andorra were also looked at.

The NRA concluded with major findings, identified risks and risk mitigation measures. The overall ML associated with VASPs sector in Andorra was determined as high.

The survey showed that the risk assessment at national level would start with an inventory of the registered entities in the jurisdiction and determining the materiality of the VASP sector. This inventory is a straight forward process, when VASPs must be licenced or registered, leaving the authorities with the tasks of estimating if and to which extent unregistered entities are still servicing clients in the respective jurisdiction. However, in practice jurisdictions experience challenges in identifying unregistered or unlicensed VASP activity in their jurisdiction.

When no specific registration is required, countries must rely on the declarations made by the legal persons in the commercial register on the type of activities (or object of activity) they undertake. Based on those declarations, the authorities apply a filter to identify those legal persons offering VA related services. This approach is less reliable to evaluate the number of VASP operating in the country, as errors (unintended ones) may occur when declaring the object of activity, or when the object of activity is too broad to determine the exact type of activities provided by certain operators which would qualify a company as VASP.

Following the first inventory of VASPs, a more in-depth analysis of the sector is undertaken, usually starting with a questionnaire sent to the entities registered (or licensed) as VASPs, or to those who potentially could provide VASP-like services. There is a risk that if the work conducted by the jurisdiction indicates that there are no businesses operating domestically that should be registered, then VAs and VASPs become less of a focus. An assessment must be made about the use of VAs in the country even if there are no registered VASPs (for instance, whether customers in the domestic jurisdiction are obtaining services in another jurisdiction).

Where it is identified that there are registerable businesses, different entities within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, business models and the strength of the entity's compliance program. When launching its sectoral strategic analysis relating to VASPs countries assessed:

- how many and which registered institutions act as operators of virtual currency wallets and virtual currency exchange offices;
- who are their clients: number of natural and legal persons; number of domestic nationals, EU and third country citizens;
- how many of the individual VASPs' clients are assigned as higher-risk clients (number and percentage of overall clients' population);
- the scope of activities: the value of operations, the country of origin and destination of incoming and outgoing funds.

In more advanced jurisdictions the risk analysis also considers the results of the supervisory actions such as the level of VASPs' compliance with CDD obligations for transactions exceeding €1,000. Financial intelligence sourced through STRs is also an important source of information when determining the potential ML/TF risks in the sector, where VA and VASPs related STRs are filed. On a less positive note, the review shows that the overreliance on technology to detect STRs has a negative impact on their quality (see section 6.1.2).

Case Box 2: Virtual Financial Asset Service Providers (VFASPs), Virtual Financial Assets and new emerging technologies - Malta

Malta launched the update of the National Risk Assessment in March 2021. The methodology adopted focused on constructive discussions with set-up working groups and discussions with the private sector representatives. The objective of this update of the NRA was to gain (also from working group discussions) a sufficiently granular appreciation of the actual threats and vulnerabilities faced by the different analysed sectors.

Different working groups were set up to assess the threats and vulnerabilities presented by a particular sector or area of activity. Each working group was composed of those authorities which have the most in-depth knowledge of the given sector, with one of them also assigned to lead the group. The process has been improved considerably when compared to the one leading to the 2018 NRA and has led to a more detailed and accurate assessment of what are the main threats, vulnerabilities, and overall risks that Malta faces with respect to ML, TF, and PF. The Virtual Financial Asset Service Providers (VFASPs), Virtual Financial Assets and new emerging technologies was one such sectoral working group that was chaired by the Malta Financial Services Authority (MFSA), and included officials from the Financial Intelligence Analysis Unit (FIAU), the Asset Recovery Bureau (ARB), the Office of the Attorney General (OAG), the Malta Police Force (MPF), the National Coordinating Committee on Combating Money Laundering and

Funding for Terrorism (NCC), and private sector representative bodies (VFA Service Providers and VFA Agents).

The data derived from supervisory data held by the MFSA and the FIAU, as well as data held by the MPF, ARB, and the OAG, including:

- Data collected by the MFSA during the licensing process and supervisory data collected following the issue of licenses.
- Data sourced from the FIAU's Compliance and Supervision Platform for Assessing Risk (CASPAR)[6] system, and especially from its sector-specific Risk Evaluation Questionnaires.
- Data from the supervisory and enforcement actions of the FIAU and MFSA.
- More granular data available to the FIAU's Intelligence Analysis Section through the goAML[7] system on suspicious transaction reports (STRs) submitted by subject persons to the FIAU, including on their quality and the predicate offence/s identified by subject persons, as well as data from the requests for information received by the FIAU, be they domestic or international in nature.
- More accurate data from the OAG and the MPF with respect to Mutual Legal Assistance requests, European Investigation Orders, and international cooperation.
- Typologies from the STRs and the financial crime investigations.
- More accurate data on assets seized including crypto assets, frozen and confiscated from the ARB.

The VASPs sector risk analysis is often supplemented by facts and data gathered from reliable studies in the sphere of VAs, issued by international organisations. Nevertheless, at the national level, the sector risk analysis heavily relies on the answers received by the authorities from the private sector itself, with very little actions taken towards the verification of the facts by the supervisor.

Due to VAs and VASPs' reliance on technology, it is relevant for countries to use technology when identifying and assessing risks in this sector. To better understand and mitigate the risks, some countries invested in blockchain risk evaluation tools and trained supervisory staff in Blockchain analysis. This proved to be a good practice overall.

The more advanced LEAs created specialized units to deal with mobile, computer and network forensics and investigation of blockchain technology and VAs, equipped with technical evaluation and analysis tools. Specialists in the investigation and prosecution of cases involving VAs were recruited.

In general, most members conducted a risk assessment of either VAs or VASPs misuse for ML purposes, some also considered TF risks. The majority of these assessments, however, seem to be more academic, heavily relying on sources and information from international reports (including those of the FATF).

[6] In March 2019, the FIAU AML/CFT Supervisory Section adopted an efficient, standardised technology solution named CASPAR to facilitate the dynamic risk assessment of subject persons, risk data collection and risk scoring process. CASPAR system draws in data from a range of sources (such as submitted by reporting entities, supervisors, adverse media, NRA/SNRA, etc.) to allow for the comprehensive risk assessment of individual reporting entities.
[7] goAML was introduced in 2020.

MONEYVAL jurisdictions have assessed the risks of the VASP sector in a varied way, with no uniformity on what risk factors or variables have been taken into account. One MONEYVAL member noted that when it conducted the update to the VASP risk assessment, risks arising from: (i) VA activities (e.g., use of tokens to raise capital and operation of VA trading platforms); and (ii) activities or operations of VASPs were additionally covered. The update draws on additional sets of data not previously available (e.g., cross-border transactions, connections to countries with strategic deficiencies, and beneficial owner by country of customer base).

Due to the limitations in the data gathering presented above, it seems that most members have a limited understanding on the type of VASPs that operate in their territory. This is the case with foreign registered VASPs providing services to domestic clients or domestic non-registered or licensed VASPs. For an in-depth risk assessment, members need a deeper understanding of the sector and its materiality.

5. Supervision of VASPs in Moneyval members

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.

5.1. Different types of VAs and VASPs

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 Virtual Assets is defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of FIAT currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

A Virtual Asset Service Provider (VASP) is any natural or legal person that provides as a business activity one or more of the following activities or operations for or on behalf of another natural or legal person: i)exchange between virtual assets and FIAT currencies; ii) exchange between one or more forms of virtual assets; iii) transfer[8] of virtual assets; iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. The term VASP is technology non-specific, it could include crypto currency businesses, NFT trading sites, ATM operators, wallet custodians and decentralized exchanges.

The analysis shows that not all members included natural persons in the definition of VASPs. In some members, VASPs are only recognized when they operate as a legal person, such as limited liability company. Another limitation of the VASP definition is related to the type of services these entities or persons can perform. Often, the scope of VASP does not extend to entities or persons providing exchange between one or more forms of virtual assets, transfer of virtual assets and participation in and provision of financial services related to an issuer's offer and/or sale of VA.

The jurisdictions that are members of the EU or that align their legislation with the EU legal framework have transposed the 5AMLD. The 5AMLD's coverage of VASPs is not as broad as the FATF Standard. In fact, the 5AMLD does not cover the participation in and provision of services in relation to coin issuance, the provision of VA transfer services, and services of exchange between VAs. Nonetheless, some EU and non-EU members have decided to go beyond the requirements of the Directive designating additional type of services.

There are rare instances of members going beyond FATF standards, with broader definitions that even cover peer to peer transactions. However, it remains to be seen how this would be implemented in practice.

[8] In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

5.2. Regulatory framework

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. According to the information gathered, most members have a legal framework in place to regulate VAs and VASPs. One MONEYVAL member has forbidden any operations with VAs in its jurisdiction.

5.2.1. Licensing or registration regime

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. However, the extent of these regimes differs. For example, some countries apply registration requirements to all persons (natural and legal) conducting VASP activities for business purpose from and to its jurisdiction, except to those already registered as a VASP in other member States of the EEA.

The stringency of the registration or licensing requirements and the type of regime is based on the assessment of the different kinds of VA and VASP activity and the ML/TF risks they are exposed to.

In some jurisdictions, the licensing regime requires VASPs to be registered and not licensed for AML / CFT purposes. The FATF's registration requirements set out may bring along different challenges. While some emphasized the difficulties to register or license due to the nature of the services provided, others reported that VASPs registered consider the lack of a licensing mechanism as an obstacle to the provision of services.

The difference between registering for the purpose of AML/CFT oversight and being licensed can have a significant impact for the prevention of crime and the management of an industry. Some members reported that mere registration is not sufficient, as less reputable firms use the registration as a stamp of legitimacy, where their customers rarely understand the difference between registration and regulation. Without a licensing regime, it is difficult to prove the legitimacy of the business, especially when the business is also to provide services abroad.

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 authorized and supervised by one regulatory authority and a different requirement for the other VASP activities.

The deficiencies that appear somewhat frequently in MONEYVAL members relate to the scope of application, such as for example - the licensing or registration regimes do not extend to natural persons that operate as VASPs but only to legal persons or they do not cover all types of legal persons.

In other countries, foreign VASPs who provide services to the jurisdiction are required to establish a local legal person in an effort to control the use of foreign VASPs. How this works in

practice is however unknown, as without impeding the wider open internet, it would be near impossible to regulate.

Countries also have limited the possibility for natural persons to be registered or licensed as a VASP, due to risk considerations. When natural persons are precluded from offering VA related services, they are considered to be outside of the country's risk appetite.

When considering licensing or registration process, necessary legal or regulatory measures need to be taken to prevent criminals, or their associates, from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP. The regulation of market entry varies across MONEYVAL members, from some having these requirements in place, to others having no regulation in relation to fit and proper checks. The analysis identified that the fit and proper requirements are sometimes only partially addressed, when the checks only cover offences which are linked to the trade or line of trade.

In some MONEYVAL members VAs are used for gaming purposes e.g., sports betting / e-sports / gambling. In such instances members have sought to include specific AML/CFT controls to limit the potential abuse of VAs within the gaming sphere. Examples of specific controls include (i) using only permitted models of VAs that preserve the payment channel for deposits and withdrawals (ii) requiring deposits and withdrawals to be made in the same denomination, (iii) imposing transaction thresholds for withdrawals or deposits and (iv) requiring the use of blockchain analysis tools to identify high-risk flags, focussing on exposure to illicit sources, number of hops from illicit sources, use of mixers, chain hopping, privacy chains, among others

Case Box 3: Licensing online gambling and gaming – Isle of Man

The Isle of Man Gambling Supervision Commission (GSC) licenses and regulates gambling including when a VA is utilised. All licence applicants undergo the same entry control checks when applying for a licence whether using FIAT or VAs or both including understanding and scrutinising beneficial ownership, carrying out due diligence on owners and controllers, conducting source of wealth checks and enhanced due diligence where proportionate.

Financial data and business plans are scrutinised and more attention is paid to models that include the use of VAs, seeking assurances around technology being used; an understanding of ML/TF risks within the use of VAs; and that the models align with the policy of enhanced controls and permissible models of deposit. Additional AML/CFT guidance for VA users is published on the GSC's website and an additional license condition is added to any license holder using VAs to ensure compliance with the GSC's policy on VA use.

All license holders that provide business-to-customer services have requirements to have internal AML/CFT controls. In addition to these controls a license holder using VAs must also apply additional specific controls such as: only operate permitted models of VA use which preserve the payment channel for deposits and withdrawals (i.e. not permitted is the mingling or exchanging of crypto types; or the exchanging of crypto for fiat) as well as thresholds for CDD and EDD.

License holders complete self-assessments on all the AML/CFT controls listed above including the extra requirements for VA use. This assesses their technical compliance. Onsite Inspections are carried out to assess effectiveness of controls along with desk top reviews. A risk-based

approach is used to determine frequency and type of visit. Use of VAs is a risk factor that contributes to risk assessments of license holders and these are updated quarterly.

During an onsite visit, customers using VAs are sampled as part of the inspection including the customers' risk statuses, monitoring, transactions, lifetime deposits, deposit methods and activity. Checks are carried out against the policy, license conditions and guidance.

5.3. AML/CFT supervision or monitoring

5.3.1. Designating the supervisory authority

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. Whichever approach the jurisdiction is taking, in the case of VASP supervision, it should be effective in supervising the sector and minimizing the ML/TF risks.

Case Box 4: Registration of VASP by FMA - Liechtenstein

The Financial Market Authority (FMA) is the competent authority for granting, amending, and withdrawing licenses for FIs, TCSPs and VASPs. The Executive Office (Regulatory Laboratory/Financial Innovation Group) is responsible for the registration of VASPs.

Ahead of registration, the due diligence "concept" of the VASP seeking licensing must be checked by an external auditor and during the registration process the FMA collects detailed information on the implementation of preventive measures.

In the first year following registration, a standard inspection (onsite visit) is performed on the licensed VASPs. The FMA is empowered to issue orders, guidelines, and recommendations for the sector.

5.3.2. Powers of supervisors to adequately monitor the sector and resources

MONEYVAL members implement the supervision and monitoring obligations to a varied degree. 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.

Case Box 5: Powers of Financial Services Commission supervising VASPs - Gibraltar

The Financial Services Commission is the authority responsible for the authorisation and supervision of VASPs operating in or from Gibraltar and has the following powers:

1) carry out on-site examinations;
2) take preventative and corrective measures to ensure compliance;
3) require all information necessary to conduct effective supervision;
4) require the provision of records, information and production of documents etc.;

5) require the provision of a skilled persons report;
6) require the appointment of inspectors;
7) impose financial and administrative penalties;
8) impose a suspension or withdrawal of license/authorisation/registration;
9) impose a temporary ban from managerial/regulated positions;
10) impose directions; and
11) take action against legal or natural persons.

Overall, when considering the supervisory approach to the VASP sector, most of MONEYVAL members are just starting implementation. Due to the recent AML/CFT regulation of VASPs, not all supervisors are comprehensively resourced in terms of staffing and knowledge.

The analysis showed an interesting trend at the supervisor's level: the IT staff becoming supervisory staff to assist in conducting effective supervision of this technology-reliant sector. In some instances, the same trend was noted at the private sector's level, where IT professionals became compliance officers and need to become aware and increase their knowledge of AML/CFT in order to comply with the obligations and manage risks.

5.3.3. Applying a risk-based approach to supervision of VASPs

In the case of supervision, the RBA applies to the way in which supervisory authorities allocate their resources. Among the MONEYVAL members that have implemented supervision for VASPs, not all have taken a comprehensive RBA. The RBA is rarely tailored on a sector specific risk assessment, with most members relying on the more high-level findings of the NRA.

When the risk-based supervision relies on the NRA, the responses to the questionnaire shows some limits such as not addressing the current development of VAs and VASPs. This negatively impacts the application of an effective RBA to supervision.

When effectively undertaken, the risk assessment of the sector is detailed and not only considers the risk in the VASP sector as a whole but looks at risks at entity level. In considering 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, VASPs' level of compliance with AML/CFT measures, as well as the risks associated with specific VA products that undermine transparency.

Case Box: 6 Supervisory Risk Assessment (Virtual Financial Asset Sector) – Malta

Malta's AML/CFT Supervisor the Financial Intelligence Analysis Unit (FIAU) uses an automated tool to risk assess reporting entities that it supervises. Risk assessments are used for various purposes: including to define annual and multi-annual supervisory plans, to enable the choice of entities exposed to specific risks when thematic reviews are undertaken, and to feed into national risk assessment processes among others.

Risk assessments are carried out based on seven main sources of information**:**

(i) AML/CFT Risk Evaluation Questionnaires (REQ) – This is the main source of risk information which is collected from every VASP. Information is obtained on inherent risks and the level of controls (see table below). Questionnaires are sector specific with a particular one tailored for the VASP sector and are issued once a year. Failures to submit such questionnaire are followed up with enforcement action. The FIAU also seeks to validate questionnaire information through cross-comparison of responses to different related questions and through comparison with data obtained from supervisory examinations.

(ii) Prudential Regulator Information – The prudential regulator for the VASP Sector (i.e. the Malta Financial Services Authority) submits a yearly questionnaire highlighting whether particular VASPs have been subject to general prudential controls which raised any concerns.

(iii) Information from the FIU – The Financial Intelligence arm of the FIAU provides information through a questionnaire on a yearly basis to the supervision section of the same entity. This questionnaire includes information on the number and quality of STRs submitted by each VFA.

(iv) Supervisory and enforcement history – Issues and breaches identified in previous AML/CFT supervisory examinations. These are identified through the compilation and collection of post-examination questionnaires, and other questionnaires filled up by the enforcement section providing data on sanctions imposed.

(v) SNRA - The risks of the VASP sector identified in the EU's SNRA are taken into consideration to determine the risk of individual entities within the sector.

(vi) NRA – Similarly the risks identified in the NRA are considered.

(vii) Adverse Information – Any adverse information identified through public or other sources is evaluated, and where considered relevant, is taken into account in the computation of individual entity risk. This allows the risk rating of individual entities to be fluid and able to be tweaked on a continuous basis.

Every inherent risk and control factor within every block has specific weighting assigned to it. These contribute to either increase or reduce the risk. These weightings have been calibrated throughout the years since the CASPAR system has been in use (i.e. 2019). The CASPAR tool based

on this weighting system allocates risk ratings to each VFA and other reporting entities. This classification then helps formulate the yearly and multi-yearly plans, to ensure that VFAs are targeted in accordance with the risk they present. Reference may be made to the following link for further information on the specific data that is collected through the Annual Questionnaire for VASPs (https://fiaumalta.org/caspar-login/#el-fcfb5f8b).

5.3.4. Detecting cross-border flows

The volume and flow of cross-border transactions is one important element that supervisors should take into account when determining the risk of the VASP sector and conducting supervision activities. It is a good practice for the supervisor to request such information from the sector, that can be used to inform the supervisory approach and understanding of the risks.

The analysis identified at least one member which collects data on transactional in-flows and out-flows with other jurisdictions. All regulated entities, including DLT Providers/VASPs are required to submit this information to the supervisor on an annual basis. Each return is then reviewed by the AML/CFT Supervision team. Any potential red flags or irregularities are then either queried with the regulated entity in question or used to inform the ongoing supervision of the entity.

Analysing the cross-border flows may also help to identify if there are any foreign customers of domestic VASPs. For example, according to information provided by one registered VASP to their supervisor, from approximately 9700 clients (i.e. 66%) were domestic. Foreign clients were predominately from other EU and neighbouring countries. Most of the registered VASPs reported that they did not have clients that are PEPs, did not have clients from high-risk third countries, did not carry out transactions linked to high-risk third countries and did not carry out transactions in cash. While these questionaries are an important step to assess and understand the VASPs activities, profiles and risks, the absence of verifications diminishes the reliability of the data. In the case of Bitcoin, although some advances have been made in the attribution of wallets and addresses, it is difficult to reliably identify the country of every transaction, more so when efforts are made to purposefully obscure a destination.

To develop a deep understanding of the VASP market, its structure, and its role in the financial system and the country's economy, supervisors invest in training, personnel, or other resources that enable them to gain the practical skillsets and expertise needed to regulate and supervise the range of VA providers. Some MONEYVAL members are engaging with third sector experts and utilizing the providers of their blockchain analytic tools to provide significant levels of training, others are establishing specific units to manage this area. Smaller jurisdictions are considering outsourcing investigation and risk analysis to third party expert service providers.

5.3.5. Sanctions

The availability of sanctions for VASP supervisors in MONEYVAL members differs in the scope and amounts of the sanctions that can be applied. Therefore, not all members are able to impose a wide range of dissuasive and effective sanctions on the VASP sector.

In some instances, even if the supervisor of VASPs has the necessary powers to impose sanctions for non-compliance, the full range is not always available. While the pecuniary sanctions can be dissuasive, often other penalties are missing from the supervisor's toolbox such as the ability to restrict or suspend the VASP's license.

In other jurisdictions, the possibility to penalize unregistered VASPs or unauthorized activities of VASPs and failure to comply with AML/CFT requirements is either within the range of powers of supervisor or the LEA. Criminal and Administrative Courts can also prohibit the activity where complaints are made. Sanctions can apply to natural persons who carry out unauthorized business as well as to legal persons that conduct VASP activity. One example of enforcement action on a VASP for violating AML/CFT requirements is described in Case Box 7.

When dealing with unregistered VASPs the issue of how to detect them in practice arises. Practically, detecting unregistered VASPs requires education on all levels, LEAs need grass roots training to identify the use of unregistered VASPs through investigation of predicate offences and parallel money laundering investigations. Traditional FIs need education and guidance to identify the flow of fiat currency into such VASPs.

Case Box 7: Enforcement Action – FIAU Malta

The Financial Intelligence Analysis Unit ("FIAU") is the Maltese authority responsible to monitor and enforce AML/CFT obligations. It is also Malta's FIU. VASPs have been regulated for AML/CFT purposes in Malta since 2018.

In 2023 the FIAU imposed a fine of €463,235 on two VASPs forming part of the same group that were providing numerous VA services including exchange services. This enforcement action followed a supervisory examination carried out in 2022, that identified breaches of the following AML/CFT obligations:

(i) Business Risk Assessment (BRA) – The BRA was not appropriate to identify and assess the risks to which the entity was exposed and failed to consider risks associated with the use of VPNs, proxy servers, mixers and tumblers**.** The BRA was also incomplete in that it failed to analyse risk scenarios, the likelihood of their materialising and the resulting impact. Officials also took note of the fact that the BRA was devised just before the on-site examination and not even adopted by the management of the entity.

(ii) Customer Risk Assessment (CRA) - At the time of the examination the entity presented a document with the risk rating pertaining to the customers selected for the review. No explanation or rationale was provided for these risk ratings. The assessment team was also provided with two different CRA methodologies which failed to consider the customer risk, product/service risks and the interface risks, and based customer risk analysis on the nationality and residential address of customers. Jurisdictional risk was also deficient failing to take into account important sources of information e.g. corruption perception index and the EU list of high-risk jurisdictions among others. Shortcomings in specific customer risk assessments were noted in several files which was indicative of a systemic issue

(iii) CDD obligations – (a) No identity verification was carried out for almost half of the customers.

(b) The VASP was not collecting information on the address from which customers were receiving or sending VAs and was unable to determine whether the wallet being used was a private, multi-signature or a custodial wallet. The FIAU expected the VASP to collect information on the wallet.

(c) For more than a third of its customers the VASP failed to collect adequate information on their source of wealth and anticipated level and nature of activity, to build an appropriate profile for

the purpose of on-going monitoring. The FIAU also took note of the fact that there were no actual transaction limits that could have mitigated transactional risks in such cases.

(d) Several on-going monitoring deficiencies were noted. The VASP stated that it monitored transactions over €10,000 using a blockchain analytical tool. Considering the voluminous transactions being processed and the ease with which such transactions are processed, this was not considered an appropriate approach. Moreover, such monitoring system not only had to include post transaction monitoring but also real-time monitoring for high-risk situations such as large value transactions. The officers also identified transactions including a single $1,000,000 for which no purpose information and source of funds were collected.

(iv) EDD obligations – The FIAU also identified a number of cases where EDD was due and was not carried out such as in relation to clients residing in high-risk jurisdictions, and a client who was receiving funds which were described as loans (including one 29.4BTC transaction – over €1,000,000) for which no additional information or supporting documentation was obtained. Typically, in such cases the FIAU, apart from imposing the sanction, would require the client to take remedial action. In this case however, the VASP filed to surrender its license and hence no directive imposing remedial action was issued.

In relation to who is the responsible authority to detect unregistered/unlicensed activity, the analysis showed that while in some countries the task is clearly allocated to a specific authority (usually the supervisor), in others, the issue is more diffused, and the authorities are expecting actions to be taken by "others". A typical situation is when in the absence of specific procedures and powers, the supervisors will assimilate the unregistered VASPs with a form of illegal activity and expect the Police (or other LEA) to take action against such, while the LEA would not feel responsible (or knowledgeable) and expect the supervisor to take action.

6. Law enforcement and VASPs – Worlds Apart?

This chapter examines the capabilities and approaches of authorities in MONEYVAL countries to investigate ML/FT cases involving use of VAs and to impose interim measures.

Investigations involving the use of VAs present several challenges which are highlighted throughout this report. Such challenges and obstacles include: (i) lack of knowledge and expertise on how to handle VA analysis and investigations; (ii) lack of legal certainty as to whether certain investigatory / interim measures are applicable in relation to VAs; (iii) lack of or inappropriate tools to analyse/investigate VA transactions in an effective manner; (iv) inefficient international cooperation which hampers the timely implementation of freezing, seizure and confiscation of VAs in international cases; and (v) difficulties to apply analytical and investigatory tools in respect of unregulated VASPs.

Nonetheless the technology behind VA (i.e. blockchain) also presents some positive features. The information (including transaction data) recorded on the blockchain is immutable and specifically useful for investigators that are following the money. This however requires the deployment of appropriate tools (such as blockchain analysis tools) which would permit investigators to follow the trail of virtual currencies.

The effective regulation of VASPs also plays a fundamental role in the international community's ability to counter financial crime through the abuse of VAs. This is because regulated and supervised VASPs constitute a useful source of information that can significantly assist in the carrying out of investigations, and tracing of VAs. To a certain extent this is being challenged by the emergence of decentralization in the VA sphere. This is because decentralised models involve no central intermediary which may be regulated and act as liaison with LEAs. The rapid evolution of the VA sector also necessitates ongoing training and upskilling for LEAs to constantly be knowledgeable in how to deal with and investigate VAs and VASPs.

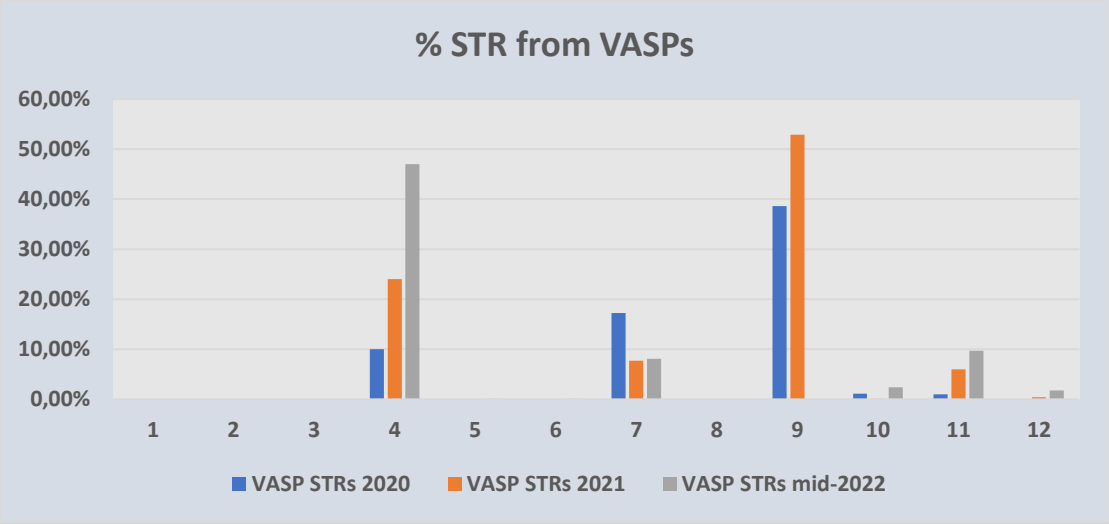
6.1. Suspicious Transaction Reports by VASPs and on VAs

SARs or STRs received by FIUs constitute an important source of intelligence to detect ML/FT cases. The project team has assessed the availability of intelligence on VA related suspicions being sourced through STRs. Data on the total number of STRs submitted by VASPs between 2020 and 2022, that was provided by 12 responding members, was used to draw conclusions. Qualitative data on the content of the STRs obtained also completes the survey.

6.1.1. Volume of STRs submitted by VASPs

A number of observations are noted. Out of the 12 members that provided STR data, four received quite a sizeable volume of STRs from VASPs, while the rest are receiving very negligible numbers or none. It is apparent that those member countries which have sought to regulate and are supervising VASPs have induced more reports from the VASP sector. Chart 12 presents the percentage of STRs received from VASPs out of the total volume of STRs between 2020 – 2022, across the 12 MONEYVAL members which participated in this analysis.

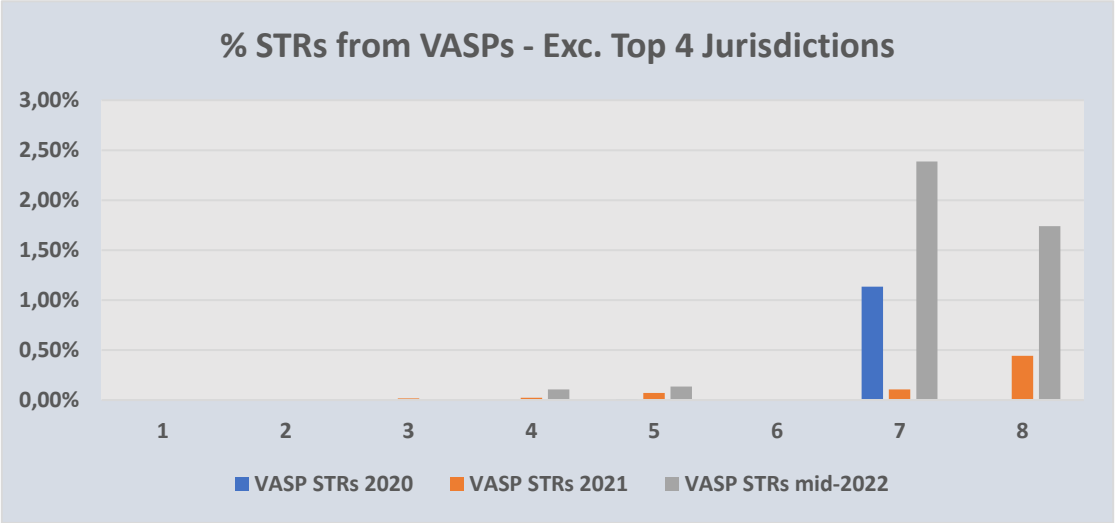
Chart 12: STRs submitted by VASPs



Some of the respondent members experienced an increase in the number of STRs submitted by VASPs when comparing 2020 to 2022 (end June).

Most respondent members (six) received less than 1% of STRs from VASPs during the 2020-2022 (end June period), with three of these jurisdictions indicating that they have never received any STRs from VASPs. Two respondents received 2.4% and 1.7% of all their STRs in 2022 (by mid-June) from VASPs. Chart 13 below provides statistics on the volume of STRs received by jurisdictions other than the top four in terms of STR reporting.

Chart 13: STRs submitted by VASPs (excluding the top 4 jurisdictions)



It is suggested that VAs feature in more STRs than those just from VASPs, and it is possible that the true abuse of VAs and VASPs could be identified from external FIs, however the data to observe this could not be obtained. This indicates that a sizeable number of FIUs from the respondents still face issues of obtaining and recording statistical information.

One striking factor when analysing the volume of STRs from the top receivers is that in most cases, STRs from the VASP sector originate from a limited number of operators. For example, in one

country a single service provider (i.e. an exchange) accounted for 96% of all VASP STRs in 2022, while in another country one VASP contributed to 95% of the total volume of STRs from the sector in 2021. In both cases these are large VASPs which take a significant share of the market in terms of client volumes.

6.1.2. Quality of STRs submitted by VASPs

An overview of the quality of STRs in jurisdictions where the number of STRs generated by VASPs is significantly higher (i.e. the top 4 jurisdictions), indicates concerns with the overall quality of STRs. Countries highlighted several issues that are impacting the quality of VASP STRs namely:

(i) STRs are automatically generated by technological tools used in managing the overall activity of the VASPs and are rarely of high quality. These tools identify "suspicious" wallets and addresses since these would be linked to other wallet addresses that are tainted in view of adverse information associating them with criminality. Sometimes this connection is apparent several hops down a transaction chain making it a very remote link. These tools constitute a useful source for identifying dubious wallet addresses however, cannot replace the detection of suspicions through analysis and detection of traits and typologies (including when there isn't a current link to criminality). The latter approach yields more useful financial intelligence. Practitioners are of the opinion that the intervention of a knowledgeable human operator in the selection of the relevant STRs would be beneficial, even if this would mean a reduction of the numbers of the STRs.

(ii) It is also apparent that "defensive reporting" represents a significant portion of those STRs. Numerous cases of STRs are being reported in view of the mere inability to conduct CDD. At times such STRs don't involve any assets or transactions.

(iii) VASPs are outsourcing their CDD obligations including transaction monitoring which is not helping to build up expertise in detecting suspicious transactions. Some countries are prohibiting the outsourcing of AML/CFT obligations or specific obligations such as transaction monitoring and suspicion analysis, with the aim to mitigate this issue.

(iv) A phenomenon of conversion of "IT to Compliance" in the private sector (VASPs) is noted. This means that the respective compliance team, while knowledgeable on blockchain technology and VA related tools, lacks basing understanding on AML/CFT matters.

(v) VASPs that operate in more than one country at times struggle to determine where to report a suspicion given that it is hard to establish the jurisdictional connection of a particular transaction, which either leads to multiple reports, or incorrect reporting.

Countries stressed the importance of outreach and investment in building up capacities of VASPs to help them detect and report more quality STRs. This may be achieved by the: (i) formulation and dissemination of information on ML/TF trends and typologies associated with VASPs and VAs; (ii) the constant gathering of data and statistics on the quality of STRs and sharing information to help bridge gaps; and (iii) holding informal discussion sessions with VASP operators which could provide for an opportunity for FIUs and supervisors to become more knowledgeable about VASP operations, while at the same time passing on expertise to VASP employees on detecting suspicious transactions.

6.1.3. Underlying Predicate Offences

Two member countries participating in this project provided data on trends and typologies that they are identifying through STRs received from VASPs. When analysing data on reported underlying predicate offences some common trends were noted.

Investment Fraud was reported as the topmost common predicate offence in one country and the second topmost in another. Typically, such cases involve clients of VASPs being tricked into transferring VAs to fraudulent third parties who generally promise them great investment opportunities, which, often results in a complete loss of assets. Social engineering is also used to gain access to email addresses through which fraudsters attempt to gain access to wallets and crypto assets.

Child sexual exploitation was reported as the top-most predicate offence in one of these countries. Most of the cases linked to child sexual exploitation involve the transfer of VAs (using the VASP's wallet) to other wallets which are directly or indirectly linked to wallets exposed to child abuse material. Using blockchain analysis tools, local VASPs can identify such links which lead to reports being submitted on the grounds of suspected links to child sexual exploitation.

It is noted that one member country reported abuse of VAs to bypass targeted financial sanctions. The global nature of VAs invariably means that the sector also attracts clients from higher-risk jurisdictions, and potential exposure to sanctioned entities and/or sanctioned jurisdictions. To move funds and circumvent sanctions, and mitigate reduced access to the SWIFT payment system, it is likely that sanctioned entities will explore alternative payment methods, including the use of VAs. The main barriers in upscaling VA use in this regard are liquidity and market size, while the transparent nature of the blockchain could reduce its appeal to circumvent sanctions.

6.2. Investigatory Capabilities

Drawing from information that was sourced through the questionnaire replies and information available through MERs, it appears that in the majority of cases, jurisdictions do not determine the ML/FT investigatory responsibilities on the basis of the *modus operandi* of cases (e.g. whether they involve use of legal entities, cash or VAs or other specific typologies). In MONEYVAL members, competence is most commonly determined on the basis of the predicate offence (e.g. specialised units to investigate corruption cases or organized crime and ML emanating therefrom, or specialized units to deal with economic crimes or complex cases). Typically, smaller jurisdictions, tend to have one central LEA and/or asset recovery unit that would have general responsibility to investigate all criminal offences including ML/FT. Generally, it appears that the investigation of ML/TF cases involving VASPs or VAs and the imposition of interim measures in connection therewith is entrusted to LEAs based on their already determined competence.

There are however jurisdictions that have opted to create specialised units or departments dedicated to the investigation of cases (irrespective of their nature) that involve the use of VAs or VASPs, or crimes perpetrated using technology in general.

Case Box 8: Specialised LEAs to investigate case involving VAs or VASPs – Bosnia and Herzegovina & Bulgaria

Bosnia and Herzegovina - The Ministry of Internal Affairs of the Republic of Srpska, has set up a specialized department responsible for detecting and investigating crimes involving virtual assets. The High-tech Crime Department is part of the General Crime Unit within the criminal police administration and assumes the role of collecting and processing information on all forms of high-tech crime, performing proactive and reactive collection, assessment, and analysis of intelligence data.

Bulgaria – Within the General Directorate "Combating Organized Crime" of the Ministry of Interior all police officers are empowered to investigate cases related to virtual assets. Nevertheless, there is a specialised department that mainly works on such cases which is the Bulgarian Cybercrime Department.

6.2.1. Collection of intelligence and evidence from VASPs

In so far as the collection of intelligence is concerned, most MONEYVAL respondent members indicated that their FIUs use the legal rights they have to collect information from persons and entities that are designated as reporting entities, which would also include VASPs. However, this legal mechanism is heavily dependent on the approach taken by the jurisdiction to designate VASPs for AML/CFT purposes. Numerous MONEYVAL members have not designated the entire scope of VASP activities identified under the FATF Recommendations. By way of example jurisdictions that are EU members and following the provisions of the 5th AMLD, would not have covered all FATF VASP activities[9]. Hence for so long as there remain gaps in the coverage of VASPs within MONEYVAL members and beyond, legal obstacles for collecting financial intelligence from VASPs will also remain.

A minority of FIUs have wider powers to request information from any person or entity irrespective of whether these are reporting entities or not, such as the case in the Isle of Man and Malta.

Case Box 9: Obtainment of intelligence from third parties – Isle of Man & Malta

Isle of Man – Article 18 of the Financial Intelligence Unit Act 2016 provides the FIU with the power to demand information from any person who is not the initial provider of intelligence but who is a person that:
(i) is mentioned in or is otherwise identifiable from the information received; or
(ii) to the reasonable knowledge or belief of the FIU, holds information that is relevant to the analysis of the information received.

Malta – Articles 30 and 30A of the Prevention of Money Laundering Act empower the FIAU to gather information from any person, authority, or entity, where the FIAU deems that such

[9] See section 1.2 for further information on coverage of VASPs throughout the MONEYVAL region.

information is relevant and useful for the purpose of pursuing any of its functions at law which also include the intelligence analytical functions.

Given that Recommendation 15 requires the licensing or registration of VASPs that are incorporated or have their personal place of businesses located in the country, it is questionable how decentralized business operators such as decentralized crypto exchanges will be regulated and subsequently how intelligence and information may be sourced from them given that there may be no specific person or persons that are responsible for the operations.

The FATF has sought to address this in the updated version of the guidance notes issued in October 2021[10]. The guidance recognises that the FATF Recommendations do not apply to the underlying software enabling VA transactions and hence decentralised finance (DeFi) applications cannot be considered as VASPs. Nonetheless, creators, owners and operators who may maintain control or sufficient influence over the functioning of these DeFi arrangements could fall under the definition of a VASP as they would be considered to provide or facilitate VASP services. However, it remains doubtful whether all DeFi arrangements would have some identifiable controllers or persons able to influence the operations to be regarded as VASPs and used as a source of intelligence and/or evidence.

Respondent members have indicated that for the purposes of collecting evidence and other information they rely on the powers they have under criminal law which are applicable to the investigations of all other crimes. In some cases, a court authorisation is required to obtain such information. All indicated that these powers of gathering evidence are also applicable to VASPs and VA transactions. Members noted that since VASPs can easily provide services remotely in various jurisdictions, difficulties arise for LEAs when gathering information from VASPs that are not residing or located within the jurisdiction. Others noted that many VASPs do not appear to have any registered physical presence which would complicate the gathering of information.

6.2.2. Special Investigatory Tools

As has been stated in the introduction to this chapter, the monitoring and analysis of VA transactions may somehow be facilitated by the fact that the whole concept of blockchain technology is based on the notion of transparency of transactions and immutability (i.e. cannot be altered or deleted). Some blockchain networks[11] are private, however the mainstream crypto currencies have publicly available transaction data.

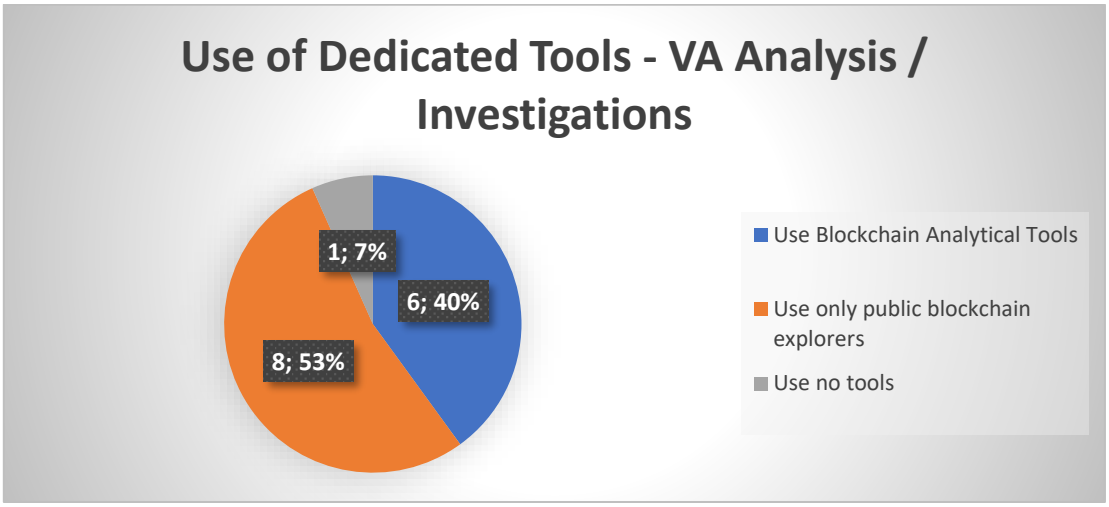
This is positive since FIUs and LEAs need not exclusively rely on data being provided by FIs and VASPs to be able to understand the flow of money but may to a certain extent[12] independently access such information. To do so in an efficient and reliable manner and to be able to decipher blockchain data in a meaningful way, specialised tools are required. Reference may be made to a report published by the EGMONT Group on Fintech Cooperation and Associated Cybercrime Typologies and Risks[13] which indicated that while some of the FIUs could not analyse VA related cases at all, over half of the respondent FIUs stated that they had to rely on open-source

[10] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
[11] E.g. Monero, Dash & Zcash
[12] Since only transactional information is available with no personal identification data.
[13] https://egmontgroup.org/wp-content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc

intelligence information since their internal analytical software did not possess the capability to analyse such transactions. This does not denote a positive outlook to FIUs' capabilities of detecting and analysing ML/TF cases involving the use of VAs.

Out of the 15 MONEYVAL members on which information was available[14] regarding whether they make use of any specific tools to analyse or investigate VA related transactions, almost all indicated that they make either use of public blockchain explorers or else have dedicated blockchain analytical tools that are provided by private entities. One respondent member indicated that its FIU/LEAs use neither but were in the process of acquiring a blockchain analytical tool. Nonetheless six member countries (out of the 15 that responded) indicated that they made use of blockchain analytical tools. Although it is not possible to compare (given that the EGMONT Group's project focused exclusively on FIUs), it appears that the MONEYVAL members follow the worldwide trend, in that the respective authorities are mostly lacking the proper tools to analyse and investigate VA related ML/TF cases.

Chart 14: Use of Dedicated Tools



MONEYVAL members were also asked to reflect on the main features that they looked for or would look for when sourcing technological tools to assist their authorities in VA related investigations or analysis. Members highlighted the following features and aspects:

- The tool should have the ability to group/cluster transactions and wallet addresses such as highlighting intermediaries and identifying potential malicious actors.
- A user-friendly and efficient tool that does not necessitate in-depth knowledge or expertise of the crypto universe.
- The ability of the tool to export data in a readable and/or analysable formats.
- Availability of reliable and up-to date data.
- Cost-effectiveness.

Some members reported they are outsourcing some of this work to specialized private sector investigators or experts, in a similar way to a pathologist, or collision expert being used in specialized criminal investigations.

[14] Information on this aspect was available either via the questionnaire responses or through available MERs.

6.3. Freezing and Seizure of VAs

MONEYVAL members were asked to provide information on the process adopted to impose interim measures for the freezing and seizure of VAs. Seven members provided information in this regard. The majority indicated that they would request the assistance of the VASPs which are in control of the VAs suspected to be proceeds of crime ordering them to freeze the assets. Some members stated that they make use of official / government wallets to transfer and hold seized VAs.

The ability to effectively seize and transfer the VAs that are not held by a VASP (which would hold the wallet keys) will depend on whether the LEAs gain possession of the wallet keys providing control of the VAs.

Case Box 10: Creation of official wallet for the seizure of assets – Bulgaria, Hungary & Slovenia

Bulgaria – The National Investigation Service which constitutes part of the Prosecutor's Office developed a procedure, whereby VAs are seized by being transferred to a wallet address that is especially created for the pre-trial proceedings in a hardware wallet of the Prosecutor's Office, or in a wallet, created with a requirement for more than one signature for executing a transaction.

Hungary – According to section 315 (Seizing and ordering the preservation of electronic data – XC of 2017 on the Code of Criminal Procedure) the seizure is rendered possible by transferring the VAs from the suspect's wallet to the official Hungarian Police (BRFK) wallet.

Slovenia – In practice the seizure of VAs is applied by the submission of a seizing order to the concerned VASP ordering it to transfer the VAs to the government wallet.

Situations will arise where VAs that are proceeds of crime perpetrated in one country may be located in a foreign jurisdiction. In such situations LEAs will encounter additional barriers in the process of freezing or seizing such VAs, since they are not held by a VASPs established within the jurisdiction. This is where effective international cooperation is fundamental to be able to pursue such cases and freeze or seize assets.

Most jurisdictions that provided practical insights as to how they would handle such cases indeed referred to the use of international cooperation channels (such as MLAs). Respondents did comment that it is questionable whether such mechanisms are efficient enough to ensure the timely seizure or freezing of VAs. MONEYVAL members also referred to the use of FIU postponement powers to efficiently freeze assets at a pre-trial stage pending the application of more formal means of freezing and seizure of assets.

Some members have also indicated that they attempt to request the direct assistance of the foreign VASP to seize and freeze the assets, however they highlight that this is highly dependent on the willingness of the VASP to voluntarily cooperate.

Case Box 11: Freezing and Seizure of VAs held with foreign VASPs - Latvia

The manner in which the freezing of VAs held with foreign VASPs is handled depends on the situation at hand. There are situations when VAs are identified together with access codes and passwords, which allows the immediate arrest and transfer of the VA to the VA wallets held by the competent authority. In such situations this asset can be transferred to VA wallets that are held by Latvian Provision State Agency for safe keeping. There are also situations when VAs are held by foreign VASPs that are willing to cooperate with LEAs. In such situations an electronic letter is sent requesting the VASP to suspend the operation involving the VA in question which VASPs execute for a short period of time. Subsequently (and depending on the extent of cooperation with the VASP and the legal framework that it is bound by), LEAs may either send a translated arrest order electronically to the VASP requesting it to arrest and transfer these assets to the official wallet held by the Latvian Provision State Agency or request the VASP to exchange the VAs into FIAT currency and transfer the equivalent FIAT value to the bank account of the LEA for safe-keeping.

Where the legal framework of the VASP would not allow it to execute such direct orders or in case of lack of willingness by the VASP to cooperate, then a MLA request may be sent to the authorities of the jurisdiction where the VASP is located. For example, there are situations where VASPs do not intend to communicate with foreign LEAs affirming that they would only cooperate with local authorities. In such cases, the success of the investigation depends on the speed and quality of police-to-police cooperation and other international cooperation mechanisms.

Latvian State Police have created VA wallets for the most popular VAs – Bitcoin, Ethereum, Tether, Ripple XRP, Dogecoin, Shiba and others. In 2022 police have successfully confiscated and sold VAs for the amount of approximately €100,000 in a public auction.

Case Box 12: Freezing and Seizure of VAs held with foreign VASPs - Germany

In one case related to the investigation of two suspects, bank account transaction analysis led investigators to detect the acquisition of Bitcoin through a VASP that was established in a foreign jurisdiction. Arrest warrants were sent via e-mail directly to the foreign VASP. Based on these arrest-warrants the VASP close the suspects' accounts so that they would not be able to use it and dissipate the VAs held on it. Afterwards the Bitcoins were seized officially through judicial legal process.

Reference may also be made to the Guide on seizing cryptocurrencies[15] which has been developed within the framework of the Joint European Union and Council of Europe iPROCEEDS-2 project. This guide can provide further practical information and best practices on the seizure of VAs.

[15] https://www.coe.int/en/web/cybercrime/-/iproceeds-2-guide-on-seizing-cryptocurrencies-available-on-the-octopus-cybercrime-community

6.4. Training and up-skilling

For FIUs and LEAs, it is crucial that they maintain a good understanding of the VA sector, and the peculiarities of the sector and VASPs operating within their jurisdiction. This necessitates on-going training to build the authorities' expertise and understanding, to keep pace with this ever-evolving sphere. A good level of cooperation between regulators, supervisors, FIUs and LEAs is also desirable for all relevant authorities to be knowledgeable about market operations in this area, understand risks and develop appropriate controls to mitigate the misuse of the sector for ML/FT purposes.

This project sought to analyse the frequency and type of VA/VASP relating training that FIUs and LEAs within MONEYVAL members are provided with. 14 members indicated that their FIU received training on VAs/VASPs over the period 2020-2022, while 13 jurisdictions indicated that their LEAs received such training over the same period. The regularity of training ranged from 1 event over the two-year period to 7 events in the case of FIUs and three to 15 events for LEAs/prosecutors. The below list provides information on the type of training that was received by FIUs in relation to VAs/VASPs.

- Tracing, Seizure and Confiscation of VAs
- Technical Training and Introductory Courses on Virtual Currencies and Blockchain Technology
- Training on the licensing and supervision of VASPs
- Training on legal aspects
- Introductory courses
- Use of Darknet
- Investigator Courses focused on the analysis / investigation of cases involving the use of VAs and effective investigatory techniques
- Dedicated training connected with the use of specific blockchain analysis software.
- Analysis of cases studies involving VAs/VASPs
- Typologies and modus operandi of ML/FT through the use of digital technology including VAs
- Focus on recent technological developments in this sector

Various FIUs, LEAs and prosecutors referred to training initiatives organised by international bodies such as CEPOL, CoE, EGMONT Group, EUROJUST, EUROPOL and FATF amongst others. Some jurisdictions also made use of available online material on VAs and VASPs provided by international institutions (e.g. ECOFEL and CEPOL), while some jurisdictions stated that they have developed internal guidance and training material such as online guidance and handbooks that are available to internal staff. This material serves to provide a basic and introductory overview to cryptocurrencies, the associated technology and some guidance on investigation techniques and red flags.

Specific positive initiatives of collaboration between FIUs, LEAs and VASPs to obtain training on the technology and operations of VASPs have been noted in some jurisdictions.

Case Box 13: Collaboration with the private sector and between public bodies for training purposes – Andorra & Slovak Republic

Andorra - In May 2021, the Unitat d'Intelligencia Financera (UIF) of Andorra collaborated with a private law firm and a law school to organise training for UIF officials focusing on regulatory issues related to blockchain and crypto-assets. Another session was held in January 2022 with the collaboration of the Andorran University focusing on legal aspects of crypto assets.

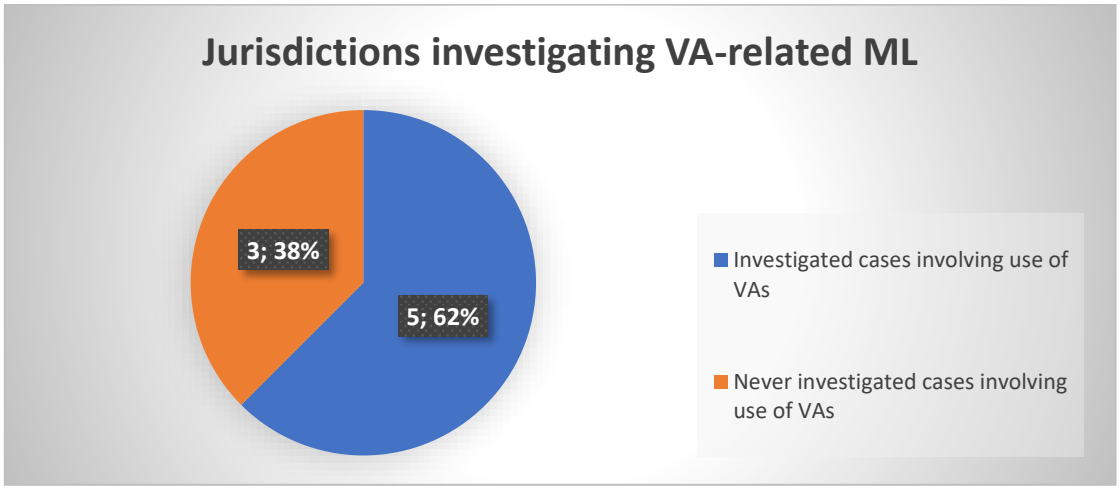
Slovak Republic – The FIU cooperated with a Slovak crypto company to organize a one-day training event for the entire staff at the FIU. Throughout the event, training was provided on the basics of VAs, and trading in cryptocurrencies and the ML risks associated with VAs. FIU officials also participated to two workshops that were organised by the Ministry of Finance and the National Bank for training on fintech technologies and innovations.

6.5. Statistical Data – Investigation, Seizure, Freezing and Confiscation of VAs

Few MONEYVAL members provided information on the total number of ML investigations carried out throughout the years 2020 and 2021. These members also provided information on how many investigations included the identification of alleged proceeds of crime which were virtual assets.

Five out of eight respondents reported that they identified VAs that were alleged proceeds of crime in their investigations. However, this happened in a very small number of ML cases out of the total that were investigated (1%). The other three members reported that they had never identified suspected proceeds of crime that were VAs. Other members reported that they did not hold statistical data that would enable them to determine which investigations detected proceeds of crime that were VAs

Chart 15: VA-related ML Investigations



Four of the five members that investigated ML involving VAs managed to seize and/or freeze VAs to the approximate value of €56.9million and $57,096. There was one member that accounted for 99% of all the approximate value of frozen / seized VAs. It is noted that in only two members and in two cases that subsequent to these investigations and freezing of assets, VAs were able to be confiscated.

6.6. Case Studies

This section presents a number of case studies from the MONEYVAL region which shed light on the use of VAs for ML purposes, such as the types of underlying crimes that are normally associated with such ML cases as well as the *modus operandi* and typologies as to how such ML cases are perpetrated. It is clear that VAs are being used and can probably be used interchangeably with FIAT currencies when looking at typologies.

Case Box 14: Theft of VAs through "typosquatting" – Isle of Man (in cooperation with UK and Netherlands)[16]

In 2019, six individuals were arrested in the United Kingdom and the Netherlands in connection with the theft of Bitcoin tokens. It is believed that the theft affected at least 4,000 victims in 12 different countries and involved a 14-month long investigation into a €24 million cryptocurrency theft. An Isle of Man company was also one of the victims of the scam.

The theft was perpetrated through a technique that is referred to as "typosquatting", whereby the website of a well-known cryptocurrency exchange was copied to replicate the genuine site and in such a manner attract users to access the replica site and obtain information on Bitcoin wallets, stealing funds and login details.

The Isle of Man Constabulary (IOMC) cooperated in this case by sharing intelligence and evidence using both Police to Police and MLA mechanisms. IOMC have also worked alongside the UK's South-West Regional Organised Crime Unit (SWROCU) and the Dutch LEA attending Eurojust coordination meetings. SWROCU assisted the IOMC with the track & tracing of the stolen Bitcoin. The larger case was part of a joint operation involving the European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) hosted at Europol after the British authorities identified possible suspects living in the Netherlands.

Case Box 15: Sale of Fake VAs – Azerbaijan

Persons (citizens of a foreign country), who previously registered a company in a foreign country, which operates in the "emission of virtual currency" field, have registered an advertising company in Azerbaijan ("ADV"). The Azeri company was promoting a fake cryptocurrency stating that soon this cryptocurrency ("XYZ Coin") would be traded on various international cryptocurrency exchange platforms. The perpetrators were able to collect large sums of money from citizens who were promised exaggerated high revenues for investing in XYZ Coin.

Three forms of earning opportunities were proposed to those who acquired XYZ Coin: (i) dividend payment corresponding to the funds invested for the purchase of XYZ Coin (after a certain period of time), (ii) commission payment for encouraging other people to invest in XYZ Coin and (iii) payment of high profits after the future listing of XYZ Coin on a foreign exchange.

[16] https://www.europol.europa.eu/media-press/newsroom/news/6-arrested-in-uk-and-netherlands-in-%e2%82%ac24-million-cryptocurrency-theft

Criminals artificially increased the price of XYZ Coin every few months to increase their illegal income, stating that the price increase was owed to the listing of XYZ Coin on a foreign exchange. The alleged criminals in order to artificially reduce the value of people's investment in XYZ Coin for their own benefit, gave a discount to the people who bought the coin on the website XYZCoin.com offering to exchange 2 XYZ Coins on XYZCoin.com for one XYZ Coin placed on the stock exchange.

Funds transferred to the cards of ADV company for the purpose of purchasing XYZ Coin amounted to several million currency units, 2/3 of which consisted of payments made through payment terminals. The investigation revealed that the company was not listed on any cryptocurrency exchange platform. Additionally, the declared cryptocurrency was just a pseudo-token where the transfer of the relevant token to another individual on the exchange was described as the sale process of virtual currency to network members. Preliminary information about the case was obtained through social networks, websites and YouTube.

Case Box 16: Use of Money Mules - Latvia

In accordance with the Virtual Assets: Money Laundering and Terrorism and Proliferation Financing Risk Assessment published by Latvia in 2022[17], cases of money mules are still considered topical. The Criminal Police Department had a criminal case involving organised group individuals who were involved in ML activities over a long period of time. Over this period nearly 100 accounts were opened with Latvian credit institutions. In this particular case and with the assistance of money mules, fraud proceeds were transferred as FIAT currency, which were then withdrawn in cash and converted into virtual currency. Investigations led to the identification of unregistered VASPs (providing exchange services), which were not monitored and did not carry out customer due diligence.

Furthermore, drawing from STR typologies the Latvia risk assessment on Virtual Currencies established that in the majority of STRs involving the use of VAs (55%) the underlying crime would involve property crimes (including fraud); in 34%, the predicate offence has not been identified and there are autonomous features of ML while 7% raised suspicions of tax offences.

Case Box 17: Drug and Arms Dealing – Slovak Republic[18]

The investigation related to a Slovak national who was trading firearms, ammunition and drugs on the darknet. Following the man's arrest a property search was performed. One of the searches revealed five firearms, ammunition of different calibers, a sophisticated indoor cannabis plantation and a Bitcoin wallet that contained bitcoins worth €203,000 which were allegedly obtained through the illegal services offered over the darknet.

Through this investigation the Slovak authorities, assisted by Europol, dismantled an online drug operation on the darknet in operation since 2015, through which at least 10kg of

[17] https://fid.gov.lv/en/roles-and-responsibilities/guidelines
[18] https://www.europol.europa.eu/media-press/newsroom/news/darknet-dealer-of-drugs-and-arms-arrested-slovak-authorities

cannabis were suspected to have been bought. The police also seized the server used to host the darknet marketplace, which enabled the authorities to widen the investigation onto users and vendors who were utilizing the marketplace. Moreover, through international cooperation and Europol's assistance, another darknet vendor living in another EU country was identified.

This case was a breakthrough in the Slovak Republic in the field of VAs, as it helped the authorities dealing with this case to obtain know-how and possible procedural solutions and helped in the development of the General Prosecutor´s Office Handbook on Virtual Currencies. This case also led to a number of enhancements following lessons learnt such as the creation of a LEA wallet to allow the seizure of assets and also legal modifications to the Criminal Code to facilitate the seizure of VAs.

Case Box 18: Laundering of Drug Trafficking Proceeds - Malta

An EU national residing in another European country opened a bitcoin wallet account with a Maltese VASP in January 2021. Over a 20-month period the subject deposited a total of £29,255.02 using cards issued by a European bank. Such funds were then used to invest in VA using the Maltese licensed VASP with the majority of investment activity occurring within a nine day period. During this same 20-month period the subject was being investigated in another European country in connection with drug-related offences. At the point that the subject's prosecution and conviction for drug-trafficking became public knowledge and was detected by the VASP through its on-going monitoring procedures, a STR was submitted to the FIAU.

The FIAU established that the subject had been jailed for seven years after officers in the European country seized a quantity of drugs and chemicals from a storage address being used to prepare drugs. Although no further financial links were identified in Malta and the subject was found not to hold any companies or bank accounts in Malta, the FIAU established a reasonable suspicion that the funds held with the Maltese VASP were proceeds of drug-related offences. This suspicion was further accentuated by the fact that the subject's VA deposits and investment activity took place at the same time of his investigation and arrest which was further indicative of attempts by the subject to dissipate the potential proceeds of crime.

Following the FIAU's analysis a report was disseminated to the Malta Police which proceeded to request the issuance of an attachment order to attach in the hands of the Maltese VASP the funds that were held in the subject's wallet address. As of January 2023, the subject held a balance of EUR 32,323.63 worth of bitcoins in his account which are currently attached.

www.coe.int/MONEYVAL

July 2023

Typologies report

MONEYVAL

Typologies Report

MONEY LAUNDERING AND TERRORIST FINANCING RISKS IN THE WORLD OF VIRTUAL ASSETS