



CYPRUS NATIONAL RISK ASSESSMENT

Prepared by



with respect to Virtual
Assets and Virtual
Asset Service Providers

Final Report
November 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	3
Key Findings.....	3
Recommended Actions.....	4
NATIONAL RISK ASSESSMENT REPORT.....	14
Preface.....	14
1. ML/TF RISKS AND CONTEXT.....	18
1.1 ML/TF Risks and Scoping of Higher Risk Issues.....	18
1.2 Materiality.....	23
1.3 Structural Elements.....	24
1.4 Background and Other Contextual Factors.....	24
2. NATIONAL AML/CFT POLICIES AND COORDINATION.....	34
2.1 Key Findings and Recommended Actions.....	34
2.2. Immediate Outcome 1 (Risk, Policy and Coordination)	36
3. LEGAL SYSTEM AND OPERATIONAL ISSUES.....	43
3.1 Key Findings and Recommended Actions.....	43
3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)	46
3.3. Immediate Outcome 7 (ML Investigation and Prosecution)	53
3.4. Immediate Outcome 8 (Confiscation)	67
4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION.....	73
4.1 Key Findings and Recommended Actions.....	73
4.2. Immediate Outcome 9 (TF Investigation and Prosecution)	78
4.3. Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions).....	82
4.4. Immediate Outcome 11 (PF Financial Sanctions)	87
5. PREVENTIVE MEASURES.....	92
5.1 Key Findings and Recommended Actions.....	92
5.2. Immediate Outcome 4 (Preventive Measures)	94
6. SUPERVISION.....	113
6.1 Key Findings and Recommended Actions.....	113
6.2. Immediate Outcome 3 (Supervision)	116
7. LEGAL PERSONS AND ARRANGEMENTS.....	155
7.1 Key Findings and Recommended Actions.....	155
7.2. Immediate Outcome 5 (Legal Persons and Arrangements).....	158
8. INTERNATIONAL COOPERATION.....	168
8.1 Key Findings and Recommended Actions.....	168
8.2. Immediate Outcome 2 (International Cooperation)	168
TECHNICAL COMPLIANCE ANNEX.....	173
Recommendation 15 – New technologies.....	173
GLOSSARY OF ACRONYMS	187
SUPPLEMENTAL ANNEX	190

EXECUTIVE SUMMARY

1. This report sets forth a national risk assessment for the Republic of Cyprus focused on ML/TF risks of virtual asset (VA) activities and virtual asset service providers (VASPs) in Cyprus as of late 2020. As requested by the Republic of Cyprus, this assessment assumes enactment of the AML/CFT Bill (the Prevention and Suppression of Money Laundering and Terrorist Financing (Amending) Law of 2021) as enacted by Parliament in February 2021.

Key Findings:

1. VA activities and VASP sector were out of scope of the 2018 National Risk Assessment and 2019 Moneyval Fifth Mutual Evaluation Report as they predated the 2019 FATF Guidance updates regarding VA and VASPs.
2. There is very limited VA or VASP (or VASP-type) activity in Cyprus. There have been limited access points for VA into the broader Cyprus economy as financial institutions regulated by the CBC have not supported VA activities or VASPs. The structure of other areas identified in the NRA or Moneyval report as higher risk generally do not appear to have provided access points as conduits for VA or VASP ML/TF risk.
3. There is a widespread perception that the VA/VASP sector is high risk, but overall there is limited direct understanding or experience regarding the specific ML and TF risks of VA and VASP sector on the part of key authorities. CySEC has had initial direct supervisory experience supervising ML/TF risks of a small subset of entities it has authorized to conduct VA/VASP activities under a controlled framework, and showed a sophisticated level of understanding of the sector (although limited to a small number of current staff), with notable attention and support from executive leadership.
4. CySEC will have a critical role supervising VA activities, leading Cyprus's efforts to mitigate VA/VASP ML/TF risks
5. The Police have acquired some direct experience and sophisticated understanding with VA. MOKAS demonstrated very little direct experience and very limited training on specific attributes of the VA/VASP sector. MOKAS has had a very limited role in the process of this risk assessment. The PPO has very limited experience with VA.
6. There is little systematic data collection or metrics specific to VA activities or VASPs.
7. There is very limited to no use of specialized commercial cryptocurrency AML compliance and intelligence/blockchain forensics and transaction monitoring tools and databases, and supervisors, law enforcement and the FIU have received little to no access to and training on their use.
8. As of late 2020 Cyprus had not implemented the wire transfer rule for transfer of VA for FIs and VASPs, often referred to as the "Travel Rule" for VA. This is a significant deficiency under the 2019 FATF Guidance, and is not covered under the AML/CFT Bill. The deficiency can be corrected in secondary legislation. The sector generally has not yet formally adopted the Travel Rule on its own. In practice the detrimental impact of this deficiency thus far has been limited, and FATF reports that many jurisdictions are not yet in compliance.
9. Current measures to mitigate NPO vulnerabilities, including the consulting project and risk assessment currently being undertaken on behalf of MOI, are not taking into account the VA/VASP sector. This is a vulnerability because Cyprus's status as an IFC and geographical proximity to conflict zones heighten its vulnerabilities to terrorist activities and risks of TF

and PF, including use of VA or VASPs to support TF, which have emerged as a channel. There have been no cases.

10. Processes for updates from supervisors to obliged entities on designations to sanctions lists and other communications are designed for normal business hours. Because VA markets, unlike traditional financial markets, are active on a 24/7/365 basis, this could be a material gap with regard to VASPs and movement of VA (partly mitigated by other sources of updates available to obliged entities through widely available databases).
11. No authority has been expressly assigned responsibility under the AML/CFT Bill for detecting and identifying unregistered VASP activities.
12. One type of VA/VASP activity, a virtual asset kiosk, generally known as a “bitcoin ATM,” falls within a regulatory gap outside CBC’s remit with no designated supervisory authority.
13. The 2019 FATF Guidance reflected international consensus and substantially more fulsome ML/TF measures for VA/VASPs than under prior FATF Recommendations. New developments continue to evolve rapidly, and accordingly FATF Guidance and best practices are likely to continue to evolve in light of rapidly evolving technology and business models for VA/VASPs, and will require ongoing monitoring.

Recommended Actions:

1. The CBC and CySEC should update their respective AML/CFT Directives to include measures dealing specifically with VA/VASPs promptly after the AML/CFT Law amendment is enacted. The revised directives should expressly incorporate the Travel Rule for VA wire transfers to address the FATF deficiency, and should make enhanced due diligence (EDD) indicators and requirements for VA that are currently implicit more explicit.
2. In light of CySEC’s role supervising VASPs and VA activities and leading Cyprus’s efforts to mitigate VA/VASP ML/TF risks, it should also provide education to its supervised obliged entities regarding identification of suspicious activity in relation to VAs
3. Firms in the FI sector should expressly adopt written policies and procedures to comply with the wire transfer rule for VA. As the highest priority, CySEC should ensure that FIs already engaging in VASP-type activities do so.
4. Authorities should start to maintain and share data and metrics specific to VA/VASPs. Although activity levels now are believed to be negligible, this will enable an evidence-based baseline as activities increase, promoting earlier detection of risks or changes to risk levels.
5. Training and significant capacity building should be made available with respect to VA/VASP ML/TF risks, as well as technological and market evolution in VA/VASP sector. Training needs should be led and monitored at the Advisory Authority level.
6. MOKAS has little direct experience of VA/VASPs. Securing more in-depth knowledge as well as benefit from knowhow and experience of other jurisdictions should greatly assist FIU’s capacity building in assessing VA/VASP related STRs and emerging risks with respect to the VA/VASP sector.
7. MOKAS should update the goAML STR reporting system with VA-related reporting fields, and provide guidance to obliged entities on VA-specific reporting and tipping issues.
8. The Police, CySEC and CBC should receive access to and training on specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases.
9. CySEC should add VASPs to its automated TFS and PF sanctions notification lists and ensure it receives MFA notifications and transmits them to obliged entities promptly, even outside

- normal business hours, given that VA markets are active on a 24/7/365 basis. Registration conditions for VASPs should ensure VASPs subscribe to databases providing notifications.
10. Cyprus should assign express responsibility to a designated authority, presumably CySEC, to detect and identify unregistered VASP activities.
 11. Cyprus should assign responsibility for “bitcoin ATM” supervision, presumably to CySEC, in any case this should be agreed and allocated between CySEC and CBC.
 12. Cyprus should leverage its collaboration with other jurisdictions that have had additional and complementary experiences with the VA/VASP sector, drawing from these relationships to identify lessons and best practices. Such international cooperation could be an important channel for Cyprus to strengthen and accelerate its capacity building for the VA/VASP sector.
 13. The Mol should widen the scope of its current NPO risk assessment to include VA/VASP ML/TF risks, prioritizing them in the RBSF methodology, and considering any NPO accepting or paying out VA, or accepting funds from VASPs, to be in a “high risk” category.
 14. Cyprus should regularly review whether its VASP registration framework is proportionate to VA/VASP ML/TF risks, or whether a licensing scheme should be considered. Cyprus should also consider whether to establish criminal liability by statute for failure to register as a VASP.
 15. CySEC should monitor issues with respect to the evolving and novel structures and legal arrangements that VA/VASP entities are likely to operate under due to their decentralized nature, outside of legal persons, (e.g. “DeFi” and stablecoin arrangements).

Risks and General Situation

2. This risk assessment focuses on the ML/TF risks posed by virtual asset (VA) activities and virtual asset service providers (VASPs) in Cyprus. There are a very limited number of firms conducting VA/VASP activities, under strict supervision of CySEC, with a high degree of attention and support from CySEC’s executive leadership. While these activities are limited and do not constitute a material sector for the Cyprus economy, the assessors prioritized them for the purposes of this assessment.
3. This assessment is designed to meet FATF requirements with respect to the ML/TF/PF risks for this emerging asset class and technology, which is of importance as Cyprus is soon to enact a legal and regulatory framework for the VA/VASP sector. This assessment also considers how existing ML/TF vulnerabilities identified by the December 2019 Moneyval Fifth Mutual Evaluation Report (Moneyval Report), which did not consider the VA/VASP sector, may be exploited with the use of VA as assets or VASPs as entities.
4. Cyprus’s status as an international financial center (IFC) heightens its vulnerability to ML, particularly originating from abroad, in the form of fund movements making use of its banking system, administrative service providers (ASPs), and other financial services. With regard to TF, Cyprus’s status as an IFC, as well its geographical proximity to conflict zones, also heightens its risks. VASPs, or any entities dealing with VA, may potentially utilize these conduits to transfer illicitly obtained funds, including through NPOs.

Overall Level of Compliance and Effectiveness

5. Given the stage of Cyprus's implementation, the assessment team performed a detailed analysis of the core issues under each Immediate Outcome to assist in designing and implementing an effective system going forward, and assist the relevant supervisory authorities in developing and executing a roadmap tailored to their sectors. The assessment team did not, however, assign effectiveness scores, out of concern that these could be a distraction from the analysis in the report as to the steps needed for implementation. An unduly low rating, as certain anticipated measures that will follow after enactment of the AML/CFT Bill are not yet in place, could be unfair. Meanwhile, an unduly high rating could promote overconfidence.
6. This report includes a detailed technical compliance assessment of R.15 as this FATF Recommendation, which directly focuses on VA/VASP ML/TF risks, was substantially expanded in 2019. The report also includes the supplemental annex regarding specific risk characteristics and mitigants of VA and VASPs.

Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7. Cyprus has completed an ML/TF NRA (published 2018) and has been subject to Moneyval MERs, most recently in 2019. Those reports and subsequent actions to remediate deficiencies identified demonstrate that Cyprus's starting point is a good understanding of its ML/TF risks (independent of VA activities and VASP sector) with a well-developed national strategy and Action Plan, as well as a long-standing body for national coordination. There are also well-established mechanisms for domestic and international cooperation for ML/TF.
8. There is a widespread perception that the VA/VASP sector is risky. Moving forward it would be timely and relevant for the Advisory Authority to ensure monitoring and information sharing with regard to these risks. This is crucial particularly given the limited understanding regarding the inherent ML and TF risks of VA and the VASP sector on the part of key authorities. Particularly where CySEC or the CBC is involved, understanding is very good (especially for CySEC which also has experience) though limited to a very small number of staff. The Police has acquired some experience and sophistication with VA/VASPs. MOKAS demonstrated limited direct experience and limited training on specific attributes of ML/TF risks of the VA/VASP sector. MOKAS has also had a particularly limited role in preparing this risk assessment, rather than the type of leadership role often associated with FIU participation in a risk assessment.
9. There is limited direct experience with VA/VASPs or of ML or TF involving VA or VASPs to date on the part of key authorities. There has been very limited VA or VASP (or VASP-type) activity in Cyprus. There have been limited access points for VA into the broader Cyprus economy as financial institutions regulated by the CBC have not supported VA activities or VASPs. Similarly, other sectors report the VA/VASP sector as higher risk and do not appear to have access points for VA or VASPs. There has been a negligible amount criminal cases or complaints, consumer complaints or MLA requests involving VA/VASPs. While there has been little data collection or metrics specific to VA activities or VASPs, for which there is little evidence-based baseline, as VA/VASP activities increase in the future, the AML/CFT Bill should provide a legal basis for the initial tools to cover most of the requirements for CySEC's oversight of registered VASPs. The

requirements can be further enhanced, through both the first stage of the registration directive (in progress) and the upcoming revisions to CySEC's AML/CFT Directive.

10. As a result, there is a significant need for training and capacity building with respect to VA/VASP market evolution and ML/TF risks, as well as tailored technological software tools to address these risks. The framework for VASPs will consist in a registration framework, not a licensing scheme. The registration framework will involve conditions prescribed or authorized by statute and others to be determined by CySEC, which will also be responsible for monitoring compliance with the registration conditions. This framework will not, however, involve prudential or conduct supervision of VASPs, nor of marketing activities or market integrity. CySEC should monitor regularly to ensure this registration framework remains proportionate to the ML/TF risks, whether additional registration conditions may be warranted, and whether a licensing scheme could also be considered in the future.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; 10.6, 7, 8; R.1, 3, 4, 29-32)

11. There is strong cooperation and understanding of procedures and persons across relevant authorities with respect to sharing, access and use of financial information. Overall, Cyprus authorities have access to a number of lawful mechanisms to freeze or confiscate VA.
12. There have been extremely limited instances to date of actual ML cases, alleged offenses, or STRs/SARs reported arising from or involving VA. There has been no practical experience with freezing and confiscation of VA to date. The assessment team found that the Police and MOKAS were familiar with a specific instance involving an MLA relating to VA in Cyprus, and had derived lessons learned for future preparedness. This case revealed there were no legal or practical restrictions on the access to or use of information of Cyprus authorities, except in relation to Customs, which understands VA to be outside its competencies due to the non-physical movements of goods.
13. MOKAS, while aware of general potential for VA to be risky for ML/TF, had very little direct experience, and very little understanding of the knowhow and experience of other jurisdictions. Securing more in-depth knowledge as well as benefiting from experience of other jurisdictions will greatly assist FIU in carrying out its role for the purposes of receiving and acting upon any STRs relating to VA activities, and assessing VA/VASP related STRs and emerging risks with respect to the VA/VASP sector.
14. MOKAS utilises the GoAML system, which obliged entities use to report SARS and STRs. There are not currently any preset identifier fields that relate specifically to whether a matter involves VA or VASPs. Introducing such fields and settings would facilitate reporting, metrics, and supervisory actions involving the VA/VASP sector.
15. The Police have already had training on cases of ML financing using VA and cases of internet fraud and investment fraud using VA. They have undergone additional training and developed

written procedures with instructions on how to confiscate VA. The Police recognized the need to preserve evidence in its original state, creating a duplicate digital version in the form of a forensic image for investigative purposes. This may present challenges in locating VA, software or hardware wallets or accounts, given that VA markets operate on a 24/7/365 basis and such assets can be transferred swiftly. The Police also rely on Europol for VA tracing using paid commercial tools or databases, and do not themselves have these tools or the training to use them.

16. It is unclear to what extent Cyprus authorities have developed the capability to manage storage and asset management of VA that it may freeze or confiscate, or that it has measures in place to safeguard VA from cyberattack or other theft or loss whilst proceedings are pending.

Terrorist and proliferation financing (Chapter 4; 10.9,10,11; R 1, 4, 5-8,30, 31 & 39.)

17. As an IFC and due to its geographical proximity to conflict zones, Cyprus has an inherently heightened risk of TF and PF. There is an emerging trend outside Cyprus making use of VA as the form of funds or NPOs as conduits to support these activities. Cyprus has a framework with a series of mechanisms at its disposal, both at an EU supranational and a national level, to implement targeted financial sanctions (TFS) without delay. The NPO sector, considered by Moneyval to be particularly vulnerable to abuse for terrorist activities and other forms of illegal activity, has revised its framework and is undergoing a risk assessment on behalf of the MOI. However, the risk assessment being prepared on behalf of the MOI regarding NPOs has not taken into account risks arising from the VA/VASP sector. This also leaves important vulnerabilities unaddressed in the form of potentially material risks in the NPO sector arising from VA that appear to be overlooked. The MOI should focus on risks arising from VA/VASP activities in the NPO sector, prioritizing them in its RBSF methodology for international and higher risk NPOs.

18. Updates to designations for TF and PF screening lists may not be communicated by supervisors to obliged entities if received outside of business hours until the next business day. Because VA markets operate on a 24/7/365 basis, there could be a meaningful gap with regard to the movement of VA for TF or PF purposes. Obligated entities understand the need to have protocols in place and VASPs should be required to subscribe directly to sanctions databases and have procedures for implementation of updates outside of standard business hours.

Preventive measures (Chapter 5; 10.4; R.9-23)

19. Cyprus has not adopted the FATF 2019 updates with respect to the wire transfer rule for transfer of VA, often referred to as the "Travel Rule," and this is not contained in the AML/CFT Bill.¹ Thus there is no legally binding requirement applicable to obliged entities or VASPs in

¹ According to the FATF Plenary statement following the June 2021 FATF Plenary, the majority of reporting jurisdictions have not yet implemented the Travel Rule for VA. <https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2021.html>

Cyprus. In practice the detrimental impact of the lack of adoption of the Travel Rule for VA is limited, due to the extremely limited to negligible VASP-to-VASP transmission of VA and non-existent transmission of VA involving CBC-supervised FIs.

20. The assessment team found strong understanding and preventive measures for VA ML/TF risks with regard to existing VA activities conducted by CIFs licensed by CySEC with special permission under CySEC Circular 244 to engage in such activities. This can be expected to be reinforced further when the registration process begins.
21. From conversations with the relevant supervisors and selected obliged entities, the assessment team noted there is a general perception by many FIs and DNFBPs of the VA and VASP sector as highly risky and outside their risk appetite. Where VA-related activity is detected by CBC-regulated FIs, customers are instructed to cease activity, or accounts terminated, or both. There is a widespread perception that VA-related activity is banned by the CBC for CBC-supervised entities, although the assessment team found there is no actual prohibition. This may change following implementation of CySEC's VASP registration and other new elements of the regulatory environment, as well with further guidance from CySEC, potentially making banks and other CBC regulated entities more comfortable engaging with FIs and specifically CySEC regulated VASPs.
22. The banking sector acts and is widely perceived as a critical line of defense against ML/TF because of its strict controls and practices. With regard to VA, it is widely understood that banks do not accept VA or serve VA activities. Thus funds transmitted from banks or bank customers are not perceived as carrying indirect VA or VASP ML/TF risks. For cases of VA deposits introduced from customers, they are regarded as highly risky, and are either broadly prohibited, or where permitted, subject to EDD and rigorous preventive measures.
23. There is a broad desire on the part of FIs to receive amended directives, or at minimum guidance, from CBC, CySEC and MOKAS, before formulating their own policies and procedures, and the general approach has been one of asking for permission from supervisors prior to engaging with new sectors such as VA/VASPs. Areas of particular interest include best practices for accepting VA from customers, STR reporting related to VA, VA layering typologies and avoiding tipping when suspicious VA transactions are initiated from customers. Use of specialized cryptocurrency AML compliance and intelligence/blockchain forensics and transaction monitoring tools and databases is also quite limited. A small number of CySEC-regulated firms engaged in VA/VASP activities do utilize these tools, and no CBC-regulated FI utilizes these tools.

Supervision (Chapter 6; 10.3; R.14, R.26-28, 34, 35)

24. VASPs will be registered by CySEC and will accordingly be supervised by CySEC, which will carry the relevant responsibility for VASPs as such.² In general, supervisors recognize VA as posing

² Since the period referenced in this report, CySEC has enacted its Directive for Registration of VASPs and has issued a Policy Statement with regard to its expectations for VASPs.

substantial AML/CFT risks and novel issues, and uniformly consider VA a high-risk sector. This perception may evolve with further training, particularly covering how risks arising from different types of VAs are different.

25. There are a range of degrees of awareness of VA-specific characteristics, as well as preparedness to mitigate the related risks. There are very few staff with direct specific understanding of VA/VASP ML/TF risks, and considerably more will be needed as activity in Cyprus grows, thus requiring substantial capacity building. Supervisors' resources are already constrained by existing activities and there is a need for utilization and training on VA-tailored AML compliance software forensics and transaction monitoring and database tools that can promote efficient offsite supervision and monitoring of compliance with policies. CySEC is in the process of initial review of these products, and depending on the registration interest by different entities (VASPs), the needs may vary.

VASP and FI Supervisors

26. CySEC is the only FI supervisor with direct experience with supervising VA activities or VASP-like entities under a limited number of authorizations granted to licensed CIFs and an AIFLNP. CySEC has developed a substantial understanding of VA and engaged closely with these entities to mitigate risks, acquiring experience and insight from applying AML/CFT procedures. Moreover, not only have VA/VASP supervision efforts been the focus at the very top of the organization's executive leadership, but CySEC also demonstrated a very high level of responsiveness and collaboration with the assessment team.
27. CySEC has also indicated a capability to allocate additional resources to support VASP oversight, which will be necessary as the designated supervisor for VA/VASP activities under the upcoming framework and is considering doing so. CySEC is developing its updated directive and determining the conditions for entities registering under the VASP registry it will manage. At this point the first directive will be for the VASP registration process. CySEC is also evaluating specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases to promote efficient off-site supervision.
28. As there is no authority expressly designated as responsible for detecting and identifying unregistered VASP activity, CySEC as the supervisor of VASPs and VASP activities should be designated by the Advisory Authority to perform that function. It would be advisable for VA Kiosks, which currently fall under a potential regulatory gap as CBC views them as outside its remit, to be supervised by CySEC as well, and in any case allocation of such responsibilities should be resolved between CySEC and CBC.
29. Other than CySEC, FI supervisors are awaiting the enactment of the AML/CFT Bill before formulating and issuing their directives or guidance regarding VA activities. FI supervisors have no VA-specific elements to their existing registration, licensing and supervision practices and written procedures to include VA activities. Neither do they have regular procedures to share information and evolving best practices regarding VA/VASP activities. This would be helpful to implement, potentially in collaboration with the Advisory Authority.

30. CBC warnings and concerns articulated by CBC in meetings with potential actors appear to have discouraged CBC-supervised entities from engaging in VA activities and created a perception that they are banned. There is in fact no CBC prohibition against VA. With no VA activity appearing to be under its purview, the CBC has not established supervisory measures tailored to VA or addressed VA. Even in the perceived absence of VA activity, however, the CBC should collect data from its registrants designed to report and detect any VA activity that may occur, and should implement checks (and cause supervised entities to check) that policies to restrict or prohibit VA activity are functioning as designed.
31. CBC and CySEC must update their respective AML/CFT Directives to include measures dealing specifically with VA activities and VASPs promptly after the AML/CFT Law Bill is enacted. The revised directives should expressly incorporate the “travel rule” with regard to procedures for transfers of VA. The CBC should update its AML/CFT Directive to refer expressly to VA, and also cover non-bank FIs like MVTs, EMIs and PSPs with regard to AML/CFT for VA activities.

DNFBP Supervisors

32. ASP supervision is a critical line of defense against ML/TF risks, which may rise as VA/VASP activities develop further in Cyprus, making use of ASP services. The three ASP supervisors were found by Moneyval to have shown different degrees of intensity applying market entry measures and a risk-based approach to licensing and supervision, which Moneyval identified as a vulnerability. ASP supervisors should align supervisory approaches for VA activities and VASPs, share information on ASPs engaged in VA/VASP activities (including rejected applications and withdrawn licenses), and coordinate regarding VA and VASP-related directives and/or guidance.
33. CySEC has acquired experience supervising non-ASP entities engaging in VA/VASP activities, as well as data collection, which could be applied to supervision of ASPs serving VA/VASP clients. ICPAC has established data collection measures to detect VA activity as part of its ongoing monitoring and supervision. It has also directly addressed VA ML/TF risks in its 2020 AML/CFT Directive, including where EDD is required or heightened TF risks may be indicated. The CBA has recently proceeded toward the revision of its AML/CFT Directive to address the VA ML/TF risks in more detail and has also proceeded to revise its standard questionnaire addressed to its members, in order to collect data on VA activity.
34. The Casino Commission at this time detects no direct risks from the use of VAs in the casino, since all transactions are conducted in fiat currency. The assessors consider there is no indirect risk of VA arising from the use of junkets at this time, since all funding should occur directly with the casino, which goes through the controls of the banking system. The NBA also considers that there are no VA being accepted or paid in the betting sector, and it does not permit any licensed firms to accept VA.

Transparency and beneficial ownership (Chapter 7; 10.5; R.24, 25)

35. Cyprus is a company formation and administration center, which increases the materiality of ML/TF vulnerabilities with respect to the misuse of legal persons and arrangements created in the country. Any such vulnerabilities would also be vulnerabilities that apply to legal persons and arrangements engaging in the VA/VASP sector, which would also carry the risk of being misused for ML/TF purposes.
36. For instance, Cyprus has not tracked metrics on percentage of companies under non-resident ownership/control, percentage of companies without Cyprus bank accounts, and percentage of companies under ASP management or part of corporate chains. The DRCOR does not record such metrics on the legal persons and arrangements listed on its registry, including entities planning to engage in VA activities. This may limit authorities' ability to detect potential patterns or typologies of ML/TF risk in connection with VA as funds or VASPs as entities.
37. As a response to Moneyval's identification of vulnerabilities, particularly regarding the outdated information on the DRCOR's company registry and the inconsistencies in the accuracy of ASPs' records, Cyprus has taken measures to improve the accuracy, availability, and transparency of information related to legal persons and arrangements. The DRCOR has undergone a revised framework and is updating its corporate registry, in addition to a series of new BO registers. These improvements should enhance the quality of record information from legal persons and arrangements engaged in the VA/VASP sector. The DRCOR is building an additional BO register for corporate entities. The Mol is updating its current NPO register and aligning it with the DRCOR register. The CBC has developed a bank account register with BO information, to be launched upon enactment of the AML/CFT Bill. CySEC is developing a BO register of trusts.
38. Most importantly, CySEC will establish a comprehensive VASP registry upon enactment of the AML/CFT Bill, with full authority to collect all necessary information regarding legal structure and arrangement, BO and management it deems necessary and to protect against market entry by unsuitable BO and management.³
39. VA activities and VASPs as entities may operate under a range of legal arrangements, outside of legal persons, including newly emerging decentralized structures. This could present novel issues, including potential for unregistered VASP activity, and could present heightened risks in Cyprus. It is advisable that CySEC monitor these developments in VASP structures over time.

International cooperation (Chapter 8; 10.2; R.36-40)

40. Cyprus has well established procedures for international cooperation with countries at an EU level, as well as outside the EU, and has also forged strong ties with relevant authorities. These procedures have shown to be effective and can be utilized for cases involving VA or VASPs. There has been no significant activity to date requiring international cooperation involving VA or VASPs, or statistics collected specific to the VA/VASP sector.

³ As noted above since the period of the report CySEC has enacted its VASP Registration Directive and issued a Policy Statement for VASPs.

41. Cyprus's pending enhancements to its repositories of basic and BO information, in addition to CySEC's VASP registry, should greatly benefit international information sharing as to VASPs and other entities engaging in or supporting VA activities. Cyprus would greatly benefit from leveraging its existing collaborations with other jurisdictions to identify lessons and best practices from international experiences to strengthen and accelerate its capacity building for VA/VASP ML/TF risks. CySEC is examining other countries' experiences and regulatory frameworks to enhance its own supervision toolkit for VASPs and virtual assets, including countries both within the EU and outside the EU.

Effectiveness & Technical Compliance

Effectiveness

42. The assessment team performed detailed analysis of the core issues under each FATF Immediate Outcome to assist in designing and implementing an effective system going forward and assist the relevant supervisory authorities in developing and executing a roadmap. The assessment team did not, however, assign effectiveness scores both because it would be premature (as Cyprus has conducted this risk assessment prior to implementing much of its overall framework for VA/VASP ML/TF risk), and also out of concern that these could be a distraction from the analysis in the report as to the steps needed. An unduly low rating could be unfair, as certain anticipated measures that will follow after enactment of the AML/CFT Bill, are not yet in place. Meanwhile, an unduly high rating could promote overconfidence.

Technical Compliance: R.15:

43. This risk assessment report includes a detailed assessment of R.15 as it directly focuses on VA/VASP ML/TF risks and was the subject of substantial expansion as part of the 2019 updates to the FATF Guidance and Implementation Methodology to incorporate VA and VASP ML/TF risks. See Technical Compliance Annex.

NATIONAL RISK ASSESSMENT REPORT

Preface

1. This report sets forth a national risk assessment for the Republic of Cyprus as prescribed under FATF R.1. The scope of the national risk assessment is expressly limited to VA activities, products, and services, as well as the risks associated with VASPs and the overall VASP sector in Cyprus.⁴ As requested by the Republic of Cyprus, this assessment assumes enactment of the AML/CFT Bill (the Prevention and Suppression of Money Laundering and Terrorist Financing (Amending) Law of 2021), as enacted by Parliament in February 2021.⁵
2. The evaluation was based on information provided by the country, and information obtained by the assessment team during its field work conducted primarily through videoconference (due to the COVID-19 pandemic) between July 15 and January 20, 2020, as well as an on-site visit to the country from October to December 2020.
3. This risk assessment was based on the 2018 FATF Recommendations and the 2019 FATF Guidance, and was prepared using the 2019 Methodology, taking into account the amendments relating to VA/VASPs and identified on page 192 thereof.
 - It analyzes – limited in scope to VA activities and the VASP sector - the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system with respect to VA activities, products, and services, as well as the risks associated with VASPs and the overall VASP sector in Cyprus, and recommends how the system could be strengthened.
 - This assessment also considers how existing ML/TF vulnerabilities identified by the December 2019 Moneyval Fifth Mutual Evaluation Report, which did not consider the VA/VASP sector, may be exploited with the use of VA as assets or VASPs as entities.
4. The assessment team and Cyprus authorities recognized in designing the scope of this risk assessment that only limited measures had as yet been put in place with respect to VA/VASP ML/TF risks. However, it was determined that application of the FATF framework for this report would actually provide the clearest identification of areas of current need, and most concrete roadmap for each authority and sector to establish a strong and effective supervisory framework, drawing in each sector on international best practices and emerging trends and threats in VA. Successful approaches to VA/VASP ML/TF risk must be anchored in and integrated with existing jurisdiction regimes and practices, enhanced to reflect the novel features, technologies and ML/TF risks of the VA/VASP sector.

⁴ See FATF GUIDANCE FOR A RISK-BASED APPROACH - VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (June 2019) Paragraph 60 at pages 19-20.

⁵ The preliminary draft of this report was submitted in January 2021 and refers to periods through December 2020. Comments were received from relevant supervisors and incorporated into the report through August 2021, however the report has not been updated except to acknowledge specific subsequent events identified in the report.

- Looking ahead, one particular international best practice indicates strong leadership and involvement on the part of a specific supervisor with respect to VA/VASP activities. In the case of Cyprus, the assessors strongly recommend that CySEC dedicate sufficient resources and attention to prepare itself to take on such a role and the corresponding responsibilities as the level of VA activities in and affecting Cyprus increase.
5. Cyprus may be vulnerable to entities licensed elsewhere in the EU, such as PSPs or EMIs under the passporting regime and supervised by their respective home supervisors, which may carry out VA/VASP activities undetected by Cyprus supervisors particularly if they do not have a Cyprus-based legal entity or physical location. Similarly, VASPs registered elsewhere in the EU may be excused from registering in Cyprus yet carry out VA activities in Cyprus under Article 61E)4) of the AML/CFT Bill.
 6. It is important to consider that the VA/VASP sector is still evolving, with emerging trends and risks arising accordingly. Trends include new developments with stablecoins⁶, DeFi (decentralized finance)⁷, and privacy-enhanced coins⁸, each posing emerging risks that Cyprus should monitor over time. Selected evolving trends and risks are illustrated in the Supplemental Annex.
 7. As the VA/VASP sector continues to expand on a global level, patterns of crime are becoming increasingly visible for countries to take into consideration for their AML/CFT strategy, and should be considered at the Advisory Authority level.
 - According to a recent industry report,⁹ thefts, hacks, and fraud instances in the VA/VASP sector reached US\$1.9 billion in the year 2020. This is the second highest yearly value of crimes recorded to date in this sector. The magnitude of the overall crime highlights the need for government institutions to play an active role in setting measures to identify and adequately respond to it.
 - The rising interest in DeFi in particular poses significant vulnerabilities, with half of all VA-related thefts in 2020 arising from this area.
 - According to another recent industry report,¹⁰ darknet market revenues have experienced an increasing trend, albeit a decreasing percentage of all VA transaction activity as the overall VA user base expands and institutionalizes around the world.

⁶ Stablecoins cover a broad range of virtual assets, with different structures that generally aim to achieve price stability. See Financial Stability Board report, October 2020, available at <https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/>. Global Digital Finance proposes a taxonomy and key considerations for this category of virtual assets: <https://www.gdf.io/wp-content/uploads/2019/10/GDF-Stablecoin-Key-Considerations.pdf>

⁷ DeFi, which stands for “decentralized finance,” covers a wide range of emerging initiatives aiming to leverage the engagement of communities of users to innovate across a broad spectrum of financial services, use cases, and entities.

⁸ Privacy coins are a category of virtual assets with enhanced anonymity features.

⁹ CipherTrace 2020 Year-End Cryptocurrency Crime and Anti-Money Laundering Report, available at <https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/>

¹⁰ Chainalysis 2020 Crypto Crime Report, available at <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>

8. Given the stage of Cyprus's implementation, the assessment team performed detailed analysis of the core issues under each Immediate Outcome to assist in designing and implementing an effective system going forward. The assessment team did not, however, assign effectiveness scores, out of concern that these could be distraction from the analysis in the report as to the steps needed. An unduly low rating, as certain anticipated measures that will follow after enactment of the AML/CFT Bill are not yet in place, could be unfair. Meanwhile, an unduly high rating could promote overconfidence.
9. The evaluation was conducted by an assessment team consisting of:
 - Mr. Jeffrey Bandman, Principal, Bandman Advisors
 - Ms. Diana Barrero Zalles, Research Associate, Bandman Advisors
10. Recent previous evaluations:
 - Cyprus previously underwent a MONEYVAL Mutual Evaluation published in 2019, conducted according to the 2012 FATF Methodology.
 - Cyprus also conducted a National Risk Assessment published in 2018.
11. Findings of Previous Evaluations:
 - The 2019 Moneyval Mutual Evaluation concluded that that the country was compliant with 16 Recommendations; largely compliant with 21; and partially compliant with 3.
 - ML/TF risks relating to VA/VASPs were outside the scope of the 2019 Moneyval MER.
12. Matters subsequent to 2018 National Risk Assessment and 2019 Moneyval Mutual Evaluation: The assessment team also took notice of and reviewed matters subsequent to these assessments. This included:
 - National AML/CFT Strategy of Cyprus, January 2019
 - Cyprus AML Action Plan – the assessment team also received updates regarding progress with respect to the Action Plan, including implementation of or modifications to the Action Plan, from Advisory Authority entities, as applicable. This assisted the assessment team in determining whether and how weaknesses identified in the risk assessment and relevant to VA/VASP ML/TF risks may have been mitigated.
 - CySEC 2019 AML Consultation
 - The Prevention and Suppression of Money Laundering and Terrorist Financing (Amending) Law of 2021, also referred to herein as AML/CFT Bill.¹¹ As noted above the assessment assumes this Bill is enacted in the form submitted to Parliament in January 2021.
13. The scope of this national risk assessment was limited to VA activities, products, and services, as well as the risks associated with VASPs and the overall VASP sector, in Cyprus.

¹¹ Excerpts related to VA/VASP were selected and translated into English for the assessment team by the Ministry of Finance.

14. The assessment team relied on the descriptions and data provided in the 2019 Moneyval Mutual Evaluation report, including its breakdown and analysis of the Cyprus economy, and legal framework, and baseline data and metrics. Where available and relevant to VA/VASP ML/TF risks the assessment team obtained updated data and metrics. Because VA and VASPs were not within the scope of the 2019 Moneyval Mutual Evaluation Report the assessment team did not rely on it with respect to those matters.
 - This assessment considered whether certain weaknesses, deficiencies or vulnerabilities identified in the 2018 National Risk Assessment or the 2019 Moneyval Mutual Evaluation could potentially be exploited in connection with VA/VASP ML/TF risks.
 - The assessment also considered the impact of controls or mitigants put in place to address those weaknesses, deficiencies or vulnerabilities, as they related to VA/VASP ML/TF risks.
15. Timing considerations: it was requested that this assessment be submitted in conjunction with consideration by Parliament of the draft AML/CFT Bill. Therefore, it was not possible for the assessment team to assess its subsequent implementation.
16. However, the assessment team was asked to take into account the expected impact of this legislation in light of its findings in this risk assessment, and to make recommendations for further strengthening Cyprus's capabilities with regard to ML/TF in respect of VA activities, products, and services, as well as the risks associated with VASPs and the overall VASP sector in Cyprus.

1. ML/TF Risks and Context

Overview of ML/TF Risks:

17. Cyprus is an island situated in the the Mediterranean Sea at the crossroads of Europe, Asia and Africa. The population of Cyprus (Government-controlled area) was estimated at 880,000 as of the end of 2019.¹² Cyprus is an independent sovereign Republic with a presidential system of government. The President is elected by universal suffrage for a five-year term of office. Executive power is exercised through a Council of Ministers appointed by the President. The legislative authority in the Republic is exercised by the House of Representatives. Justice is administered through the Republic's independent judiciary. This report only covers those parts of the island which are under Government control.
18. Cyprus has been a member of the European Union since 1 May 2004 and a Euro Area member since 1 January 2008. Cyprus is also a member of numerous international organisations.

1.1 ML/TF Risks and Scoping of Higher Risk Issues

19. The Moneyval 2019 Report identified a number of sectors, as are set forth in the following paragraphs, as the key risk areas for Cyprus's overall ML/TF Risk Profile. The assessment team found nothing to suggest that these findings were unreasonable, or that responsible Cyprus authorities differed. The assessment team found the risks with respect to VA/VASP ML/TF risks in a number of these areas to be more limited than those found by Moneyval to be arising more generally.
20. Cyprus's status as an international financial centre (IFC): Moneyval found that Cyprus is primarily exposed to external money laundering (ML) threats as non-residents may seek to transfer criminal proceeds to or through Cyprus, particularly through the Cypriot banking system or using trust and company service providers, known in Cyprus as administrative service providers (ASPs) or TCSPS. Moneyval also observed that the risks related to ASP business had experienced some fluctuation between 2012 and 2019. This sector was also identified by the assessment team as potentially relevant to VA/VASP ML/TF risks.
21. Moneyval described domestic ML threats, particularly those deriving from fraud, corruption and drug smuggling, while less significant than foreign threats, as not negligible. The assessment team found no evidence of heightened or additional risk with respect to VA/VASP ML/TF risks in this area.

¹²[https://www.mof.gov.cy/mof/cystat/statistics.nsf/All/6C25304C1E70C304C2257833003432B3/\\$file/Demographic_Statistics_Results-2019-EN-301120.pdf?OpenElement](https://www.mof.gov.cy/mof/cystat/statistics.nsf/All/6C25304C1E70C304C2257833003432B3/$file/Demographic_Statistics_Results-2019-EN-301120.pdf?OpenElement)

22. The Cyprus Investment Programme (CIP) was identified by Moneyval as inherently vulnerable to abuse for ML purposes, along with real estate, both in general and as the apparent preferred investment to acquire citizenship. The assessment team met with the unit at MOI responsible for the CIP and looked closely at this area in the context of VA/VASPs, as well as to understand modifications and controls imposed subsequent to the time of the Moneyval report. The preliminary understanding of the assessment team was that the vulnerabilities in this sphere did not extend to VA/VASP sector, and the way that was CIP is constructed did not appear to allow the easy use of VAs or VASPs. During the on-site visit, news stories about potential political corruption and gaps in controls of the CIP led to the CIP being suspended indefinitely (October 2020) and then terminated. If the programme is someday reintroduced, it could be with new and additional controls, which could include consideration of source of funds arising from VA/VASP ML/TF activities.
23. Moneyval identified the risk landscape of banks within its scoping of higher risk issues. The assessment team found no incremental or heightened ML/TF risks in the VA/VASP sector associated with banks; on the contrary, the assessment team found low VA/VASP ML/TF risk in this sector.
24. Moneyval observed that although the terrorism threat is considered to be low in Cyprus, the authorities rate terrorist financing (TF) risk as medium due to the fact that the country is an IFC and its proximity to conflict areas.
25. VA/VASP Sector: For purposes of a risk assessment focused on VA/VASP ML/TF risk, this sector naturally requires inclusion.

Country's Risk Assessment

26. Cyprus published its first National Risk Assessment (NRA) in October 2018¹³ with the participation of all relevant competent authorities and the involvement of private sector entities. The NRA was based on the World Bank methodology, and the process was managed by the Central Bank of Cyprus (CBC) and the Cyprus FIU (MOKAS). The 2018 NRA found that the international engagement of the financial system heightened the risk of ML. The sectors primarily exposed to external ML threats were found to be the banking sector, followed by Trust and Company Service Providers (TCPS), known in Cyprus as Administrative Service Providers¹⁴ (ASPs), and the real estate sector. TF was analysed separately from ML in the 2018 NRA. It was concluded that Cyprus faces a medium threat level since, despite the low number of any indicators, as an IFC the country faces an elevated exposure. The proximity of the country to areas of intense conflict was also taken into account, as Cyprus is in close proximity to conflict countries with a large amount of terrorist activity. This increases the risk of terrorists

¹³ The NRA was concluded in 2017, covering the period between 2011- June 2016.

¹⁴ The term "Administrative Service Providers (ASPs)" is Cyprus-specific and includes those persons and entities that are licensed to provide administrative services as listed in Section 4(1) of the Administrative Services Law (ASL). Under FATF terminology, administrative service providers are equivalent with the so-called "Trust and Company Service Providers (TCSPs)"

using future Cypriot VASPs to transact in VA they may receive through donations or by selling illicit goods.

27. The present report constitutes Cyprus's first national risk assessment with respect to VA activities, products, and services, as well as the risks associated with VASPs and the overall VASP sector in Cyprus. Prior to the 2019 FATF Guidance and 2019 updates to the FATF Methodology, there was not a requirement to perform such an assessment. Accordingly, the scope of work for this risk assessment included determining Cyprus's understanding and assessment of its own risks, as well as the assessment team's assessment of the reasonableness of said understanding and assessment.
28. The European Commission published its most recent Supranational Risk Assessment in July 2019. This covers risk across the entire European Union, not limited or specific or targeted to Cyprus. The assessment team took note of the risks, threats and vulnerabilities identified in the EC Supranational Risk Report and accompanying staff report, while recognizing that its findings were with regard to the entire European Union and not limited or specific or targeted to Cyprus. The Commission identified 47 products and services that are potentially vulnerable to ML/TF risks. These products and services fall under 11 sectors, including the 10 sectors or products identified by the 4th Anti-Money Laundering Directive.¹⁵ The Supplemental Annex discusses certain of these products. The EC Supranational Risk Assessment also identified an additional category of products and services relevant for the risk assessment which includes virtual currencies.¹⁶ With regard to virtual currencies, the EC Supranational Risk Assessment took particular note of risks relating to anonymity as follows:
- Virtual Currencies - Risk to Financial Sector due to the use of new technologies (FinTech) that enable speedy and anonymous transactions with increasingly non-face-to-face business relationships, while bringing considerable benefits, may pose a higher risk if customer due diligence and transaction monitoring are not conducted efficiently across the delivery channel.¹⁷
 - Virtual Currencies – Horizontal Vulnerabilities Common to All Sectors – where there is potential to achieve anonymity in financial transactions through virtual currencies.¹⁸
 - Risks and Inherent Vulnerabilities: The accompanying staff report noted risks related to use of virtual currencies in crowdfunding.¹⁹

¹⁵ These are: Credit and financial institutions, money remitters, currency exchange offices, high value goods and assets dealers, estate agents, trust and company service providers, auditors, external accountants and tax advisors, notaries and other independent legal professionals, and gambling service providers. EC. July 2019 Supranational Risk Assessment Report at 1.

¹⁶ "This category includes cash-intensive businesses, virtual currencies, crowdfunding and non-profit organisations." Ibid. at 1.

¹⁷ Ibid. at 2-3.

¹⁸ Ibid. at 7.

¹⁹ Staff working document accompanying EC Supranational Risk Assessment at 61. "The inherent risk of crowdfunding is higher if crowdfunding platforms allow use of virtual currencies or (anonymous) electronic money." Ibid at 64, see also ibid. at 65.

- Virtual Currencies – The accompanying staff report also detailed risk scenarios for ML and TF; threat assessment, including significant TF and ML threat related to VAs; and vulnerabilities.²⁰

Scoping of Higher Risk Issues

29. The Moneyval report identified nine areas as those which required an increased focus. All nine were considered by the assessment team to determine whether they merited an increased focus with respect to VA/VASP ML/TF risks. In addition, the assessment team identified within scope of higher risk issues two additional areas:

30. A Securities Sector subsector comprising a limited number of firms already engaged in VA activities; these firms are licensed by CySEC and supervised by CySEC with respect to non-VA activities.

31. The online and offline betting sector (although this sector had been excluded from the scope of the Moneyval report).

32. Here follows a summary of how the assessment team considered those sectors:

- Securities Sector: CySEC-regulated firms already engaged in VA activities: The Moneyval report found the ML risk in the Securities sector to be medium low. The assessment team determined that a small number of firms in the Securities Sector are already engaged in VA activities in Cyprus, and that such firms are licensed and supervised with respect to their non-VA activities by CySEC. The assessment team found that the conduct of these firms of VA activities was known by CySEC and was reported in the context of other activities under MiFID statutory framework. While the existence of these activities does not in and of itself constitute a per se ML/TF threat, these activities are not directly subject to prudential or conduct supervision under existing regulatory framework. The assessment team therefore considered whether these known but not directly supervised activities conducted by regulated firms posed ML/TF threat levels, and assigned this segment of the Securities sector a high priority. The assessment team met directly with several firms within this category.
- Banking sector – The Moneyval report characterized the banking sector as the most vulnerable in Cyprus due to its exposure to external ML/FT threats. The banking sector engages in non-resident business, which often features complex corporate structures, cross-border wire transfers with counterparties in various jurisdictions, introduced business, the use of nominee shareholders/directors, trusts and client accounts. The Moneyval report focused on the banks' ability to effectively mitigate these risks through the application of mitigating measures. The assessment team focused closely on this sector due to these findings. Cyprus banks, including both those domestically focused as well as those engaging in non-resident or international business, had strict policies in place against servicing VASP sector customers or VA activities, as well as monitoring

²⁰ Ibid at 97-105.

controls to detect or prevent such activity. Accordingly the assessment team did not detect any heightened risk with regard to VA activities or VASP sector.

- Administrative Service Providers (ASPs) – The Moneyval report observed that, given that international business is largely introduced to banks by ASPs (including advocates and lawyers’ companies), this sector plays a crucial gatekeeping role in Cyprus. ASPs also act as nominee shareholders and/or directors for Cyprus-registered companies owned/controlled by non-residents. The 2018 NRA considered this sector as the second most vulnerable sector of being misused for ML/FT purposes. The ASP/TCPS sector falls within the responsibility of three different supervisors: the Cyprus Bar Association, the Institute of Certified Public Accountants of Cyprus and the Cyprus Securities and Exchange Commission. The assessment team met directly (separately) with all three supervisors to review the risks, threat and vulnerabilities as well as to examine the effectiveness of supervision (with respect to VA activities and VASP sector) and also to determine whether policies, supervision and monitoring processes of the three supervisors are sufficiently harmonised to ensure consistency in the implementation of preventive measures by the ASP sector as a whole with respect to risks arising from VA activities and VASP sector.
- Transparency of legal persons – The Moneyval report observed that significant levels of international business involve the setting up of companies where the ultimate control is exercised outside of Cyprus by the beneficial owner (BO). Usually, such companies take the form of private limited companies, whose shares may be held by ASPs on behalf of foreign BOs. The Moneyval report analysed the effectiveness of the country’s mechanisms aimed at ensuring the transparency of these entities.
- Citizenship Investment Programme (CIP) – out of scope due to programme termination, as discussed above.
- Real Estate Sector – One of the most common investments to acquire citizenship is real estate. The Moneyval assessment examined whether real estate agents involved in transactions related to the CIP understand the risks and apply effective preventive measures, and considered the role of real estate developers in this context. Due to the suspension and subsequent termination of the CIP, the assessment team did not prioritize this sector.
- Casino – The Moneyval report found significant weaknesses in AML/CFT compliance by the casino, and expressed concerns about planned expansion, including significantly increasing the size of the gaming operations, attracting foreign junket operators, and attracting foreign VIP customers. Because of these identified weaknesses and concerns, the assessment team reviewed closely risks associated with the casino, including CDD, interactions with junket operators, and procedures with foreign VIP customers and customers of the casinos affiliates located in Macau and the Philippines, to ascertain controls and how they might be implicated with respect to risks related to VA or the VASP sector.
- Online casinos are prohibited from operating in Cyprus, however online and in person sports betting is permitted. The assessment team considered risks relating to sports betting as they related to VA and the VASP sector.

- Money Service Businesses (MSBs) – the Moneyval report noted its determination that Cyprus hosts a fairly large population of temporary resident workers from South East Asia and that a considerable amount of outgoing remittances flow through MSBs. The Moneyval report weighted the measures implemented by the sector and the supervision of the sector by the CBC more heavily than those of other financial institutions. The assessment team likewise considered risks of MSBs in relation to VAs and the VASP sector.

33. International cooperation – Moneyval determined that Cyprus is an international financial centre facing a high foreign ML/TF threat. Moneyval also identified concern as to the extent to which Cypriot authorities provide and proactively seek assistance, both formal and informal, from their foreign counterparts to initiate and carry forward domestic ML/FT investigations received additional attention by the assessment team. Another important area in the context of Cyprus is the provision of assistance in the identification, freezing and confiscation of illegal assets traced or channelled through Cyprus and requests concerning BO of Cypriot companies owned by non-residents. Since Cyprus hosts many branches and subsidiaries of banks licensed abroad, attention was also paid to international cooperation. The assessment team considered whether there were additional or heightened risks or other considerations due to the nature or novel technologies presented by VA and the VASP sector, in relation to the foregoing aspects of international cooperation. The assessment team also considered whether there had been specific instances of requested cooperation with regard to VA/VASP sector.

34. Reduced Focus: The areas which were identified by the Moneyval report for reduced focus were the following:

- The insurance sector mainly services domestic clients and is small in terms of assets under management compared to the other financial sub-sectors. The assessment team did not treat this as a sector for reduced focus.
- At the time of the Moneyval’s on-site visit and report, dealers in precious metals and stones (DPMS) were prohibited from conducting any transaction in cash exceeding EUR 10,000 and therefore were not subject to AML/CFT requirements. The assessment team likewise treated this as a sector for reduced focus.

1.2 Materiality

35. The Moneyval report reported the following, which was relied upon by the assessment team:

- Cyprus is a small open economy. Services sectors like tourism, business and financial services are critical for the economy. In 2017 and 2018, the economic growth rate was 4.5% and 3.9% respectively. The GDP in 2018 accounted for EUR 20.730 billion. According to its national accounts, the largest share of Cypriot GDP in 2018 was wholesale and retail trade, followed by real estate activities and financial activities. Tourism, even though not specifically captured in national accounts, contributes significantly to the GDP through national account captured services such as accommodation, recreation, retail trade and associated services.

- Cyprus is an IFC with an important company formation and administration sector. The expansion of the international business sector in Cyprus is largely due to the country's strategic geographical location, at the crossroads of three continents, its advanced professional services sector, its legal framework which is closely based on the English common law, as well as on the existence of a wide network of treaties with other countries for the avoidance of double taxation.
- The Cyprus Investment Programme was material within the economy of Cyprus prior to being suspended and then terminated. The total volume of the funds invested under the CIP for the period 2013-2018 was EUR 6.64 billion. Real estate property is by far the most common type of investment.

36. Cyprus has of course been affected by the COVID-19 pandemic, sharply reducing tourism income and broadly affecting all sectors of the Cyprus economy. However the assessment team did not seek to develop alternate definition of materiality. The assessment team did consider whether conditions of or responses to the pandemic had resulted in identifiable lapses in controls that could increase risk, threats or vulnerabilities of ML/TF with respect to VA/VASP sector; none were identified.

37. VA activity in the Securities sector is low on an outright basis, and accounts for a very small percentage of activities in the Securities sector on a relative basis.

38. CySEC provided data to the assessment team with regard to VA activity by certain of its regulated entities, which enabled the assessment team to develop an understanding of the relatively low level of such activity; however this data has been redacted from this report at CySEC's request due to confidentiality and sensitivity considerations.

1.3. Structural Elements

39. The Moneyval report found that Cyprus has all of the key structural elements required for an effective AML/CFT system including political and institutional stability, governmental rule of law, and a professional and independent judiciary. The assessment team relied on this finding.

1.4. Background and Other Contextual Factors

40. The Moneyval report found that Cyprus has an increasingly mature and sophisticated anti-money laundering/counter-terrorist financing (AML/CFT) system, albeit there is room for improvement in sensitive areas, and that Financial exclusion is not a widespread issue in the country.

41. While Cyprus has a mature and sophisticated AML/CFT system, its system has had quite limited direct experience with AML/CFT issues arising from VA activities or the VASP sector.

1.4.1 AML/CFT Strategy

42. Apart from the registration and initial supervision stages, for which an AML/CFT strategy has been established based on the law that has been amended, Cyprus has not yet articulated an overall AML/CFT Strategy specifically for VA/VASP ML/TF risks. Such risks currently fall within the AML/CFT Strategy described in this section; however, it is anticipated that the findings and recommendations of this risk assessment will be considered in determining whether new or specific modifications to the national AML/CFT Strategy are warranted.
43. The Moneyval report found that Cyprus effectively formulates its national AML/CFT policy and strategy through the Advisory Authority for Combating Money Laundering and Terrorist Financing. The Advisory Authority is presided over both by the Ministry of Finance and the FIU. Its role is primarily to inform the Council of Ministers of any measures taken and the general policy applied against ML/TF and to advise the Council of Ministers about additional measures which, in its opinion, should be taken for the better implementation of the AML/CFT Law.
44. A national AML/CFT strategy was adopted by the Advisory Authority in January 2019 and endorsed by the Council of Ministers in March 2019. The strategy is based on the findings of the NRA and contains the following nine pillars:
1. Minimise the threat and further strengthen supervisory processes in the banking sector;
 2. Upgrade the supervisory processes of the ASP sector;
 3. Upgrade the structure, training and capacity of investigators and prosecutors;
 4. Build on the international cooperation procedures and systems;
 5. Improve data collections and statistics procedures;
 6. Enhance supervisory processes and procedures in other sectors;
 7. Increase transparency of corporate entities and legal arrangements;
 8. Enhance counter TF measures;
 9. Monitor the implementation of anti-corruption measures.
45. The strategy is expected to be subject to ongoing review based on the experience of the authorities involved in its implementation, changes in legislation, developing best practices and the findings of future NRAs. Accordingly, the assessment team recommends that the national AML/CFT strategy be considered in light of the findings and recommendations set forth in this risk assessment.
46. DLT National Strategy: The Republic of Cyprus has also adopted Distributed Ledger Technologies (Blockchain) – A National Strategy for Cyprus (DLT National Strategy). The DLT National Strategy affirms Cyprus’s commitment to ensure that there are adequate AML and consumers/investors protection safeguards in place.
47. The Assessment Team met with the members of the Advisory Authority to confirm these perceptions and observations.

1.4.2 Legal and Institutional Framework

48. Legal Framework: The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007- 2018 (the AML/CFT Law) is the central piece of legislation on AML/CFT matters. It sets out the preventive measures but also provides for the establishment and functioning of the FIU, criminalises ML, includes provisions on the identification, tracing, freezing and confiscation and regulates the international exchange of information, among others. Other relevant pieces of legislation include the sectorial laws regulating the financial and DNFBP sector, the Criminal Code (CC), the Code of Criminal Procedure (CPC), the Suppression of Terrorism Law, the Implementation of UN Security Council Resolutions and EU Restrictive Measures Law, the Control of Cash Law, the Companies Law, the Law Regulating Companies Providing Administrative Services and Related Matters (The ASP Law), the Trustee Law, The International Trusts Law and the Law on Societies and Institutions and other related Matters Law (LSI).
49. The AML/CFT Law is supplemented by various directives issued by the supervisory authorities, including CBC, CySEC, the Casino Commission, the CBA and ICPAC.
50. The AML/CFT Law will be amended by the AML/CFT Bill in 2021 and includes provisions requiring registration for VASPs in Cyprus. The requirements for registration include prerequisites relating to the organisation and operation of the VASP as well as fitness requirements (and absence of criminal background) for management and BOs of the VASP. Further registration conditions are expected to be established by CySEC, which can be expected to further strengthen and safeguard this process.
51. Under the amendment to the AML/CFT Law, VASPs are obliged entities and VA are clearly and unambiguously brought within the AML/CFT Law's definition of property.

1.4.3. Institutional Framework

52. The institutional framework involves a broad range of authorities. The most relevant ones are set forth below. The assessment team found strong understanding with respect to institutional coordination and cooperation, including understanding of respective functions and roles, as well as procedures for coordination and cooperation. The assessment team also found consistently strong direct experience with coordination and cooperation with respect to ML/TF matters generally (not necessarily for VA/VASP-specific ML/TF risks however) :

Coordination and Cooperation and Ministries

- **The Advisory Authority for Combating Money Laundering and Terrorist Financing** (the Advisory Authority) serves as a mechanism for co-operation among all AML/CFT stakeholders and co-ordination for the development and implementation of policies and activities. It is a body established by the Council of Ministers composed of a representative from the FIU, the supervisory authorities, the Ministry of Finance, the Ministry of Justice and Public Order, the Ministry of Foreign Affairs, the Customs and Excise Department, the Cyprus Police, the Company Registry, the association of international banks, the association

of commercial banks, the Inland Revenue Department (the Tax Department), the Casino Commission, the Betting Authority and the Estate Agents Registration Council.

- **The Fusion Centre** is an intergovernmental strategy body which analyses trends and provides quarterly threat assessments on terrorism threats and comprises representatives of the CIS, Police, National Guard and officials of the MFA and the Mol.
- **The Ministry of Finance** co-chairs the Advisory Authority.
- **The Ministry of Foreign Affairs (MFA)** represents Cyprus on issues pertaining to the imposition of UN and EU sanctions.
- **The Ministry of Interior (Mol)** is responsible for the oversight of non-profit organisations (NPOs)
- **The Ministry of Energy, Commerce and Industry (MECI)** issues export licences for dual use goods and military equipment following consultations with, *inter alia*, the MFA, where necessary.
- **The Department of Registrar of Companies and Official Receiver (DRCOR)** within the MECI serves as the company registry.
- Criminal Justice and Operational Agencies
- **The Cyprus FIU** is an independent body within the Law Office of the Republic's Public Prosecutor Office. It discharges the functions set out under R. 29, but also executes MLA requests related to freezing and confiscation.
- **The Cyprus Police** has the general power for investigating all offences in Cyprus, including ML, predicate offence and TF.
- **Law Office of the Republic's Public Prosecutor Office (PPO)** is responsible for the prosecution of ML, predicate offence and FT.
- **The Customs and Excise Department** is responsible for investigating customs-related offences and the implementation of the declaration system for cash/bearer negotiable instruments entering and leaving Cyprus. It is also responsible for controlling the exportation and importation of sensitive goods.
- **The Tax Department** assesses tax and combats domestic tax evasion and provides assistance to overseas tax authorities.
- **The Ministry of Justice and Public Order (MJPO)** is the central authority for the receipt of MLA (including European Investigation Orders (EIOs)) and extradition (including European Arrest Warrants (EAWs)) requests.
- **The Asset Recovery Office (ARO):** The FIU serves as the Asset Recovery Office set up pursuant to the requirements of the relevant EU legislation concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds.
- **The Cyprus Intelligence Service (CIS)** is the intelligence-gathering body of Cyprus.
- **The National Betting Authority (NBA)** is responsible for examining applications, and licensing, auditing and supervising prospective betting shops and online betting operators, for legalised online and offline sports betting under the Betting Law 2012.

Financial and Non-Financial Supervisors

- **The Central Bank of Cyprus (CBC)** licenses and supervises banks, payment institutions, electronic money institutions, credit acquiring firms, currency exchange offices and financial leasing companies.
- **The Cyprus Securities and Exchange Commission (CySEC)** licenses and supervises the capital and stock exchange market, including investment firms, funds and fund managers. It also licenses and supervises ASPs which do not fall under the supervision of the other ASP supervisors (see below).
- **The Insurance Companies and Control Service (ICCS)** licenses and supervises life insurance undertakings.
- **The Institute of Certified Public Accountants (ICPAC)** supervises accounting professionals and licenses and supervises accounting professionals who provide administrative services.
- **The Cyprus Bar Association (CBA)** supervises legal professionals and licenses and supervises legal professionals who provide administrative services.
- **The Estate Agents Registration Council** took over competency from the FIU in May 2018 and since then supervises real estate agents.
- **The Cyprus Gaming and Casino Supervision Commission (Cyprus Gaming Commission or CGC)** licenses and supervises the only operational casino.

VA Activities and VASPs

- CySEC will be responsible for registering of VASPs and operation of the VASP registry under the AML/CFT Bill.
- With regard to ML/TF for VA activities and VASPs, the institutional framework for formulating and implementing the government's ML/TF policies and strategy will be implemented within the structure already in place for other aspects of ML/TF as set forth above.

1.4.4. Financial Sector, DNFBPs and VASPs.

53. There are no VASPs designated as such operating in Cyprus, as the VASP registry has not yet been established. As of June 30, 2020, there were seven firms regulated by CySEC that reported Trading Income deriving from activities as these are defined in Section 5(5)(b) of Law 87(I)/2017, that relates to Trading Income from VA trading, and four firms that reported Volume from activities under Section 5(5)(b) (Volume in VA). An AIFLNP focused on investments in VA has also been licensed by CySEC in 2019.

54. Banking sector: The banking sector was weighted by Moneyval as being the most important in Cyprus based on its materiality and risks. The aggregated assets are about two and a half times the GDP of Cyprus. The banking sector is highly consolidated with the two largest banks accounting for two thirds of the overall assets. The NRA also identified the banking sector as being at high ML risk as its relative size and openness to international business make it attractive to criminals seeking to hide the proceeds of crime among the huge volumes of legitimate business. The assessment team also treated this as a high priority sector in the context of potential exposure to VA activity and VASPs.
55. ASPs or TCSPs: The Moneyval report weighted ASPs as the second most material sector. ASPs, which provide administrative services under the ASL, were rated as medium-high risk by the NRA. ASPs play a critical gatekeeping role since international business is largely introduced to banks by ASPs. ASPs also act as nominee shareholders and/or professional directors for Cyprus-registered companies owned/controlled by non-residents and administer and manage trusts. The assessment team treated this as a high priority area.
56. Real estate agents: these were weighted in the Moneyval report as the third most important sector given their exposure to international risks. As noted, one of the most common investments to acquire citizenship is real estate. The assessment team focused separately on the Cyprus Investment Program and the banking sector, each of which were assigned high priority. After the suspension and subsequent termination of the CIP, the assessment team did not prioritize the real estate agent sector.
57. Casino: The Moneyval report weighted the casino fourth in terms of materiality. There is one licensed land-based casino operator currently in Cyprus (license issued in July 2018), with plans to expand its activities significantly to become an integrated casino resort in 2022. The enlargement of the temporary casino structure, the extension of the services (including junket services) and further satellite casinos were identified as factors that could increase the ML/TF risks and require a number of further mitigation measures. Because of the Moneyval report's findings, the assessment team assigned the casino a high priority level.
58. Money service businesses: The Moneyval report weighted the money service business sector as fifth in terms of priority. Although the sector is not a significant contributor to the economy, representing around 0.02% of GDP, it was found that relatively significant migrant remittance outflows mainly by household workers from the Far East are typically done via the money service business sector. The assessment team assigned similar priority to this sector.
59. Betting Shops and Online Betting Operators: These were out of scope for the Moneyval report. However, the assessment team considered this a priority area in order to determine whether there was a risk of ML/TF involving VA. The assessment team also took note that the National Betting Authority is a constituent of the Cyprus Advisory Authority and is accordingly viewed by Cyprus as a constituent of its AML/CFT efforts.

60. Securities Sector: The Moneyval report found the ML risk in the Securities sector to be medium low. The assessment team determined that a small number of firms in the Securities Sector are already engaged in VA activities in Cyprus, and that such firms are licensed and supervised with respect to their non-VA activities by CySEC. Specifically, a small number of CIFs have sought and received special permission to engage in VA activities under the Cyprus CIF Law of 2007 and CySEC circular C244, which also provides that VA activities must remain under 15% of turnover. No new permissions under C244 have been granted since 2018.²¹ An AIFLNP has been authorized to engage in VA investment. The assessment team found that the engagement of these firms in VA activities was known and specifically authorized by CySEC and was reported in the context of other activities under MiFiD statutory framework. The assessment team therefore assigned this segment of the Securities sector a high priority.
61. VASPs: At the time of the report there was not yet a VASP registration scheme in place in Cyprus, and data were not available as to the size and importance of the VASP sector²². VASPs have not been required to indicate their intention to register once such a framework becomes available. The assessment team assigned this sector a high priority and sought to determine whether there was substantial unregistered or undetected VASP activity in Cyprus.

1.4.4 Preventive Measures

62. Moneyval report found that the preventive measures are set out under the AML/CFT Law and are broadly compliant with the Standards.²³ The AML/CFT Law does not exempt any sectors or activities from these requirements. It extends to certain activities which are not covered by the Standards i.e. auditors and tax advisors.
63. Regarding VA Activities and the VASP sector, preventive measures consistent with 5AMLD and with the Standards are set forth in the forthcoming amendment to the AML/CFT Law. These laws do not exempt any VA activities or any part of the VASP sector from their requirements, with the exception of the deficiency that the AML/CFT Bill does not contain the Travel Rule for wire transfers in VA. This needs to be remediated through establishment of legally binding

²¹ The relevant provision that CIFs were granted permission to engage in VA activities was under the 2007 CIF Law and not under the C244. Firms had submitted their applications under the CIF Law as it was considered an “other service” and “(b) it has received the Commission’s permission, which is granted, at its absolute discretion, in exceptional circumstances” The 15% limitation on the CIF’s total turnover was included in the C244, as the law did not include a provision that applied specifically in DLT services. This was included in a Circular that has now been replaced as in 2018 CySEC stopped accepting any new applications. C244 was published as ESMA/EU had not yet issued their official position determining whether the trading on CFDs relating to virtual currencies falls under paragraph 9, Section C, Annex 1 of MiFiD. Following the publication of the EU’s bodies re the above determination C244 was replaced.

²² Such a registration framework is being instituted under the authority of the new AML/CFT Law and anticipated CySEC registration directive.

²³ Moneyval noted however that dealers in precious metals and stones (DPMS) were prohibited from conducting any transaction in cash exceeding EUR 10,000 and therefore were not subject to preventive measures. The Moneyval report also found that the notarial profession does not exist in Cyprus.

obligations for VASPs and FIs under amended CySEC and CBC AML/CFT Directives (or could be achieved through amendment of the AML/CFT Law).

64. Under the amendment to the AML/CFT Law, VASPs will be obliged entities and VA are clearly and unambiguously brought within the AML/CFT Law's definition of property.

1.4.5 Legal Persons and Arrangements

65. *Legal Persons*: Moneyval found that the types of companies that may be established in Cyprus are provided under Chapter 113 of the Companies Law of Cyprus, namely companies limited by shares and companies limited by guarantee (with or without share capital). Both types of companies can be either private or public. Additionally, the Companies Law contains provisions on the establishment and registration of a place of business of foreign companies in Cyprus (so-called overseas companies). Provisions on the European Company (SE) are made by the Council Regulation (EC) No. 2157/2001, which is directly applicable to Cyprus.

66. Moneyval also found that limited and general partnerships and general partnerships can also be established. Partnerships are governed by the Partnerships and Business Names Law. According to the Partnerships and Business Names Law, general and limited partnerships do not have a separate legal personality. Partnerships are subsumed under the definition of "legal persons". The other forms of legal persons that may be established in Cyprus are societies, federations and associations, which are governed by the LSI.

67. Moneyval reported that private companies of limited liability by shares are by far the most common form of legal person. These companies comprise about 94 % of the total number of registered legal persons as of December 31, 2018.

68. With regard to VASPs or companies engaged in VA activities, there is no separate form of legal person established, recognised or restricted under Cyprus law or that will be established under the amendment to the AML/CFT Law. An emerging form of business undertaking in the VA/VASP landscape is so called "DeFi" or decentralized finance, which may (but does not necessarily) involve initiatives that lack a legal personality or entity. There are no specific or recognised forms of such "DeFi" entities under Cyprus or EU law.

69. *Legal Arrangements*: Cyprus is a signatory to the Hague Convention on Laws Applicable to Trusts and their Recognition. Cyprus has two pieces of trust legislation, namely the Trustee Law of 1955 and the International Trusts Law 1992.

70. According to Section 25A of the ASL, the CySEC, the CBA and the ICPAC each establish and keep a trust register with respect to each trust governed by Cyprus law and where one of its trustees is a regulated entity resident in Cyprus and supervised by the CySEC, the CBA or the ICPAC in its capacity as a competent supervisor. As of December 31, 2018, there were approximately 4,000 registered trusts.

71. In addition to trusts, the LSI provides for the incorporation of institutions.²⁴ According to Section 2 of the LSI, an institution includes assets with a value above EUR 1,000 appropriated by a founder to serve a certain non-profitable object. The incorporation of an institution is effected either by an inter vivos trust instrument or by a will or testament. As from the incorporation of the institution, the founder is bound to transfer to it the property as promised by him (Sections 26 (3), 27 (1) and 30 of the Societies and Institutions Law). As of December 31, 2018 there were approximately 400 institutions registered.

1.4.6 Supervisory Arrangements

72. Sec. 59 of the AML/CFT Law designates the relevant authority to supervise VASPs, FIs and DNFBPs subject to AML/CFT requirements. The CBC supervises banks, payment institutions, electronic money institutions, credit acquiring firms, currency exchange offices and financial leasing companies. CySEC supervises VASPs, the capital and stock exchange market, including investment firms, funds and fund managers, and ASPs which do not fall under the supervision of the other ASP supervisors. The ICCS supervises life insurance undertakings. ICPAC supervises accounting professionals and ASPs. The CBA supervises legal professionals and ASPs. The Casino Commission supervises the only operational casino. The National Betting Authority supervises online and offline sports betting facilities. The Real Estate Registration Council supervises real estate agents.

Supervisory Arrangements for VASPs and VA Activities

73. Article 61E of the AML/CFT law as amended by the 2021 AML/CFT Bill provides authority for CySEC to establish a registry of VASPs and to perform vetting of management and BOs within defined parameters and fitness standards, as well as organizational and operational requirements. A potential VASP that fails to meet these requirements would not be eligible for registration on the VASP registry and would not be permitted to operate or offer services as a VASP in Cyprus.

74. Thus CySEC will be performing supervisory functions as to VASPs, constituted as registration and monitoring, including monitoring compliance with conditions to registration.

75. Other supervised firms providing services to VASPs, or whose customers or counterparties are VASPs or engage in VA activities, products or services but who are not themselves considered VASPs, will continue to be supervised by their existing supervisors.

1.4.7 International Cooperation

76. The Moneyval report found that Cyprus has a broadly comprehensive framework for international co-operation, with incoming and outgoing MLA and extradition requests coming from/going to a wide range of jurisdictions both within and outside of the EU. The MJPO is the

²⁴ Since R.25 broadly applies to “legal arrangements” meaning express trusts and other similar arrangements, institutions are considered legal arrangements for the purposes of this report.

central authority for the receipt of MLA and extradition requests. Requests are transmitted by the MJPO to other domestic authorities for execution, depending on the nature of the request (except for requests dealing with Tax and Customs matters, that go directly to relevant authorities). The Police execute requests for the collection of evidence, such as bank information. Requests relating to freezing and confiscation are executed by the FIU. Extradition requests and EAWs are executed by the Police and the Attorney General's Office. Requests may also be executed by the courts if these relate to the taking of testimonies on oath for cases the hearing of which is ongoing before a foreign court.

77. Cyprus thus has well established procedures for international cooperation with countries at an EU level, as well as outside the EU, and has also forged strong ties with relevant authorities. These procedures have shown to be effective.
78. The assessment team found that Cyprus's existing comprehensive framework for international cooperation would be applied to ML/TF incoming and outgoing requests relating to VA, VA activities or VASPs, or where VA are utilized or implicated, or where requests are made for evidence or relating to confiscation or freezing of VA. The assessment team also found that the appropriate staff at the relevant authorities were aware of procedures that would be applied to ML/TF incoming and outgoing requests relating to VA, VA activities or VASPs, or where VA are utilized or implicated, or where requests are made for evidence or relating to confiscation or freezing of VA. The assessment team found that limited requests related to VA/VASP activity have taken place to date.
79. Cyprus's pending enhancements to its repositories of basic and BO information, in addition to CySEC's VASP registry, should greatly benefit international information sharing as to VASPs and other entities engaging in or supporting VA activities. Cyprus would greatly benefit from leveraging its existing collaborations with other jurisdictions to identify lessons and best practices from international experiences to strengthen and accelerate its capacity building for VA/VASP ML/TF risks.

2 National AML/CFT Policies and Coordination

2.1 Key Findings and Recommended Actions

Key Findings:

1. Cyprus has completed an ML/TF NRA and has been subject to Moneyval MERs, most recently published in 2018 and 2019. Those reports and subsequent actions demonstrate that Cyprus's starting point is a good understanding of its ML/TF risks (independent of VA activities and VASP sector) with a well-developed national strategy and Action Plan, as well as a long-standing body for national coordination. There are also well-established mechanisms for domestic and international cooperation for ML/TF. These provide an effective foundation for Cyprus to be positioned to address ML and TF risks of VA activities and VASP sector.
2. VA activities and VASP sector were out of scope of the 2018 NRA and 2019 Moneyval Report.
3. There is a widespread perception that the VA/VASP sector is high risk, but overall there is limited direct understanding or experience regarding the specific ML and TF risks of VA and VASP sector on the part of key authorities. CySEC has had initial direct supervisory experience supervising ML/TF risks of a small subset of entities it has authorized to conduct VA/VASP activities under a controlled framework, and showed a sophisticated level of understanding of the sector (although limited to a small number of current staff), with demonstrated attention and support from executive leadership.
4. There have been limited access points for VA into the broader Cyprus economy as financial institutions regulated by the CBC have not supported VA activities or VASPs. Similarly, the structure of other areas identified in the NRA or Moneyval report as higher risk do not appear to have access points for VA or VASPs. The assessment team found that VA are not accepted, transmitted or disbursed by banks, securities sector firms, the casino, online or offline betting entities, money transfer businesses, e-money institutions, payment institutions, nor was it accepted as a means of investment under the Cyprus Investment Programme.
5. The Police have acquired some direct experience and sophisticated understanding with VA. MOKAS demonstrated very little direct experience and very limited training on specific attributes of the VA/VASP sector. MOKAS has had a very limited role in the process of this risk assessment. The PPO has very limited experience with VA. This reflects the very limited number to date of criminal cases or complaints, consumer complaints or MLA requests.
6. The assessment team consistently found that a number of authorities expressed an appreciation of the inherent potential riskiness or high risk of VA/VASPs with respect to ML/TF, including the FIU, while noting that they had little or no direct experience to date with VA or VA activities relevant to the scope of their authority in order to actually form a view as to the riskiness. Similarly, while there was an appreciation that the ML/TF risks of VA activity and VASPs may be more likely to originate from outside Cyprus than within, as is the case with other ML/TF risks, threats and vulnerabilities, most authorities, including

the FIU, reported little or no direct experience to date with VA or VA activities relevant to the scope of their authority in order to actually form a view as to the most likely point of origination.

7. Cyprus is mindful of its obligations under the FATF Framework with respect to ML/TF of VA activities and VASP sector, which resulted in the initiation of this national risk assessment. The timing has been delayed by the pandemic, however there has been strong official support for its implementation and execution. Cyprus also is actively seeking recommendations for enhancements to its risk measures based on the findings of this assessment team as well as international best practices.
8. Outreach to the private sector has generally taken the form of consumer warnings as to the riskiness of VA; because there is not widespread use or adoption of VA in Cyprus there generally have not yet been advisories or guidance as to best practices or mitigants to VA/VASP sector ML/TF risks and mitigants.
9. Existing AML/CFT guidance and directives generally do not yet expressly address VA/VASP ML/TF risks or mitigants (other than ICPAC's AML/CFT Directive).
10. No authority has been expressly assigned responsibility under the AML/CFT Bill for detecting unregistered VASP activities.
11. There is little systematic targeted data collection specific to VA activities or VASPs.
12. One type of VA/VASP activity – a virtual asset kiosk, generally known as a “bitcoin ATM” falls within a regulatory gap. Although other authorities assumed it would fall under CBC, the CBC takes a different view as there is not a payment account from which funds are being withdrawn or to which funds are being deposited.

Recommended Actions:

1. As very few specific metrics are collected and maintained at a national level, the relevant authorities should start to maintain and share data and metrics specific to VA/VASP, such as number of SARs/STRS relating to VA/VASPs. Although levels now are negligible, this will enable an evidence-based baseline as activities increase in the future.
2. Further, supervisors should require supervised entities to identify and collect relevant VA/VASP-specific data and metrics in their reporting and recordkeeping so that an evidence-based baseline can be established. Although levels now are negligible, this will enable an evidence-based baseline as activities increase in the future.
3. The regulatory gap regarding bitcoin ATM VA kiosks should be addressed and specific authority for registration established, as the ML/TF risks associated with these kiosks is widely recognised as significant wherever they are offered.
4. Because CySEC will have a critical role leading Cyprus's efforts to mitigate VA/VASP ML/TF risks and educating obliged entities, securing more in-depth knowledge as well as benefit from experience of other jurisdictions will greatly assist it in carrying out these missions.
5. CySEC should be designated as the authority primarily responsible for detecting unregistered VASP activity.
6. It is recommended that directives to be issued by supervisors after enactment of the AML/CFT Bill should make this EDD requirement's application to VA/VASP sector explicit, except for ICPAC whose AML/CFT Directive already makes such reference to this sector.

7. Cyprus should regularly review whether its VASP registration framework is proportionate to VA/VASP ML/TF risks, whether additional conditions to registration are warranted, or whether a licensing scheme should be considered.
8. VA/VASP ML/TF risks should become a regular item on Advisory Authority agenda at least quarterly to enhance monitoring and coordination.
9. Cyprus should communicate the results of this risk assessment to supervisory authorities and to private sector. This should include publication of a concise version, as occurred with the 2018 NRA.
10. If or when Cyprus reinstates the Cyprus Investment Programme, it should consider including controls relating to source of funds arising from VA/VASP ML/TF activities.
11. Further training should be made available with respect to VA/VASP ML/TF risks as well as technological and market evolution in VA/VASP sector.

80. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

2.2 Immediate Outcome 1 (Risk, Policy and Coordination)

2.2.1 Country's understanding of its ML/TF risks with respect to VA activities and VASPs

81. Cyprus has completed an ML/TF NRA and has been subject to a Moneyval MERs, in recent years. Those reports, and subsequent actions in response, demonstrate that Cyprus's starting point is a strong understanding of its ML/TF risks (excluding VA activities and VASP sector, which were out of scope for both reports) with a well-developed national strategy and Action Plan, as well as a long-standing body for national coordination. There are also well-established mechanisms for domestic and international cooperation for ML/TF. These provide an effective foundation for Cyprus to be positioned to address ML/TF risks of VA activities and VASP sector.
82. VA activities and VASP sector were out of scope of the 2018 NRA and 2019 Moneyval Report, however Cyprus was found to be largely compliant with respect to new technologies under R15, again providing an effective foundation, .
83. The assessment team consistently found that authorities expressed an appreciation of the inherent potential riskiness or high risk of VA/VASPs with respect to ML/TF, while noting that they had little or no direct experience to date with VA or VA activities relevant to the scope of their authority in order to actually form a view as to the riskiness. Similarly, while there was an appreciation that the ML/TF risks of VA activity and VASPs may be more likely to originate from outside Cyprus than within, as is the case with other ML/TF risks, threats and vulnerabilities, most authorities reported little or no direct experience to date with VA or VA activities relevant to the scope of their authority in order to actually form a view as to the most likely point of origination.

84. This is not a reflection of indifference or inattention however; rather, it reflects the very limited number to date of criminal cases or complaints, consumer complaints or MLA requests. The FIU and Cyprus Police are well aware that activity with respect to VA/VASPs is likely to increase in the future, and that the inherent risk in these areas can be expected to result in increased ML/TF risk or activity. Within the Police, the Economic Crime and Cyber Units displayed sophisticated and concrete understanding of VA risks and challenges to mitigating them. CySEC has the most supervisory experience with respect to VA due to the CySEC-regulated firms engaging in limited VA activities under current licensing arrangements.
85. The FIU, while aware of general potential for VA to be risky for ML/TF, had very little direct experience, and very little understanding of the knowhow and experience of other jurisdictions. Looking forward to the time after the AML/CFT Bill is enacted, the FIU will nevertheless have an essential role in receiving and acting upon STRs relating to VA activities, and contributing to Cyprus's efforts to mitigate VA/VASP ML/TF risks.
86. CySEC, given its experience with the VA/VASP sector, is well positioned to take a leadership role in Cyprus's efforts to mitigate ML/TF risks arising from VA/VASP activities, such as educating obliged entities regarding identification of suspicious activity in relation to VAs. Securing more in-depth knowledge as well as benefiting from experience of other jurisdictions will greatly assist CySEC in carrying out these missions.
87. Access points for VA into the broader Cyprus economy have been effectively highly limited, as financial institutions regulated by the CBC have not supported VA activities or VASPs. Similarly, the structure of other areas identified in the NRA or Moneyval report as higher risk do not appear to have access points for VA or VASPs. VA are not accepted, transmitted or disbursed by banks, securities sector firms (other than a subset of those known and approved by CySEC to be engaging in VA activities), the casino, online or offline betting entities, money transfer businesses, e-money institutions, payment institutions, nor was it accepted as a means of investment under the Cyprus Investment Programme.
88. Cyprus is mindful of its obligations under the FATF Framework with respect to ML/TF of VA activities and VASP sector, which resulted in the initiation of this national risk assessment. The timing has been delayed by the pandemic, however there has been strong official support for its implementation and execution. Cyprus also is actively seeking recommendations for enhancements to its risk measures based on the findings of this assessment team as well as international best practices.
89. There is very limited data collected or available at this stage of VA and VASP activity in Cyprus to support further evidence-based assessment of actual ML/TF risk or misuse. The absolute number of SARs, STRs or MLAs relating to VA or VASPs reported to the assessment team is less than a handful to date.
90. During the on-site visit period, weaknesses were identified in the Cyprus Investment Programme due to highly publicized media reports. As a result, the Programme was

suspended, then terminated. These weaknesses do not appear to have any specific reference to VA activities or VASP sector and were not considered relevant to the assessment by the assessment team of Cyprus's understanding of its VA/VASP ML/TF risks.

91. Public sector engagement in this risk assessment process at the formative and assessment stage has been robust on the part of relevant Advisory Authority stakeholders other than the Ministry of Foreign Affairs, whose participation was not deemed material by the assessment team.
92. Private sector stakeholder input from both FIs and DNFBPs have formed an integral part of this risk assessment, with the encouragement and facilitation of three relevant supervisory authorities including CBC, CySEC and the Casino Commission.
93. The NPO sector presents an area of potential vulnerability to VA/VASP ML/TF risk separate from the risks likely to be overseen by CySEC with regard to registered VASPs.

2.2.2 National policies to address identified ML/TF risks with respect to VA activities & VASPs

94. The Moneyval report found that there is strong political commitment to AML/CFT, the work of the Advisory Authority and of individual authorities, and that this commitment has been demonstrated by the support provided to AML/CFT initiatives over time. It also found that there is a positive relationship between the Advisory Committee (via its two Co-Chairs) and the Council of Ministers.
95. In light of the membership of the Advisory Authority, the work of the Advisory Authority was found by Moneyval report to comprise part of a national policy and strategy process to address identified risks, developed as a mechanism to formulate, discuss, agree and promote national policies. Where policies require more than bilateral or multi-agency operational activity or agreement, endorsement of the Council of Ministers, to which the Advisory Authority reports, is sought. Prior to 2019 national ML policies arose from this mechanism. Legislative initiatives have been discussed by subcommittees of the Advisory Authority, considered by the Advisory Authority and presented to the Council of Ministers for endorsement.
96. Accordingly, the support of the Advisory Authority in the aggregate and in the capacity of its individual authorities and entities for this risk assessment was viewed by the assessment team as itself forming part of national policy to address identified ML/TF risks with respect to VA/VASPs, as well as to promote the identification of not yet recognized risks.
97. Existing national policies to support ML/TF risks broadly (i.e. not targeted to VA/VASP ML/TF risks) can readily be applied without limitation to ML/TF risks with respect to VA/VASPs. The assessment team did not detect any impediments to applying existing national policies for ML/TF risks to VA/VASP ML/TF risks.

98. The Cyprus national AML/CFT strategy and the Advisory Authority's AML/CFT Action Plan do not expressly address risks arising from VA activities or VASP sector; this omission cannot be demonstrated to have impeded application of existing national policies for ML/TF risks to VA/VASP ML/TF risks. Future updates of both the National Strategy and the Action Plan should address these explicitly where warranted and should be modified in response to the findings of this risk assessment report. The assessment team's understanding is that the Advisory Authority has discussed matters arising from or relating to VA/VASP ML/TF risks, including the need to conduct this risk assessment.

2.2.3 Exemptions, enhanced and simplified measures

99. FIs and DNFBPs are required to apply enhanced due diligence measures in a number of circumstances under the AML/CFT Law, and VASPs once registered will likewise be considered obliged entities subject to that requirement. The assessment team found that the AML/CFT Law may be understood to require EDD for VA activities or circumstances where a customer of an FI or DNFBP or VASP were a VASP or were engaging in VA activities, although VA/VASPs are not expressly enumerated. Specifically, Article 64(3) provides that enhanced customer due diligence measures should be performed for high-risk factors, and in Annex III stipulates a non-exhaustive list of high risk factors that could readily be understood to apply to VA. These include (b) "products or transactions that might favour anonymity"; and (e) "new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products". Certain Cyprus authorities expressed a view that these provisions already implicitly applied to VA/VASPs, thus requiring EDD; however the obliged entities under CySEC which were interviewed by the assessors consistently expressed the understanding that the AML/CFT Law and supervisory Directives did not yet expressly cover VA or VASPs. Nevertheless, the assessment team found that obliged entities were applying EDD with respect to customers engaging in VA activities under their own internal policies.

100. It is recommended that directives to be issued by supervisors after enactment of the AML/CFT Bill should make this EDD requirement's application to VA/VASP sector explicit, except for ICPAC which already currently includes these provisions in its Directive.

101. The enabling framework under the AML/CFT Bill for the VASP registry establishes a legal basis for CySEC to require as a condition of registration of a VASP an obligation to perform EDD measures with regard to customers engaging in VA activities, and it is recommended that CySEC do so. For example, CySEC should make it explicit that for obliged entities considering high risk factors in determining whether to perform EDD, the reference in Annex III(2)(b) to Section 64(3) of the AML/CFT Law with regard to "products or transactions that might favour anonymity" includes VA in light of the propensity of VA products to favour anonymity or pseudonymity., in order to eliminate any ambiguity as to the applicability of Annex III(2)(b) to VA.

102. It is the understanding of the assessment team that Cyprus authorities will apply the findings of this risk assessment to identify areas where requiring enhanced measures may be warranted.
103. Moneyval found a limited exemption from some CDD requirements (identification and verification of identity requirements) exists in relation to electronic money, subject to nine enumerated conditions. The Moneyval report found no information to suggest this exemption was other than low risk. Because of these limitations, including a limitation excluding use of anonymous electronic money, the assessment team did not consider this exemption to pose meaningful risk with respect to VA/VASP ML/TF risk.

2.2.4 Objectives and activities of competent authorities

104. The Moneyval Report found that the national AML/CFT strategy and the Action Plan developed on the basis of the results of the NRA, serve as policy tools which shape the objectives and activities of competent authorities, and that the strategy, which is endorsed by the Council of Ministers, is an expression of Cyprus's political commitment to implement an effective AML/CFT system. It also found that most supervisors are in the process of addressing the specific measures set out in the AA's action plan in order to strengthen the supervisory framework. The assessment team likewise found that AA members and supervisors had strategic plans and had generally advanced in implementing the Action Plan since the time of the Moneyval report.
105. The NRA and the Action Plan did not specifically address VA or the VASP sector or associated ML/TF risks. The assessment team did not find any strategy specific to VA/VASP ML/TF risks. The assessment team found that the improvements identified and executed through the NRA, the Action Plan and the strategic plans of the respective authorities should be helpful with respect to VA/VASP ML/TF risks, although further action will be required to address the VA/VASP ML/TF risks identified in this risk assessment.
106. The assessment team found that authorities are seeking to receive the outcome of this risk assessment in order to identify specific risks and develop policies and controls in response thereto.
107. The assessment team found that the Cyprus Police has dedicated economic crime and cybercrime units and that it had invested in expanding those units, and that these units had developed relevant experience and expertise for matters involving VA. The assessment team also found that the Cyprus Police had developed written plans for confiscating VA, although it has not yet successfully done so.
108. Authorities to date have not yet provided guidance on suspicious transaction reporting and suspicious activity reporting with respect to suspicious VA/VASP activities, or on when to allow a suspicious transaction involving VA to proceed to prevent tipping off. The FIU has not yet updated the automated STR reporting systems to facilitate as well as track VA-related

reports. These are activities that the FIU has indicated that it would consider upon enactment of the framework.

109. The assessment team found that CySEC, which already has supervised entities engaging in VA activities, had an advanced risk-based AML/CFT programme that includes a risk-based supervision framework (RBSF) driven by quantitative as well as qualitative metrics, and that Cyprus is applying its AML oversight to these supervised entities with respect to their VA activities.

2.2.5 National coordination and cooperation

110. The Moneyval report found strong national coordination and cooperation at the policy level as well as at the operational level. It identified the AA as the main coordination mechanism. It also identified AML/CFT cooperation mechanisms across supervisors, such as supervisors of ASPs.

111. With regard to VA/VASP ML/TF, as the sector is quite nascent and the level of activity is low or negligible, the assessment team did not find substantial coordination specific to VA/VASP ML/TF risks, or any specific authority or entity designated as responsible for ensuring coordination or cooperation with respect to VA/VASP ML/TF risks.

112. The assessment team found strong coordination and cooperation at the operational level for VA with regard to MLA between MOKAS and the Cyprus Police. Although actual instances have been very limited, authorities were well versed operationally on who their counterparts were and what procedures and mechanisms to follow for collaboration and cooperation. Coordination with the PPO appeared quite limited however.

113. The assessment team found that the relevant authorities provided sufficient resources to support its performance of this risk assessment, although timeliness of responses varied significantly. The assessment team found that authorities sought to receive the outcome and recommendations of this risk assessment in order to identify specific measures recommended for ensuring appropriate cooperation and coordination.

114. In light of the novelty of the VA/VASP ML/TF framework being introduced in the AML/CFT Bill, the potential for emerging risks, and to ensure that risks do not develop undetected, it would be beneficial for one authority be designated for leading coordination with regard to VA/VASP ML/TF risks, and to put VA/VASP ML/TF risks on the AA docket as a regular agenda item where AA members would be expected to report on any developments in their respective areas of responsibility.

2.2.6 Private sector's awareness of risks

115. The Moneyval report found that the private sector had been involved to an appropriate extent in the risk assessment process and that private sector representatives had been

informed of the results of the 2018 NRA published in its concise form. It also found that some authorities had undertaken additional actions to ensure private sector awareness. With regard to VA/VASP ML/TF risks, those were out of scope of the NRA and Moneyval and thus there were no relevant Moneyval findings on this specific aspect of private sector ML/TF risk awareness.

116. The assessment team finds that the private sector has been substantially involved in the development of this risk assessment through extensive on-site interviews, including the banking sector, the securities sector, the ASP sector and the casino sector. Authorities including the CBC, CySEC and the Casino Commission communicated the nature and importance of this risk assessment to relevant private sector stakeholders who in turn made themselves available to the assessment team. In addition, the AA includes several industry self-regulatory bodies, including ICPAC and CBA, and private sector trade associations, that participated in the risk assessment. Private sector stakeholders for the latter group were not selected to be interviewed by the assessment team, given the greater focus on other entities and sectors.
117. The assessment team found that the private sector strongly understood the ML/TF risk of VA activities and the VASP sector, regardless of whether they or their customers engaged in VA activities or whether they had prohibitions or restrictions on VA activities or servicing the VA sector. The assessment team also found strong understanding on the part of supervised entities with respect to supervisory concerns about ML/TF risks with respect to VA activities and the VASP sector.
118. The assessment team also found that the private sector appreciated the potential for a regulated framework for VASPs or VA activities to be introduced in Cyprus, and that the private sector actively seeks guidance from supervisory authorities as to how achieve ML/TF compliance once the regulatory framework under the AML/CFT Bill is introduced.
119. The assessment team has been informed that it is the intention of Cyprus to make a concise version of this risk assessment available to the private sector and to disseminate its findings to supervised firms and obliged entities. We recommend that this should indeed occur within a reasonable period after submission of this report in conjunction with the effectiveness of the AML/CFT Bill, establishment of the VASP registry and provision of secondary legislation or guidance from relevant authorities, most notably CySEC, CBC and MOKAS.

3 Legal System and Operational Issues

3.1 Key Findings and Recommended Actions

Key Findings:

Immediate Outcome 6

1. There were no specific findings in the NRA or Moneyval reports with respect to ML or FT related to VA activities or VASP sector as those were out of scope.
2. Overall Moneyval report rated Cyprus's level of effectiveness for IO.6 as moderate. Areas identified as in need of major improvement include better use of financial intelligence, such as launching a higher proportion of investigations in response to STRs and FIU reports, which (as Moneyval acknowledges) had been identified by Cyprus in the NRA and was already part of the Cyprus Action Plan. Previous lack of expertise to handle complex analysis cases had been identified as a national vulnerability in the NRA and was also addressed in the Action Plan. These improvements appeared to the assessment team to be well underway, although it did not make a formal assessment in this regard.
3. Moneyval report's assessment of access and use of financial information considered under IO6 the Cyprus Police, FIU, Tax Department and Customs Department. Moneyval found strong cooperation and collaboration across those authorities with respect to sharing, access and use of financial information. The assessment team likewise found evidence of strong collaboration and strong understanding of procedures and persons to collaborate and cooperate with across authorities and a strong history of having done so.
4. The assessment team met with all those stakeholders and found limited specific experiences with access or use of financial information related to VA activities or VASPs. The assessment team found that the Police and MOKAS were familiar with the limited specific instance involving MLA relating to VA in Cyprus and had derived lessons learned from that direct experiences that are informing their future preparedness.
5. In the limited cases that did involve VA activities or VASPs, there were no legal or practical restrictions on the access to or use of information of Cyprus authorities, except in relation to Customs.
6. The assessment team found that Customs understands VA to be outside its competencies due to the non-physical movements of goods. Accordingly, there are no specific procedures for Customs with respect to VA (or VA-related devices) nor are there Customs border declarations regarding VA or metrics regarding VA. Further, there is no legal or statutory requirement to cover any obligation to declare VA movement by passengers or persons crossing borders into Cyprus.
7. The assessment team found that there have been no more than a handful of SARs or STRs in Cyprus to date that related to VA or VASP sector. Cyprus Police and FIU encountered no specific barriers or restrictions.
8. MOKAS utilises the GoAML system with respect to SARs/STRs, and that is also the system that obliged entities in Cyprus use to report SARs and STRs. There are not currently any identifier fields preset for input in GoAML that relate specifically to whether a matter involves VA or VASPs. MOKAS is considering adding an indicator to the form to indicate

VA, to make it easier for obliged entities to report and for metrics to be tracked by obliged entities and MOKAS.

Immediate Outcome 7

1. There were no specific findings in the NRA or Moneyval reports with respect to ML or FT related to VA activities or VASP sector as those were out of scope.
2. Overall Moneyval's rated Cyprus's level of effectiveness for IO.7 as moderate.
3. The assessment team found that there has been an extremely limited population to date of actual incidences of ML cases or alleged offenses arising from or involving VA and that there have been none identified or reported to date involving Cyprus VASPs.
4. The assessment team did not learn of any statistics specifically with respect to VA recorded or maintained with respect to cases or prosecutions specifically involving VA activities or where proceeds of VA are involved. This may be explained by the paucity of incidences to date.
5. The assessment team found that the Police have strong procedures that ensure that if there is an indication that a suspect is in possession of VA or that VA may have been involved in a crime, the cybercrime/forensics units are brought in promptly to perform the relevant actions including investigation.
6. The Police have already had training with regard to VA in regard to cases of ML financing using VA and cases of internet fraud and investment fraud using VA.
7. The Police indicated a need for more investigators and technician resources and expertise proportionate to the anticipated growth in crime, ML and TF using the dark web and VA, and to monitor the dark web more continuously in connection with potential crime or cybercrime, which Police believe is frequently funded, paid for with or rewarded through VA.
8. The Police evinced a highly sophisticated appreciation of the need to preserve evidence, including evidence, in its original state and the necessity of creating a duplicate digital version in the form of a forensic image for investigative purposes or to attempt to locate VA or VA software or accounts. The assessment team also found that the obligation of the Police to preserve evidence in its original state may prove an obstacle to aspects of investigation. While the CyberCrime unit has specialized understanding and tools to make a forensic image and analyse and investigate therefrom, the technology associated with VA may provide opportunities for suspects to make arrangements to move VA before Cyprus authorities can access it, or for it to be impossible to access VA devices without a suspect's cooperation to provide passwords or PINs.
9. Cyprus Police have access to free publicly available tools and databases for investigating and tracing VA. However, Cyprus Police rely on Europol when they have needed to do tracing of VA using paid tools or databases, and do not have the tools or database resources, or training in the use of such tools or database resources, to do so themselves. The Police submit a request to Europol, which responds with a file containing results Europol has found.

Immediate Outcome 8

1. There were no specific findings in the NRA or Moneyval reports with respect to ML or FT related to VA activities or VASP sector as those were out of scope.
2. Overall Moneyval's rated Cyprus's level of effectiveness for IO.8 as moderate.
3. Cyprus authorities have access to a number of lawful mechanisms to freeze or confiscate VA.
4. The assessment team found that there have been no successful freezings or confiscations of VA to date. There has been to date, only one occasion where there was attempt to freeze VAs.
5. The assessment team found that the Cyprus Police have developed written procedures with instructions on how to confiscate VA, and that there has been substantial training of personnel to develop expertise (including forensic expertise) for confiscating VA.
6. It is unclear whether Cyprus authorities have developed the capability to manage storage and asset management of VA that it may freeze or confiscate, or that it has measures in place to safeguard VA from cyberattack or other theft or loss whilst proceedings are pending.
7. It is unclear whether Cyprus authorities have determined how to dispose of or liquidate VA following completion of confiscation.

Recommended Actions:

Immediate Outcome 6

1. MOKAS should request and implement enhancements to the GoAML system to provide for identifier fields that relate to VA activity or VASP so it can more easily direct such requests to appropriately trained personnel and so it can more readily quantify on an evidence-based approach the level of suspicious VA and VASP ML/TF activity and the level of activities develops in the future.
2. While it is likely that the low number of STRs relating to VA and VASP ML/TF risks reflects the low level of activity and low level of abuse in Cyprus, enhancements to the GoAML system should be made to facilitate targeted reporting by obliged entities with respect to VA activities.
3. The FIU should revise its written procedures to add specific VA or VASP-specific procedures, or consider whether a classification of VA STRs as medium/high risk in its analysis process could ensure that such items are included into its enhanced analysis category.
4. It should be considered whether Customs should receive clear statutory authority to examine or inspect for VAs, including VA hardware or storage devices. It should also be considered whether Customs should receive additional and ongoing training to assist them in matters involving VA hardware, such as dedicated crypto wallet storage devices, as well as computer hard drives, in conjunction with relevant staff from the Police.
5. Consider whether Customs should consider whether to add VA as a specific line item on reporting and data collection forms.

Immediate Outcome 7

1. The Police should have direct access to paid blockchain intelligence tools for tracing cryptocurrencies, as well as the appropriate training in use of such tools. Currently the Police go to Europol to do the tracing for them. Because of strong cooperative and collaborative relationship as well as legal arrangements between the Police and Europol, where requested by the Police this has taken place to date reliably and without significant delay. As ML/TF activity relating to VA increases, the time delays could become significant as time may be of the essence or allow suspects or bad actors more time to move the VA out of reach of Police and FIU. We recommend that the Police should not outsource this function from perspective of both time and developing the relevant expertise in house. After meeting with the Economic Crime and Cyber Crime units of the Police, the assessment team believes the Police already has the necessary skill set to perform these activities itself with suitable training. However additional staff or resources may be necessary to build 24/7 capability as activity in this area grows.
2. The Police should collect specific metrics regarding the number and types of cases involving VA so it can calibrate the appropriate level of resources for VA related ML/TF and economic/cyber crime as activity grows in Cyprus and as EU and international activity with a nexus to Cyprus grows. The Police should monitor these metrics, and share with appropriate authorities, to assist in determining the scale and rate of increase and the resulting risk-based need for further training, resources, tools or skill sets.
3. The Police should receive further and ongoing training to assist them in matters involving VA hardware, such as dedicated crypto wallet storage devices, as well as computer hard drives.

Immediate Outcome 8

1. Cyprus should develop a plan for holding and safeguarding VA so that it is prepared to freeze and hold such assets, and safeguard them against attack, theft or loss during pendency of any proceedings. Due to the range of technologies currently used and still evolving in VA, a single approach may not work for all types of VA.
2. In this regard, consideration should be given to the availability and cost of third party service providers as opposed to attempting to perform self-custody.
3. Cyprus should develop a plan for liquidating or auctioning VA in the event of confiscation. Many other jurisdictions have done so, in Europe and internationally, so Cyprus should avail itself of available technical assistance and expertise.

The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

3.2 Immediate Outcome 6 (Financial Intelligence ML/TF)

3.2.1. Use of financial intelligence and other information

Access and use of financial information

120. The Moneyval report found no legal or practical restrictions on the Police's access to information, including financial information and multiple government databases. While the assessment team did not seek to assess the full range of Police access or use of information, as that was beyond the scope of this risk assessment, the assessment team found no specific constraints or differences upon the Police with respect to VA/VASP information or financial information. The Police also provided the assessment team with broad information regarding its overall organization and legal basis for access to information as well as the organization and operation of relevant Police units.
121. Additionally, following the adoption of the AML/CFT amending Law on 23/2/2021, the Police now have access to the Central Bank Accounts Registry and the Police have advised the assessment team that this tool has since been utilised in several cases. The Police have also indicated that in the framework of transposition of "Directive (EU) 2019/1153 of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA", into national law, and following the expected adoption of the relevant Draft Law which has been prepared which amends the AML/CFT Law, the access of the Cyprus Police to bank account information, the exchange of financial information between the Police and the FIU, the exchange of information between Police authorities of different Member States and the exchange of information with Europol, is expected by the Police to be further enhanced.
122. The Moneyval report recognised close collaboration between the Police and the FIU in a wide range of cases and circumstances.
123. Overall the Moneyval report rated Cyprus's level of effectiveness for IO.6 as moderate. The principal areas identified as in need of major improvement include better use of financial intelligence, such as launching a higher proportion of investigations in response to STRs and FIU reports, which (as Moneyval acknowledges) had been identified by Cyprus in the NRA and was already part of the Cyprus Action Plan. Previous lack of expertise to handle complex analysis cases had been identified as a national vulnerability in the NRA and was also addressed in the Action Plan. These improvements appeared to the assessment team to be well advanced, although there is not a formal assessment in this regard.
124. Moneyval reported that the Police access financial and other information fairly frequently in the course of their investigations through court disclosure orders. There are no legal or practical restrictions to the Police's access to information. The Police seek information from a wide variety of sources throughout a criminal investigation.²⁵

²⁵ In particular, the Police acquire banking, beneficial ownership and other CDD information from banks, ASPs, lawyers and accountants. Information is requested from the CBC on licenced entities, the Land Registry on real estate property, including purchase agreements deposited with the Department, the Tax Department on tax declarations and VAT

125. Moneyval identified a robust range of metrics tracked and available regarding access to types of information accessed or disseminated.²⁶
126. The assessment team sought comparable metrics in relation to VA or VASP ML/TF, including any cases where VA was involved even if not the primary focus of alleged or suspicious activity. However, there were limited examples. Metrics regarding Police investigations involving VA are set forth in Section 3.3.1 below (IO.7)
127. VA and VASP-related ML/TF activity or involvement are not currently tracked with any dedicated identifier or classification fields. Determining whether there was a VA component currently requires a manual review of statistics. Consideration should be given to adding a prepopulated field to facilitate tracking of such metrics and establishing a baseline against future growth in VA activities.
128. *Use of Financial Intelligence:* As noted above this was found to be a major weakness in the NRA and Moneyval reports, and the subject of amelioration under the Action Plan. Moneyval noted measures that had already enhanced the capacity of the Police to use FIU financial intelligence.
129. As from 21/1/2021, the reception, registration and processing of all SARs/STRs submitted to the Police by the FIU is undertaken by the newly established Sub-Directorate of Combating Economic Crime (SDCEC) – Economic Crime Investigation Branch which is staffed by properly trained and experienced investigators. Relevant feedback is to be provided to the FIU with respect to the usage of the information distributed and the result of the investigations/measures undertaken on the basis of this information, pursuant to the provisions of section 55(1)(b) of the AML/CFT Law. The work of the Crime Combating Department is coordinated and supervised by the Assistant Chief of the Police (Operations).

information, the Registrar of Companies on company information including financial statements of companies, the Social Insurance Services on the income/salary of individuals and other financial information with respect to companies/individuals acting as employers, the Customs Department on cash declarations and other taxes, the Cyprus Stock Exchange (CSE) on CSE listed companies, the Civil Aviation Department on the ownership of aircrafts and the Merchant Shipping Department on the ownership of vessels. Information is also sought from foreign counterparts both formally and informally. Moneyval also reported that the Police have direct immediate access to the following governmental databases: database of temporary vehicle imports of the Customs Department; database of the Road Transport Department on the owners and details of motor vehicles, driving licenses including professional driving licenses, insurances and road taxes; database of the Registrar of Companies and database of the Civil Registry and Migration Department, including data concerning entry/exit.

²⁶ Such data and measurements include: Court disclosure orders obtained by the Police; Requests sent by the Police to the FIU – for example to determine whether a suspect is known to the FIU, for assistance in asset tracing, or for obtaining information from counterpart FIUs; Requests sent by Customs Department to the FIU; Disseminations by the FIU to the Police and the disposition or use of such FIU intelligence by the Police; Disseminations by the FIU to the Tax Department; Use of FIU Intelligence by the Tax Department; and Disseminations by the FIU to the Tax Department.

130. There has been extremely limited incidence of financial intelligence or other relevant information used in investigations with respect to VA/VASP ML or TF.. Statistics provided by the Police did not identify any instances of receipt or use of STRs or financial intelligence in connection with VA/VASP ML or TF. Metrics regarding Police investigations involving VA more generally are set forth in Section 3.3.1 below (IO.7).

3.2.2. STRs received and requested by competent authorities

131. The Moneyval report found that to a reasonable extent, competent authorities receive reports from the private sector which contain relevant and accurate information that assists them to perform their functions.²⁷

132. In 2019, the FIU received the following reports from obliged entities

Table 3.2.2: FIU Reports by Sector in 2019

Sector	Reports
Banking Institutions	693
Money Service Businesses	567
Investment Firms	157
Company Service Providers	72
Accountants	63
Report Dissemination from FIUs	62
Paypal & Amazon	58
Gambling Businesses	26
Lawyers	23
E-Money	21
Supervisory Authorities	1
Others	20

²⁷ In determining relevance and accuracy, the Moneyval report considered factors such as (1) volume and quality of STRs received; (2) the categories of reporting entities submitting STRs; (3) the number of STRs subject to further analysis by the FIU; (4) the number of STRs used in investigations; (5) the circumstances (indicators) giving rise to the STRs; and (6) whether the STRs correspond to the main risks that Cyprus faces (in terms of volumes of funds, underlying predicate offences, resident and non-resident legal and natural persons involved, typologies, trends and patterns, etc). The Moneyval report also considered STRs relating to significant volumes of funds relating to legal persons registered in Cyprus with non-resident BOs or foreign-registered legal persons with non-resident BOs having bank accounts in Cyprus, of which most related to high-risk predicate offences such as fraud, corruption and tax evasion. The Moneyval report found satisfactory basis to conclude that that the circumstances which generally give rise to reports being submitted to the FIU correspond to the type of business that is carried on from and through Cyprus, which include: insufficient documentation, customers not providing supportive documentation for executed/intended transactions, or provision of fake documents; transactions not in line with declared activity/customer profile; availability of negative information on the customer in open sources; unusual client behaviour, e.g. unclear business activities; absence of economic rationale of activity; and systematic and large cash deposits.

133. During 2018 and 2019, FIU analysis identified that SARs/STRs submitted were triggered by a range of common indicators that triggered submission of reports on the part of obliged entities. These indicators included the following:
- Adverse media about clients
 - Insufficient supporting documentation provided upon request from financial institutions for the purpose of executing transactions
 - Fraud, mostly in the form of investment fraud, electronic fraud, and in some cases VAT fraud
 - Unusual client behavior, either through lack of detail on the underlying business activity, or reluctance to cooperate with authorities, for instance, to provide supporting documentation
 - Transactions with no economic rationale, contrary to normal profit-seeking patterns of business activity
 - Transactions that are not aligned with customer profile or declared activities
 - Law enforcement investigations of clients for any reason, such as court disclosure orders
 - Strawmen, indicating the use of BOs without the necessary knowledge, professional experience, or financial standing to engage in significant transactions, generally for the purpose of hiding true company owners.
 - Discrepancies between declared and actual turnover, without providing adequate justifications
 - False documents submitted, for instance, for the purpose of justifying transactions
 - Systematic cash deposits, which indicate high risk and potential illegal activities
134. The Moneyval report did not specifically consider or analyze STRs relating to VA activities or VASP sector ML/TF risks, nor did it identify or break out separate metrics for these. The above metrics and analysis from MOKAS likewise do not indicate any substantial population of reports arising from or relating to VA or VASP sector ML/TF risks.
135. The assessment team found that there was clear understanding at both a procedural and substantive level as to the actions to be taken in the event of STRs relating to VA/VASP activities or risks. There was not a significant data set of actual SARs or STRs received from which to draw further conclusions.
136. The Moneyval report observed that a low number of STRs were filed relating to TF during the review period and that the majority of these did not really relate to TF but were simply included as a tick-box exercise on the STR by the reporting entity. Concern was expressed that the low number of STRs may suggest a lack of awareness or pro-activeness regarding TF by reporting entities, despite outreach and training given to reporting entities after this issue was identified in the NRA. Moneyval also found under IO 4 that TF risk understanding was less developed than that of ML risk within the private sector generally, and that could also be a factor contributing to the low number of TF-related STRs.

137. Use of VA for TF has been identified as a known and growing risk internationally, and in light of Cyprus's location in relation to conflict areas, Cyprus should ensure that due consideration is given to ensuring that obliged entities consider potential TF risk in formulating STRs with respect to VA and VASP activities.
138. Customs – cash and bearer instruments – Moneyval report found that the FIU has access to information on cash declarations maintained in the Customs Department database, including through the permanent posting of two Customs officers at the FIU, and that Customs information is used regularly in the course of the FIU's analysis. In addition, Moneyval found that the FIU receives and analyzes reports on suspicious declarations from the Customs Department and forwards them appropriately.
139. The assessment team found that Customs regards VA as outside its competencies due to lack of physical transfer of goods, and lack of statutory authority to require any declaration relating to VA. Currently, persons entering or leaving Cyprus with software or hardware VA wallets bear no requirement of any declaration, nor is such a declaration recommended or required by FATF. This is not considered a weakness under FATF guidelines as VA have not been categorised by FATF as requiring treatment as, or comparable to, cash currency or BNI. However, in the event a VA device were identified with respect to a suspicious entry or departure, it is not clear that comparable procedures could be applied.

3.2.3. Operational needs of competent authorities supported by FIU analysis and dissemination

Operational analysis

140. The Moneyval report found that through its analysis and dissemination functions the FIU has the ability to support the operational needs of competent authorities to a large extent, albeit some further enhancements were needed. It found that:
- The staff at the FIU has long-standing experience and is highly qualified;
 - The FIU is equipped with the necessary IT tools to generate actionable financial intelligence which is of value to law enforcement;
 - The internal procedures in place are rigorous; and
 - FIU staff receives training on an ongoing basis.
141. Moneyval also found that the analysis procedure of the FIU is regulated by a written procedures manual which details the actions to be taken at every stage of the analysis. Further, the analysis of STRs is prioritised based on the judgement of the principal officer in consultation with the secondary officer, both of whom are responsible for the case. Reports are categorised as 'high', 'medium', 'medium low' or 'low', depending on the seriousness of the suspicion, the results of the initial intelligence check, and a list of non-exhaustive risk indicators. The risk indicators are generally aligned with the risks identified in the NRA, such that the resources of the FIU are appropriately allocated to the highest risks facing the country. The prioritisation process is conducted manually. Reports that are categorised as low or medium low are accorded a lower degree of attention, though not entirely dismissed. They are recorded in the

FIU database and analysed under a simplified procedure. The focus of the analysis department is on high and medium category cases.

142. The assessment team confirmed that this risk-based approach continues in place. The FIU did not identify any VA or VASP-specific procedures or risk factors as being currently in place.
143. The FIU should consider adding specific procedures with respect to VA, and automatically classifying VA as medium/high risk so that the existing analysis prioritization process ensures that such items are included in the enhanced analysis category.

Strategic Analysis

144. The Moneyval Report observed that the analysis procedures manual instructs analysts to conduct strategic analysis of private sector reports to identify any trends and patterns of ML and FT, and that information on typologies on trends developed on the basis of analysis of private sector reports is presented in the FIU's Annual Reports.
145. The assessment team found that there have not been sufficient private sector reports with respect to VA or VASP ML/TF risks for the analysts to identify any emerging trends or patterns to date of VA or VASP ML and FT in Cyprus, or to present independently developed typologies in the FIU's annual report or other strategic analysis reports.
146. However, the FIU should provide feedback as to quality or trends to other supervisory authorities of obliged entities regarding STR reporting it has received regarding VA, perhaps referencing as relevant red flags and typologies relating to VA/VASP ML and FT, utilising for example the FATF's 2020 Red Flags report. This could be expected to assist in mitigating and preventing emerging risks or activities as use of VA and development of a VASP sector progresses in Cyprus.

Dissemination

147. The Moneyval report recognised that the FIU may disseminate data and information to the Police for the purpose of conducting investigations where reasonable suspicions are identified that ML, predicate offences or FT has been committed. The FIU may also send disseminations to the Customs Department and the Inland Revenue Department for investigation purposes and supervisory and other government authorities for information purposes only.
148. The assessment team found that there had not been any cases of dissemination regarding VA activities or VASP sector; however the assessment team also confirmed that should any such cases arise, the FIU has a clear understanding of how and to whom to disseminate any relevant information.

149. It should be noted with respect to dissemination to Customs that Customs regards VA as generally outside its competencies, thus the effect of dissemination to customs with respect to VA may be of limited or null effectiveness.

3.2.4 Cooperation and exchange of information/financial intelligence

150. The Moneyval report found that the FIU receives full co-operation from all other domestic competent authorities. Moneyval also found that there are no legislative or other barriers which serve as an obstacle to the proper cooperation or exchange of information between the FIU and other competent authorities.

151. The Moneyval report observed that due to close contacts between the FIU and other competent authorities, the FIU often resorts to informal channels of co-operation to expedite the sharing of information. The FIU indicated that it has contact with the Police on a daily basis to strengthen the quality of disseminations. The assessment team likewise found indicia of regular cooperation and communication between the FIU and the Police.

152. Moneyval report expressed concern that the authorities excessively rely on interagency informal contacts, which may result in positive short-term results but not bring about systematic and long-lasting changes.

153. Cooperation and information exchange between the FIU and supervisors is underpinned by a legal provision in the AML/CFT Law. Moneyval found that in practice, there is very close co-operation. Along with the participation of the FIU in the Advisory Authority, where both policy and operational issues are discussed, the FIU communicates with supervisory authorities where compliance matters are identified in the course of the analysis of STRs, in order for appropriate supervisory actions to be taken. The FIU also receives STRs from supervisory authorities where suspicions come to their attention. Strategic analysis and typology reports issued by the FIU are shared with supervisors who apply their contents to their supervisory policies.

154. The assessment team found that there was clear understanding at both a procedural and substantive level as to the cooperation and exchange of information to be performed in the event of STRs relating to VA/VASP activities or risks. As there has only been a single instance of an STR relating to VA/VASP activities there was not a significant data set of actual SARs or STRs received from which to draw further conclusions.

3.3 Immediate Outcome 7 (ML investigation and prosecution)

This outcome relates primarily to Recommendations 3, 30 and 31, and also elements of Recommendations 1, 2, 15, 32, 37, 39 and 40.

Moneyval report found Cyprus to have a moderate level of effectiveness for IO.7.

Cyprus Police – General Overview

155. Cyprus has one national Police Service with 4.950 employees. The Cyprus Police is under the political supervision of the Ministry of Justice and Public Order. The organization of the Police is based upon a hierarchical structure. The Chief and Deputy Chief of Police are appointed by the President of the Republic (Article 131 of the Constitution). The administration of the Police is vested in the Chief of Police who may, for this purpose, issue Police Standing Orders (section 12(1) of Police Laws of 2004-2018). The functions of the Police are divided into four principal areas: education, administration, operations and support services. Each area is supervised by the respective Assistant Chief of Police. As far as the administrative and functional set-up is concerned, the Cyprus Police is divided into Departments, Directorates, Services, Units and Districts. The Police Headquarters is situated in Nicosia and is divided into 5 Departments, 4 Directorates, 5 Services and 5 Units. Cyprus is divided into six operational geographical districts. Divisional HQs operate in each district, situated in the central town of the district, and each has its own geographical / district jurisdiction.
156. Article 130 of the Constitution defines the Police as one of the security forces of the Republic and section 6 of the Police Law of 2004 empowers the Police to act throughout the territory of the Republic for the maintenance of law and order, the preservation of peace, the prevention and detection of crime and the apprehension of offenders. Section 4(1) of the Criminal Procedure Law (Cap.155) provides that any police officer may investigate into the commission of any offence.
157. On the basis of the above-mentioned provisions, the Police is empowered to investigate into any act which by virtue of any law constitutes a criminal offence.
158. Therefore, criminal offences related to financial crime and ML/TF are investigated by the Police. It is noted that pursuant to Section 4(2) of the Criminal Procedure Law (Cap.155), the Council of Ministers or the Attorney General of the Republic may authorise any person, by name or by his office, who appears to be competent for the purpose, to investigate into the commission of any offence. Pursuant to this provision, criminal investigations with particular difficulties may be supported by expert investigators.
159. The allocation of competencies and responsibilities with respect to the recording and investigation of criminal offences within the Police is illustrated in Police Standing Order no.3/4. Paragraph (4) of this Order prescribes in detail the respecting competencies concerning the investigation of serious crime. Accordingly, the recording and investigation of serious criminal offences, including financial crime, is undertaken by the District Crime Investigation Departments. Very serious cases i.e. murder, attempted murder, and also other offences committed within the territorial jurisdiction of Rural Stations, are investigated by officers of the District Crime Investigation Department, at the judgement of the District Police Director.
160. Within the Crime Investigation Departments of Nicosia and Limassol, a separate Economic Crime Section has been established, taking into consideration the number of recorded financial crime in the respecting Districts.

161. The investigation of serious and complicated cases, cases in which prominent persons are involved or cases of public interest is undertaken by officers of the Operations Office of the Crime Combating Department at the Police Headquarters, upon approval of the Chief of Police. This Department has competency and ability to act throughout the Republic.
162. The general supervision and coordination of the investigation of all serious criminal offences, vests with the Director of the Crime Combating Department at the Police Headquarters, without prejudice to the powers and competencies of the District Police Director. For this purpose, the Director of the Crime Combating Department may make observations on mistakes or omissions of the investigator or indicate the procedure to be followed by the investigator. Relevant provisions as to the competencies of the Director of the Crime Combating Department are also provided for in Police Standing Order no. 3/1.
163. The Crime Combating Department consists also of Subdivisions and Offices responsible for combating specified areas of crime and with authority also to act throughout the Republic. These include:
- Office for Combating Intellectual Property Theft and Illegal Gambling
 - Cybercrime Subdivision
 - Domestic Violence and Child Abuse Office
 - Office for Combating Discrimination
 - Office for Combating Trafficking in Human Beings
 - Counter Terrorism Office
 - Office for Handling Mutual Legal Assistance Requests and European Investigation Orders
164. It is noted that the Office for Handling Mutual Legal Assistance Requests and European Investigation Orders, is responsible for the execution of MLA requests and European Investigation Orders submitted to the Police and has also the mandate of assessing the content and particularities of each request, with a view to examine whether there are sufficient grounds to initiate a criminal investigation in Cyprus.
165. The Crime Combating Department is also responsible for the reception and evaluation of analytical files of STRs/SARs submitted to the Police by the FIU for the purpose of conducting investigations on the ground of reasonable suspicions that a money laundering, other offences or terrorism financing offences have been committed. In particular, as from 21/1/2021, the reception, registration and processing of all SARs/STRs submitted to the Police by the FIU is undertaken by the newly established Sub-Directorate of Combating Economic Crime (SDCEC) – Economic Crime Investigation Branch which is staffed by properly trained and experienced investigators. Relevant feedback is to be provided to the FIU with respect to the usage of the information distributed and the result of the investigations/measures undertaken on the basis of this information, pursuant to the provisions of section 55(1)(b) of the AML/CFT Law. The work of the Crime Combating Department is coordinated and supervised by the Assistant Chief of the Police (Operations).

166. The Counter Terrorism Office functions also under the auspices of the Crime Combating Department. The mission of this Office, according to Police Standing Order no.3/39, is the coordination of the activities of the Police for the prevention and combating of terrorism. The main task of this Office, according to paragraph 3(1) of the Police Standing Order no. 3/39, is receiving, analyzing and assessing information concerning terrorism. According also to paragraph 4(2)(2) of Police Standing Order no.3/39, a criminal investigation with respect to terrorism/financing of terrorism offences, may also be initiated on the basis of information/intelligence received by the Counter Terrorism Office and this Office may in turn provide support to local investigations concerning these offences.

167. Drug related crimes are investigated by the Drug Law Enforcement Service at the Police Headquarters. Each District has a Drug Unit, which is administratively and operationally subordinated to the Commander of the Service.

168. It is noted that the work of both the Crime Combating Department and the Drug Law Enforcement Service is coordinated and supervised by the Assistant Chief of the Police (Operations).

Sub-Directorate for Combating Economic Crime (SDCEC), under the Crime Combating Department (CCD).

169. Cyprus Police has established on 11/3/2021 a new Sub-Directorate for Combating Economic Crime (SDCEC), under the Crime Combating Department (CCD). Relevant to the functions of this Sub-Directorate is Police Standing Order 3/20. This Sub-Directorate substitutes and expands the functions of the former Economic Crime Investigation Office (ECIO). The mission of the Sub-Directorate is the investigation of serious and/or complex cases of economic nature, with competency to act throughout the Republic and is composed by the Economic Crime Investigation Branch (ECIB) and the Financial Investigations Branch (FIB). The Sub-Directorate is staffed by properly trained and experienced investigators as well as specialized accountants/auditors. Following the adoption of the AML/CFT amending Law on 23/2/2021, the Cyprus Police has now access to the Central Bank Accounts Registry and the Police report that this tool has since been utilised in several cases.

170. The Economic Crime Investigation Branch is mainly responsible for:

- The investigation of serious criminal cases of corruption and misappropriation of public funds.
- The investigation of serious and complex cases concerning CySEC and the Cyprus Stock Exchange.
- The investigation of criminal cases concerning infringement of EU restrictive measures or UN sanctions.
- The investigation of criminal cases concerning fraud against the financial interests of the European Union

- The investigation of serious and/or complex cases of economic nature (all other cases of financial crime will continue to be investigated by the Economic Crime Offices of the District CIDs and will be supervised and guided by the SDCEC. In case the contribution of the SDCEC is deemed necessary, this will be provided upon approval of the Director of the CDD).
- The reception, registration and processing of all SARs/STRs submitted to the Police by the FIU (as from 21/1/2021).
- The investigation of cases emanating from the execution of European Investigation Orders or Mutual Legal Assistance Requests (concerning in particular foreign predicate proceeds).
- The execution of requests for information submitted through the National SPOC (Interpol, Europol, Liaison Officers, etc) concerning economic crime.

171. With respect in particular to parallel financial investigations, the Chief of Police issued a Circular, dated 12/3/2020, which introduces a "Protocol on Financial Investigations" and provides clear instructions concerning the conducting of financial investigations in the framework of investigation of serious criminal offences. This Protocol is now reflected in Police Standing Order 3/40, dated 11/3/2021, concerning the newly established Sub-Directorate for Combating Economic Crime (SDCEC). The Protocol defines clearly the term "financial investigation", describes in detail the available sources with respect to the collection of financial information and provides guidelines including criteria and preconditions as to the collaboration of investigators with the Team for Conducting Financial Investigations established on 26/9/2019 (this Team forms now a separate Branch of the SBCEC).

172. It is highlighted that according to this Protocol, the Financial Investigations Branch provides support and expertise in conducting financial investigations with respect to the following instances:

1. In the course of investigation of serious criminal cases in connection with offences which incur an imprisonment sentence of five or more years and are complex or involve amounts in excess of EUR 50,000 and from which proceeds have been derived.
2. In all serious criminal cases involving persons involved in organized crime.
3. In any other criminal case where the conduct of a financial investigation is necessary and imposed after consultation and approval of the Deputy Director of the Sub-Directorate for Combating Economic Crime.

173. The Police reported to the assessment team that the Financial Investigations Branch is fully operational and has recently been enhanced by an additional four accountants (total no. of personnel is 7 officers - 5 accountants and 2 police investigators).

174. The Cybercrime Subdivision is capable and responsible for the effective investigation of cybercrime.
175. The specialised body for cybercrime investigation is the Office for Combating Cybercrime of Cyprus Police. The Office was established in September 2007 based on Police Order No. 3/45 in order to implement the Law on the Convention on Cybercrime (Ratifying Law) L.22(III)/2004. This legislation covers hacking, child pornography, racism and fraud committed via electronic communication and the Internet. According to Police Order No. 3/45, the Office is responsible for the investigation of crimes committed via the Internet or via computers and at the same time it is responsible for the investigation of all offences that violate the rules laid down in Law 22(III)/2004. This Office has recently been transformed to a specialized Sub-division of the Crime Combating Department.
176. The main duty of the Subdivision is the investigation of child pornography and hacking cases as well as the following:
- Monitoring of the cases that might be under investigation by other departments and are connected with Internet-related crimes;
 - Co-operation with investigators from other departments;
 - Co-operation with officers from other organizations;
 - Organisation of training sessions;
 - Preparation of statistical reports;
 - Participation in events and lectures;
 - Keeping up-to-date with the latest technology in the area.
177. According to the statistics maintained, the main trends related to cybercrime in Cyprus are the following:
- Child Pornography- possession and invitation of children to take part in child pornography
 - Police Ransomware (cryptolocker)
 - DDos attacks
 - Man in the Middle- emails scams
 - Phishing sites
 - Sexting/sextortion
178. Its work is supported by the Digital Evidence Forensic Laboratory (DEFL), Cyprus Police, which is responsible for the effective examination of electronic evidence. DEFL is staffed with specialised officers for the collection and forensic analysis of electronic devices.

The Digital Evidence Forensic Laboratory (DEFL)

179. The DEFL was established in 2009 and is responsible for the effective examination of electronic evidence. DEFL is staffed with specialised officers for the collection and forensic

analysis of electronic devices. Their mission is the collection and forensic analysis of digital devices as well as the presentation of expert scientific evidence to the courts.

International Cooperation by Cybercrime Subdivision

180. Cyprus cooperates with EU and third countries on the basis of bilateral and multilateral agreements in this field and other channels for exchange of information. The Subdivision cooperates closely with the following organisations:

- Europol/EC3/AWF/ EMPACTS
- EUCTF (European Union Cybercrime Taskforce)
- CIRCAMP (COSPOL Internet Related Child Abusive Material Project)
- ENISA (European Network and Information Security Agency)
- ECTEG (European Cybercrime Training and Education Group)
- CEPOL (European Police College)
- EUROJUST (European Union's Judicial Cooperation Unit)
- CERT-EU (Computer Emergency Response Team)
- INTERPOL (International Criminal Police Organization)
- European Commission
- EEAS (European External Action Service)
- USA FBI
- VCACITF (Violence Crime Against Children International Task Force) USA FBI.
- Council of Europe (T-CY Assessment)

Legislation

181. The main laws in the field of cybercrime in Cyprus are:

1. The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004. This legislation covers hacking, child pornography and fraud committed via electronic communication and the Internet.
2. The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014. This legislation ratifies the EU Directive 2011/93/EE and covers child pornography, grooming and notice and takedown.
3. The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004. This legislation covers racism and xenophobia via computer systems and the Internet.
4. The Law on the Processing of Personal Data, L.138(I)/2001.

5. The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007. This legislation transposed Directive 2006/24/JHA. Although the Directive was invalidated by the Court of Justice of the EU, the national law is still valid. The national law is founded on a constitutional provision and it includes specific safeguards for the protection of privacy; for example, communication data are released only following a court order. A case was recently filed with the Supreme Court on the impact of the annulment of the EU Directive on Law 183(I)/2007 and the Supreme Court found that it complied with the European Convention of Human Rights.
6. Law 112(I)/2004 Regulating Electronic Communication and Postal Services.
7. Law implementing Directive 2013/40/EU on attacks against information system, 147(i)/2015.
182. The National Cybersecurity Strategy was adopted by the Ministerial Council. The Office of the Commissioner of Electronic Communications and Postal Regulations is responsible for its monitoring and implementation. The National Cybersecurity Strategy is the instrument for steering the efforts made by Cyprus to prevent and combat cybercrime. It has provided the structures for the cooperation between all competent authorities, including public, private and non- governmental agencies especially in the field of awareness-raising, to which Cyprus devotes much effort in order to combat this form of crime.
183. Specific emphasis is placed on prevention and awareness-raising. Cyprus has invested a great deal of effort and enthusiasm in teaching and prevention programmes, which may be considered as examples of best practice. This effort is based on the close collaboration of the public sector (Ministry of Education and Culture through the Cyprus Pedagogical Institute) and the private sector, through the Industry (e.g. ISPs), non profit organisations (e.g. Cybersafety, Hope for Children, CNTI), organised groups (School for Parents) which are contributing with enthusiasm in awareness and prevention programmes.
184. The Ministry of Justice and Public Order, together with the Cyprus Police, are the authorities responsible for the prevention and combating of cybercrime.
185. The Subdivision cooperates closely with other governmental departments, NGOs and the private sector as regards the prevention of cybercrime. The Subdivision is responsible for raising awareness in the field of cybercrime. Furthermore, a member of the Subdivision participates on the Advisory Board of “Cybersafety” a co-funded project, which is coordinated by Cyprus Pedagogical Institute. Moreover, the Subdivision implemented in January 2014 the Cybercrime Reporting Platform
https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm
and the Cyprus Police Mobile Application
<http://mobile.cypruspolice.com/landing/Desktop#.VbclTfmm2jw> that allows the public to report cybercrime online.

186. Within the framework of “Prevention of and Fight against Crime Programme” of the European Union (ISEC), Cyprus was granted funding for the establishment of the Cyprus Cybercrime Centre of Excellence (3CE). Furthermore, the Subdivision takes part in Action 14 of the Cybersecurity Strategy of the Republic of Cyprus which deals with cybersecurity awareness, including cybercrime. The Republic of Cyprus is a party to the Council of Europe Convention on Cybercrime (Budapest Convention). The relevant ratification law is L.22(III)/2004.

Cyprus Police Strategic Plan:

187. The Cyprus Police functions on the basis of a comprehensive three-year Strategic Planning which is based on the provisions of the Budgetary Responsibility and Budgetary Framework Law of 2014 (L.20(I)/2014 as amended) which imposes on all public Authorities an obligation to submit for approval a Strategic Planning.

188. The Strategic Planning of the Police is formulated with the contribution of all Police Departments/Services and Units and sets out the strategic targets of the Police, including the determination of the vision and priorities of the Police on the basis of the Governmental policy.

189. The Strategic Planning for the years 2019-2021, as approved by the Minister of Justice and Public Order (as the Minister with whom the general supervision of the Police vests) and the Minister of Finance, comprises of five Strategic Targets, which include fighting of terrorism and radicalization (Strategic Target 2) and combating of serious and organized crime (Strategic Target 4). The activities under the Strategic Target 4 concern in particular actions aiming to combat organized crime and corruption, combating of economic crime, systematic action against narcotic drugs, combating cybercrime and combating trafficking in human beings. The activities to be promoted in implementation of the Strategic Planning include the enhancement and exploitation of all available international police cooperation channels.

3.3.1 ML identification and investigation

190. *Identification of ML cases:* As reported in the Moneyval report, the Cyprus authorities have stated that the sources from which ML may be identified, and investigations initiated, are

- The investigations of predicate offences;
- Intelligence provided by the FIU based on analysis of STRs;
- Disclosures from the Customs Department;
- Incoming mutual legal assistance requests or other information from foreign counterparts (e.g. through EUROPOL/INTERPOL); and
- Complaints by victims of predicate offences or public authorities.

191. Police also receive complaints via other means – for example, via emails alleging fraud arising in Cyprus from businesses or individuals located in Cyprus. The Police have established procedures for following up on such complaints. Where the complaint involves a firm regulated or supervised by CySEC, the first step is typically to contact CySEC with respect to CySEC-regulated firms.

192. Once VASPs are established in Cyprus under the revised AML/CFT Law designating CySEC to operate the VASP registry, the Police should update their procedures to cover receipt of a complaint involving a VASP, providing expressly to contact CySEC with respect to any complaint pointed toward a registered VASP.
193. The assessment team found that to date there had been only a handful of actual cases involving VA, VA activities or VASPs arising under any of these five established and traditional channels. These are described below.
194. The assessment team found that while the relevant authorities could inform the assessors with confidence that there had not been cases arising from these channels, there are not formal metrics maintained tracking VA/VASP sector as a specific category or that support automated retrieval of cases involving VA, and that accordingly for the Police providing statistics on VA-related investigations required a manual process. It could be useful for the Police to start tracking VA-related metrics as a formal category in a manner that supports automated retrieval now, to establish a baseline in the event these categories become more significant.
195. Larnaca Divisional Headquarters: On 01.02.2020, an individual reported to the CID Larnaca, that between the months of November and December 2019, after an advertisement he saw on Facebook of a certain company for the purchase of Bitcoin, he had contact with a male individual. After this individual's phone conversation and guidance, he installed a software program and gave him free access to both his Computer and his Bank account, through which he defrauded € 25000. The case is under investigation.
196. Limassol Divisional Headquarters: Since January 1st, 2016 up until today, a total of 21 complaints have been made which are related to cryptocurrencies, however only one case is still being investigated by the CID Limassol. More specifically, the Complainant was convinced through a fraudulent e-mail and proceeded to invest a total of 20,440 euros in Bitcoin while in the process she lost access to her e-wallet. The other complaints were either referred to the Cybercrime Subdivision, or it was found that the e-wallets had been violated while the complainants were abroad, so they were referred to the authorities of the countries under their jurisdiction.
197. Nicosia Divisional Headquarters: During the last 5 years, 4 complaints have been made to the CID Nicosia regarding internet fraud in relation to Bitcoin. Two of the afore-mentioned complaints have been made for the purpose of providing a relevant certificate and the event was simply recorded, as it was the wish of the complainants, while the other two cases are under investigation. Both cases regard fraud, with the first one amounting to €17000 and the second one to €8220.
198. The Moneyval report recounted that Cyprus recognises in its NRA, Action Plan and AML/CFT Strategy the need to be more proactive in identifying and investigating all types of

ML, particularly where the predicate offence has been committed elsewhere and Cyprus' financial system has been targeted. This has resulted in the setting up of the Cyprus Police's Office for Handling MLA Requests and European Investigation Orders in 2018. This Office is responsible for the execution of MLA requests and European Investigation Orders submitted to the Police and has also the mandate of assessing the content and particularities of each request, with a view to examine whether there are sufficient grounds to initiate a criminal investigation in Cyprus.

199. Since the establishment of the Office, only one EIO relating to VA has been received. This came from the Latvian Authorities, in relation to an ongoing investigation of a fraud case. The EIO was received on 24/9/2020 and has been sent to the CID Limassol for execution. The FIU observed that there have been other MLAs or requests from other FIUs that mentioned VA but without requesting any specific assistance from Cyprus authorities with regard to VA. It will be useful to track metrics specifically relating to VA/VASP ML in such MLAs and EIOs, to provide a baseline in the event activity levels increase after enactment of the AML/CFT Bill.
200. **Investigation of ML cases:** The Moneyval Report did not identify any relevant shortcomings with regard to financial crime investigations, and also highlighted the ability of the Police to avail themselves of the assistance of qualified external accountants. These findings suggest a strong foundation is in place for when ML cases involving a VA or VASP component do in fact arise.
201. The assessment team found that the Police have strong procedures that ensure that if there is an indication that a suspect is in possession of VA or that VA may have been involved in a crime, the cybercrime/forensics units are brought in promptly to perform the relevant actions including investigation.
202. The Police have already had training with regard to VA in regard to cases of ML financing using VA and cases of internet fraud and investment fraud using VA.
203. The Police indicated a need for more investigators and technician resources and expertise proportionate to the anticipated growth in crime, ML and TF using the dark web and VA, and to monitor the dark web more continuously in connection with potential crime or cybercrime, which Police believe is frequently funded, paid for with or rewarded through VA.
204. The Police evinced a highly sophisticated appreciation of the need to preserve evidence, including evidence, in its original state and the necessity of creating a duplicate digital version in the form of a forensic image for investigative purposes or to attempt to locate VA or VA software or accounts. The assessment team also found that the obligation of the Police to preserve evidence in its original state may prove an obstacle to aspects of investigation. While the CyberCrime unit has specialized understanding and tools to make a forensic image and analyse and investigate therefrom, the technology associated with VA may provide opportunities for suspects to make arrangements to move VA before Cyprus authorities can

access it, or for it to be impossible to access VA devices without a suspect's cooperation to provide passwords or PINs.

205. The Police have access to a number of free blockchain forensic tools that assist them in tracing and investigating VA. However, the assessment team found that the Police lacked access to commercial blockchain forensics intelligence tool and databases with respect to VA/VASPs, and that in order to utilise such tools and databases they followed a procedure of sending a request to Europol, which would conduct that aspect of the investigation using the tool/database and send back the results. The Police should have their own direct access to one or more such paid tools and databases, as these are increasingly widely used internationally by law enforcement and FIUs. In addition the Police should be provided with appropriate and ongoing training in use of these tools and databases. Absence of such tools or training could delay or constrain ability of Police to perform timely and effective ML or TF investigations involving VA as adoption in Cyprus increases.

206. **Parallel Financial Investigations:** The Moneyval report observed that the majority of ML investigations have been based on, and parallel to, predicate offence investigations and on STRs/FIU. The Chief of Police issued a Circular, dated 12/3/2020, which introduces a “Protocol on Financial Investigations” and provides clear instructions concerning the conducting of financial investigations in the framework of investigation of serious criminal offences. This Protocol defines clearly the term “financial investigation”, describes in detail the available sources with respect to the collection of financial information and provides guidelines including criteria and preconditions as to the collaboration of investigators with the Financial Investigations Branch. According to this Protocol, the Financial Investigations Branch provides support and expertise in conducting financial investigations with respect to the following instances:

- In the course of investigation of serious criminal cases in connection with offences which incur an imprisonment sentence of five or more years and are complex or involve amounts in excess of EUR 50,000 and from which proceeds have been derived.
- In all serious criminal cases involving persons involved in organized crime.
- In any other criminal case where the conduct of a financial investigation is necessary and imposed after consultation and approval of the Director of the Crime Combating Department.

The assessment team considers that this resource could therefore be made available in cases involving VA/VASP ML whose seriousness or economic magnitude meets the relevant thresholds.

3.3.2 Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

207. Overall: The assessment team found that with regard to investigations there is limited history on which to base findings on this core issue. Dissemination and training regarding materials such as the FATF Red Flag typologies document published in 2020 should be of assistance in helping investigators recognise matters to pursue in future investigations. The

assessment team learned of one prosecution confirmed by the PPO's office associated to date with financial crime related to VA or VA/VASP ML.

208. The assessment team is not aware of well-developed data as to whether VA or VASP ML tends to fall within the category of third party ML, self-laundering or standalone/autonomous ML. As further data regarding any such trends develops internationally or within the EU, this may be monitored by FIU and Police investigators to ensure focus is aligned with evidence-based risk categories.

209. ML risks arising from Cyprus's status as an IFC: Moneyval report found that the relevant authorities all appear to have a good awareness of the substance of the NRA, and are all on the same page as regards implementing the NRA and Action Plan and achieving more systematic targeting of stand-alone/third party/foreign ML. The assessment team found no basis on which to reach any different conclusion with regard to potential VA/VASP ML falling within these categories. While the NRA and Moneyval report found greater incidence of foreign ML arising from foreign predicate criminality targeting Cyprus, and could perhaps be expected to be repeated with respect to VA/VASP ML, the assessment team found no evidence demonstrating this pattern to be repeated as yet. As further data regarding any such pattern develops internationally or within the EU, this should be monitored by FIU and Police investigators to ensure focus is aligned with evidence-based pattern typologies.

210. ML risks arising from domestic criminality: The assessment team found no evidence to date of VA or VASP ML risks arising from domestic criminality, although this is certainly well within known typologies. The assessment team found no reason to expect any hesitation or reluctance to pursue investigations or prosecutions with respect to domestic criminality and related VA or VASP ML.

211. ML risks arising from specific events/issues: As a result of disclosures regarding the CIP, which was suspended and then terminated, authorities are conducting an in-depth review of passports awarded under the programme dating back to 2007. This process, which commenced during the period during which this report was being prepared, may lead to ML investigations or prosecutions. The outcome is not known at the time of this assessment. The assessment team met with subject matter experts involved in reviewing the programme. There is no indication to date of any VA or VASP related ML associated with applications or awarding of passports under the programme.

3.3.3 Types of ML cases pursued

212. The assessment team found that there has been one ML prosecution or conviction to date involving VA or VASP ML, as confirmed by the PPO office. In this case, which was a drug trafficking case, a court order to freeze VA was obtained, and the Police's Electronic Crime Department (Cybercrime Sub-Directorate of Cyprus Police) provided assistance.

213. The Moneyval report found that Cyprus has a strong framework for prosecuting ML, in that there is no requirement for a previous or simultaneous predicate conviction, and that the knowledge, intention or purpose which are required as elements of the ML offence may be inferred from objective and factual circumstances.
214. The Moneyval report noted that there is no specialised unit for ML (or financial crime generally) within the PPO and that prosecution authorities may benefit from further specialisation in financial crime (including ML and TF) and having dedicated units (e.g. Roskill model) as the police do, although it also acknowledged the recent GRECO report. Moneyval also took notice that cases were generally allocated now depending on experience, so financial crime cases are handled by those with sufficient expertise.
215. The assessment team found that prosecutors have not to date received special training regarding VA or financial crimes involving VA, and that any case involving VA that arises would not be handled by a specialized unit within the PPO, but would be handled by an experienced prosecutor as any other serious case in the office, with the assistance of MOKAS and the special unit of the Police. Prosecution of ML offenses involving VA may require specialised expertise, and the assessment team has observed that in other jurisdictions there are increasingly prosecutors and prosecution units who have specialised expertise in VA. Current levels of activity in Cyprus do not appear to warrant such specialisation at this time but should be considered should future levels start to increase.

3.3.4 Effectiveness, proportionality and dissuasiveness of sanctions

216. The Moneyval report found that the framework in the AML/CFT Law provides for sufficiently effective, proportionate and dissuasive sanctions.
217. The AML/CFT Law as amended by the AML/CFT Bill clearly provides that cryptoassets (VA) are to be included within the statutory definition of “property” and thus will unambiguously fall within this framework, which has been found to be sufficiently effective, proportionate and dissuasive.

3.3.5 Extent to which other criminal justice measures are applied where a ML conviction is not possible

218. The assessment team did not learn of any such scenarios that had actually arisen with respect to VA or VASP ML to date.
219. Cyprus has a Non-Conviction Based Forfeiture (NCBF) regime limited to where the defendant is no longer alive or is outside the jurisdiction. The Moneyval report observed that as a regime, it has been underutilised, and suggested that there are practical restrictions on being able to utilise the regime.

220. It seems plausible that MLA may form a basis for future prosecution of ML for foreign predicate offending.

221. Where there are VA assets in Cyprus, it may be practical to use NCBF powers to disrupt ML and dilute any attractiveness of Cyprus as a centre for laundering proceeds. The assessment team has confirmed that the AML/CFT Bill clarifies that VA is included as a category of property under the NCBF framework. However, it is the view of MOKAS that the provisions of the AML/CFT Law regarding domestic court orders for non-conviction based forfeiture (confiscation) can be applied only in very limited circumstances and under very strict specific conditions that make it unlikely that the Cyprus NCBF regime would be highly effective with regard to VA. Therefore, as far as freezing and confiscation of VA is concerned, it is most likely that this should be made on the freezing and confiscation Court orders obtained under the provisions of the AML/CFT Law and not on NCBF Confiscation Orders, unless the legal requirements for NCBF are adjusted in the future.

3.4 Immediate Outcome 8 (Confiscation)

3.4.1 Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective:

222. The Moneyval report found unequivocally that Cyprus has a comprehensive framework in place for confiscation and identified numerous indicators to reinforce that clear national policy objective.

223. The AML/CFT Law as amended in 2020 expands the definition of property in line with the 2019 FATF Guidelines to include VA; this has the legal effect of clearly applying forfeiture provisions – both criminal and NCBF – to VA.

224. The assessment team found no limitation of this framework or policy objective in respect of VA.

225. The assessment team was informed that in 2018 the Cyprus Police had prepared a manual with clear instructions on how to confiscate VA. The assessment team also was informed that 2-3 personnel had undergone training to become forensic experts in confiscating VA.

3.4.2 Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad

226. Moneyval concluded that Cyprus has demonstrated to a reasonable extent that it is confiscating criminal property (primarily proceeds or property of an equivalent value) further to domestic criminality, or on the request of another jurisdiction as regards the proceeds of foreign criminality, and that LEAs appear to be well resourced and equipped to carry out the

investigations required to trace and seize property in relation to domestic cases and build those cases to successfully get confiscation orders. A concern was expressed however as to Cyprus's capacity to manage increased confiscation activities. An increase in general quantity of activities of confiscation relation to VA, or novel confiscation processes related to VA, could accordingly per the Moneyval finding challenge the jurisdiction's ability to manage.

227. Moneyval highlighted the FIU's particularly successful record in achieving the confiscation of assets representing foreign proceeds of crime pursuant to requests from other jurisdictions (where the majority of such cases relate to property held by legal entities in Cyprus). Moneyval also noted that the FIU has the power to issue postponement orders under §55 of the AML/CFT Law. These powers have been used and the FIU has also sought freezing orders (even when not requested to do so by the requesting jurisdiction) to enable the effective prevention of assets being removed/dissipated prior to their confiscation and repatriation to the requesting jurisdiction. The Moneyval report recognised that Cyprus is at an advantage having the use of such formal postponement powers.
228. *Enforcement of orders and experience of freezing and confiscations:* The assessment team learned of a single instance, as described in Box 1 below, where Cyprus authorities attempted to freeze VA in response to a domestic case of drug trafficking, but were unable to do so in time. Cyprus authorities were able to freeze other non-VA assets of the same suspect.
229. The assessment team learned of no other instances where Cyprus authorities had sought to freeze, confiscate or otherwise access VA. The assessment team found that to date Cyprus has not effected a freezing or confiscation of VA. The number of opportunities to do so has been quite limited as of the date of the on-site visit. The assessment team found that there had been timely development of written procedures for freezing/confiscation of VA as well as dedicated training, and a sophisticated level of understanding by the Cyprus Police with regard to freezing and confiscating VA.
230. The assessment team also found that the obligation of the Police to preserve evidence in its original state has already been an obstacle to effective freezing or confiscation. While the CyberCrime unit has specialized understanding and tools to make a forensic image, the technology associated with VA may provide opportunities for suspects to make arrangements to move VA before Cyprus authorities can access it, or for it to be impossible to access VA without a suspect's cooperation to provide passwords or PINs.
231. The assessment team found that Cyprus Police are aware that in the time that may elapse between the time of seizure of a device such as a computer at a crime scene and the time at which it may be examined by the CyberCrime unit, a suspect may be able to access VA through different means and potentially transfer it, thus effectively thwarting potential for freezing or confiscation. Accordingly, if the Police have information that the suspect may have been using VA or VA in somehow involved, they know to bring the CyberCrime Unit and DEFL digital forensics team in right away. To the extent this understanding is informal rather than

based on formal written procedures, such procedures should be adopted and communicated to relevant personnel.

232. The assessment team found that Cyprus Police have a clear understanding with regard to procedures to follow in the event that a suspect is located in another jurisdiction, or has a wallet at an exchange operating or headquartered in another jurisdiction, and stands ready to seek VA through such procedures.

Box 1: Domestic Case of Drug Trafficking

MOKAS has had one case involving freezing of VA (bitcoin) and other property. MOKAS was able to successfully obtain the freezing order. The suspect managed to arrange to move the VA before Cyprus Police, which was responsible for executing the freezing order, was able to execute the freezing order for the VA. (Other property of the suspect was in fact frozen). Cyprus Police and MOKAS personnel have subsequently undertaken further training with regard to executing freezes of VA more rapidly.

Box 2: Confiscation Attempt Involving VA

The Cyprus Police had a case involving an attack on a local ISP. The Police identified the suspect and confiscated cash and some credit cards. The Police also forensically examined his mobile phone and detected that there were some VA wallets on it. However, the Police were not able to access these online wallets. The Police noted a number of limitations impinging their ability to do so. First, from a forensic perspective, the Police have a duty to protect evidence. Thus, Police procedures dictate they first generate a forensic image of a computer, laptop, tablet, mobile or other device, then use the forensic image and use special tools. Second, persons with VA wallets on their phones typically enable 2FA or 3FA (two factor authentication or three factor authentication) to access the wallet, which requires Police to have access to associated email accounts or other means. As confirmed by the FIU, however, no confiscation order was obtained.

Box 3: Investigation/Confiscation Attempt involving VA

The Cyprus Police had a case where the underlying predicate offense involved gambling. The suspect had a dedicated hardware wallet (Trezor) device. Cyprus Police attempted to access the device in the forensics lab but were unable to access any VA stored on or with the device because it was protected by unknown PIN codes that the suspect was unwilling and was not compelled to provide. As confirmed by the FIU, however, no confiscation order was obtained.

233. *Management of seized and confiscated assets:* The assessment team did not determine whether Cyprus authorities have developed the capability to manage storage and asset management of VA that it may freeze or confiscate, or that it has measures in place to safeguard VA from cyberattack or other theft or loss whilst proceedings are pending. In the event Cyprus authorities succeed in freezing or confiscating VA, it will be necessary for Cyprus to have measures in place to preserve and manage the value and safety of VA.
234. Cyprus should develop a plan for holding and safeguarding VA so that it is prepared to freeze and hold such assets, and safeguard them against attack, theft or loss during pendency of any proceedings. Due to the range of technologies currently used and still evolving in VA, a single approach may not work for all types of VA. In this regard, consideration should be given to the availability and cost of third party service providers as opposed to attempting to perform self-custody.
235. Cyprus should develop a plan for liquidating VA in the event of confiscation. A number of other jurisdictions have liquidated VA through public auction, or other means, in Europe and internationally, so Cyprus should consider availing itself of such technical assistance and expertise from other jurisdictions.
236. ***Non-Conviction based forfeiture:*** Cyprus's non-conviction-based forfeiture (NCBF) regime goes beyond the FATF standards and enhances the Law Enforcement Authorities' arsenal in confiscating criminal property. The NCBF regime applies when the defendant is outside the jurisdiction or has died. The prosecutor must still present evidence and establish a prima facie case that the suspect committed the offence, and also satisfy the court that reasonable efforts have been made to locate the suspect. The Moneyval report found, therefore, that the NCBF system was useful only to a certain extent and suggested Cyprus consider amending it. Cyprus has also enacted legislation to register NCBF orders made in other jurisdictions, with the first order successfully registered in July 2019.
237. The assessment team did not learn of any specific instances where the NCBF regime had been applied to VA. Helpfully, due to the amendment to the AML/CFT Law, VA are included as eligible assets for NCBF under the applicable statute. In theory, this regime could provide Cyprus authorities with a useful tool with respect to VA in excess of FATF requirements.
238. However, it is the view of MOKAS that the provisions of the AML/CFT Law regarding domestic court orders for non-conviction based forfeiture (confiscation) can be applied only in very limited circumstances and under very strict specific conditions that make it unlikely that the Cyprus NCBF regime would be highly effective with regard to VA. Therefore, as far as freezing and confiscation of VA is concerned, it is most likely that this should be made on the freezing and confiscation Court orders obtained under the provisions of the AML/CFT Law and not on NCBF Confiscation Orders, unless the legal requirements for NCBF are adjusted in the future.

3.4.3 Confiscation of falsely or undeclared cross-border transaction of currency/BNI

239. This core issue is not applicable to VA. VA does not have the legal status of a currency in Cyprus or the EU. While VA shares certain attributes with BNI (to greater or lesser degrees depending on the privacy features of the VA), FATF has not classified VA as BNI nor suggested in the Assessment Methodology that VA should be assessed under IO8 in connection with this core issue.

240. The assessment team found that Customs had an awareness of the potential for persons entering or leaving Cyprus to be in possession of VA hardware devices, however there has been no specific guidance nor specific procedures established in this regard. Notwithstanding that these have been a feature of this new technology, the 2019 updates to the FATF Guidelines (including R.15 and INR.15) have not introduced any recommendations with regard to such devices.

241. The assessment team found that it is the understanding of Customs that VA fall outside the scope of Department of Customs and Excise competencies due to the non-physical movement of the goods, and the absence of legislation covering any obligation of passengers or persons crossing borders to declare movement of VA.

3.4.4 Consistency of confiscation results with ML/FT risks and national AML/CFT policies and priorities

242. The Moneyval report found Cyprus has achieved appreciable results as regards the confiscation of assets representing the proceeds of domestic criminality and, pursuant to requests for assistance, those representing the proceeds of foreign criminality. In contrast, it found Cyprus less effective in freezing and confiscating the proceeds of foreign criminality, on the initiative of the domestic authorities (as opposed to be where it is triggered by requests from other jurisdictions).

243. The assessment team found that there has been insufficient activity, regardless of locus of the criminality, to determine whether this concern may repeat itself with respect to VA.

244. The assessment team found the sample size of confiscation results related to VA is extremely limited. While the Cyprus Police have yet to effect a successful confiscation, the assessment team expressly finds that that is not an outcome of lack of policy attention or prioritization.

245. Metrics should be maintained with regard to VA proceeds of criminality in Cyprus, and with respect to effectiveness of attempts to freeze or confiscate VA, so that effectiveness as well as alignment with policy priorities can be addressed once sufficient activity has transpired for any such pattern to emerge.

246. Conclusion: while consistency of results has not matched policy priorities, available evidence suggests it should be attributed to low levels of VA activity rather than to any weakness of policy alignment or prioritisation.

4. Terrorist Financing and Financing of Proliferation

4.1 Key Findings and Recommended Actions

Key Findings:

Immediate Outcome 9

1. Cyprus's status as an ICF and geographical proximity to conflict zones heighten its vulnerabilities to terrorist activities and risks of TF, including use of VA or VASPs to support TF.
2. While supervisory authorities have taken steps to enhance their capabilities to investigate and respond to TF cases, and also harvest additional TF investigations, there have still been few cases of TF identified.
3. The TF Convention, incorporated into the 2001 Cyprus Law to Ratify the International Convention for the Suppression of the Financing of Terrorism, provides a definition of funds that is broad enough to cover VA as a form of asset for TF purposes.
 - a) There have been no TF cases reported as involving VA, and hence no prosecutions, convictions, or sanctions implemented for TF VA.
4. National strategies for the purpose of counterterrorism do not specifically address TF risks arising from VA activities or VASP sector.
5. Most supervisory entities have no VA-specific targeted measures or capabilities to investigate and prosecute TF cases involving VA as a form of funding, or VASPs.
 - a) There is also a lack of direct and immediate access to commercial VA tracing and risk intelligence tools. This could hinder TF investigations with a VA component, and also inhibit investigations of VA activity that could lead to detection of TF activity.

Immediate Outcome 10

Targeted Financial Sanctions

1. Cyprus has a framework with a series of mechanisms at its disposal, both at an EU supranational and a national level, to implement targeted financial sanctions (TFS) without delay.
 - a) Cyprus has adopted international agreements and legislation for TFS.
 - b) Domestic communication systems notify competent authorities and obliged entities of new designations and also any freezing measures applied under the TFS regime. While these systems have not prepared to notify VASPs as obliged entities under the AML/CFT Bill, doing so will be a simple procedural step for applicable supervisors, primarily CySEC.
 - c) VASPs will be obliged entities under the AML/CFT Bill, and as such it can be expected that the designations, obligations and measures communicated to obliged entities would also be effectively communicated to VASPs.
2. There have been no TF cases detected and thus no TFS implemented.

3. Cyprus has no TF risk mitigating measures in place tailored to the VA/VASP sector, either with VA as the form of funds, or involving VASPs. This heightens existing vulnerabilities for the VA/VASP sector in addition to the existing vulnerabilities.
4. Obligated entities understand the need to have protocols in place to freeze assets as component of TFS implementation. Yet there are shortcomings with respect to screening practices of certain obliged entities, which could represent vulnerabilities in the ability to implement TFS measures when necessary. In the absence of VA/VASP-targeted measures, this vulnerability would be heightened for cases involving TF actors using VA as funds or VASPs.
5. Decisions on updated designations for lists announced after Nicosia business hours on a Friday may not be communicated by supervisors until the next Business Day. Because VA markets, unlike traditional financial markets, are active constantly and outside of business hours, and transactions and movements of assets occur 24/7/365 unlike traditional movements of fiat currency, this could be a meaningful gap with regard to VASPs and movement of VA for TF purposes. Although VASPs as obliged entities should also subscribe directly to databases that also provide these updates independent of the supervisory notification channel, thus mitigating the risk of this gap, a gap remains.

Non-profit organizations

6. The assessors found the current measures to mitigate NPO vulnerabilities, including the consulting project and risk assessment currently being undertaken on behalf of MOI (described below), are not taking into account the VA/VASP sector. This leaves important VA/VASP ML/TF vulnerabilities unaddressed.
 - a) Existing overall ML/TF vulnerabilities can be exploited through VA/VASP activities.
 - b) Upon the enactment of the Cyprus framework for the VA/VASP sector and the expected rise of such activities, vulnerabilities may take the form of receiving VA obtained from illicit activities as donations to fund NPOs, or TF activities raising funds in VA through NPOs.
7. The Cyprus NPO sector has not developed or implemented targeted AML/CFT measures, which represents a significant vulnerability emphasized by Moneyval.
 - a) There are no measures to identify source of funds or conduct due diligence.
 - b) NPOs are not obliged entities as defined by Article 2A of the Cyprus AML/CFT Law.
 - c) The NPO sector has not been subject to AML/CFT risk assessments, defined the nature of existing threats, identified the subset of most vulnerable NPOs, or established best practices to address vulnerabilities.
 - d) The NPO sector has not implemented a risk-based approach or developed the capabilities to do so.
 - e) The banking sector considers NPOs to be high risk, and the existing vulnerabilities may discourage NPOs from utilizing Cyprus banks

8. The role of the Ministry of Interior as competent authority is to receive NPO account information including the original funding amount or trust and yearly accounts, with no further investigations or insights gathered by the MOI.
 - a) There is no mechanism by the MOI to check for abuses of the NPO sector for the purposes of ML/TF, not even a threshold approach.
 - b) This may be mitigated by the function of auditors performing required audits of NPPOs.
9. Under the provisions of the Law on Societies and Institutions and other related matters (LSI), which sets a basis for a risk-based approach, the Ministry of Interior manages and updates an NPO registry.
 - a) The NPO registry is envisioned to eventually align with the broader UBO registry, the Beneficial Ownership Registers Interconnection System (BORIS), being developed under the Department of the Registrar of Companies and Official Receiver (DRCOR).
10. The Ministry of Interior as the competent authority for the NPO sector has stated that it intends to develop and implement targeted AML/CFT measures to address the existing vulnerabilities identified in the Moneyval report. The Ministry of Interior has hired external consultants to perform a risk assessment on NPOs, evaluate the riskiness of the sector, and develop a risk based supervisory framework (RBSF). The consultants are tasked with identifying vulnerable NPOs and the threats they are subject to.
11. The consulting project is expected to identify measures for the Ministry of Interior to begin identifying source of funds and conducting due diligence.

Immediate Outcome 11

1. As with TF, Cyprus's status as an IFC and geographic proximity to conflict zones heightens its risk of PF.
2. Most PF risk mitigation measures in place are common to TF, including both EU supranational and domestic tools, and domestic communication methods to notify authorities and obliged entities of new designations. There are, however, few measures specific to PF (with the exception of the banking sector).
 - a) The TF Convention, incorporated into the 2001 Cyprus Law to Ratify the International Convention for the Suppression of the Financing of Terrorism, provides a definition of funds that is broad enough to cover VA as a form of asset for PF purposes.
 - b) VASPs as obliged entities under AML/CFT Bill would be required to comply with existing obligations.
3. There have been no PF cases detected and thus no measures implemented.
4. Authorities demonstrate an understanding of the differences between PF and TF, but obliged entities in general have been found not to demonstrate a similar level of understanding, have not been adequately trained on PF, and have not received substantial communications on PF from authorities.

5. Cyprus has no PF risk mitigating measures in place targeting the VA/VASP sector, either for the use of VA as funds for PF, or the use of VASPs for such activities. This heightens existing vulnerabilities for the VA/VASP sector in addition to the existing vulnerabilities.
6. Decisions on updated designations for lists announced after Nicosia business hours on a Friday may not be communicated by supervisors until the next Business Day. Because VA markets, unlike traditional financial markets, are active constantly and outside of business hours, and transactions and movements of assets occur 24/7/365 unlike traditional movements of fiat currency, this could be a meaningful gap with regard to VASPs. Although VASPs as obliged entities should also subscribe directly to databases that also provide these updates independent of the supervisory notification channel, thus mitigating the risk of this gap, a potential gap remains.

Recommended Actions:

Immediate Outcome 9

1. Supervisory authorities should adopt targeted measures to investigate and address TF risks arising from VA and the VASP sector.
 - a) The Cybercrime Sub-Directorate of the Police and other anti TF units should adopt procedures for real time use of information for VA, given the ease and speed of transferring VA funds across wallets.
2. Outreach should be increased to the VA/VASP sector, FIs, and NPOs, in order to enhance and improve their understanding of TF risks, including risks relating to the use of VA, and ensure they are capable of meeting their obligations given their role as first line of defense against TF.
3. The non-conviction-based forfeiture (NCBF) regime, which has legal basis to include VA as a category of property as per the amended AML/CFT Law that defines property according to the 2019 FATF guidelines that include VA, can enhance the tools available for authorities to freeze and confiscate criminal property as VA. Under current law, it is the view of MOKAS that the provisions of the AML/CFT Law regarding domestic court orders for non-conviction based forfeiture (confiscation) can be applied only in very limited circumstances and under very strict specific conditions that make it unlikely that the current Cyprus NCBF regime would be highly effective with regard to VA, unless the legal requirements for NCBF are adjusted in the future. Cyprus should consider broadening the statutory conditions for its use of the NCBF regime, leveraging its availability and its applicability for TF cases involving the VA/VASP sector.

Immediate Outcome 10

Targeted Financial Sanctions

1. In order to ensure VASPs as obliged entities under the AML/CFT Bill are adequately notified of designations, obligations and measures communicated to all obliged entities, CySEC as supervisor should add VASPs in the VASP registry to its automated

notification lists. CySEC should also require registered VASPs to subscribe to EU and/or other appropriate databases of sanctioned persons and entities.

2. Cyprus should adopt TFS measures specific to VA and VASPs, and train supervisory authorities accordingly. The Cyprus Police and other CTF authorities should have direct and immediate access to commercial VA database and tracing tools.
3. CySEC should expressly require suitable procedures for TF screening, freezing, and confiscation of assets as part of the application requirements and ongoing conditions for the VASP registry. CySEC should also monitor practical readiness and compliance, as well as provide guidance to enhance readiness and compliance.
4. Practices for supervisory communication of TF designations, obligations and measures should ensure that there are not gaps over weekend or holiday periods between when MFA is notified and when VASPs are notified through supervisory channel.

Non-profit organizations

5. The Ministry of Interior should widen the scope of its current consulting project to include consideration of VA/VASP ML/TF risks in its risk assessment and for potential inclusion in the risk-based supervisory framework.
 - a) The NPO risk assessment should identify specific ML/TF risks arising from VA/VASP activities and develop a targeted approach tailored to these risks (e.g. risk rating, due diligence and source of funds investigations with specific technologies to trace VA activity). This could entail prioritizing VA/VASP risks in its RBSF methodology, and including NPOs that accept or pay out in VA, and NPOs that accept funds from VASPs, in the “high risk” category.
 - b) Resources should be allocated for any necessary human and technical resources to carry out a risk assessment considering the impact of VA/VASP activities on the NPO sector.
 - c) MOI should ensure training of its staff at the Ministry of Interior to adequately detect, monitor and mitigate risks arising from VA/VASP activities in relation to the NPO sector.
6. The Ministry of Interior should consider establishing targeted VA/VASP-related measures for the NPO sector, particularly heightened measures for the subset of NPOs identified as most vulnerable to abuse with regard to VA/VASP activities (e.g. frequency of monitoring and reviews of NPOs, information gathering, sustained outreach, remedial measures including sanctions).
7. To mitigate risks from VA/VASP ML/TF activity in the NPO sector, the Ministry of Interior should consider taking actions to encourage NPOs to conduct transactions utilizing formal traditional financial channels through entities supervised by CBC, particularly Cyprus banks, and promote steps by NPOs to meet banks’ risk standards. Although VA activity in Cyprus is not widespread at the time of the assessment, the country’s geographic proximity to conflict zones is a factor that heightens the risks.
8. Resources, both from NPOs and the MOI, should be allocated to enhance NPOs’ understanding of their ML/TF vulnerabilities with respect to VA/VASP activities and risk mitigation measures.

Immediate Outcome 11

1. Upon the enactment of the VA/VASP framework, authorities should apply measures specific to the VA/VASP sector, both for the use of VA as funds for PF, or the use of VASPs for such activities. This would require specialized training.
 - a) The added vulnerability posed by the lack of PF-focused measures, which could be magnified in cases involving the use of VA in PF, may be mitigated by use of offsite supervisory tools to monitor compliance, such as commercial VA trading and database software tools. The use of such tools by CySEC in supervising VASPs is recommended, as well as the Cyprus Police and other relevant authorities.
2. In order to ensure VASPs as obliged entities under the AML/CFT Bill are adequately notified of designations, obligations and measures communicated to all obliged entities, CySEC as supervisor should add VASPs in the VASP registry to its automated notification lists related to PF. CySEC should also require registered VASPs to subscribe to EU and/or other appropriate databases of sanctioned persons and entities.
 - a) As obliged entities under the AML/CFT Bill, VASPs should be required to immediately notify their supervisors of any freezing measures applied and report attempted transactions.
 - b) CySEC should ensure procedures are in place to ensure communications to supervised VASPs are made without delay, particularly updates on designations, given the nature of VA markets that run consistently and outside of business hours. CySEC should also ensure it receives communications from the MFA without delay.
3. CySEC should expressly require suitable procedures for PF screening, freezing, and confiscation of assets as part of the application requirements and ongoing conditions for the VASP registry. CySEC should also monitor practical readiness and compliance, as well as provide guidance to enhance readiness and compliance.
4. Practices for supervisory communication of PF designations, obligations and measures should ensure that there are not gaps over weekend or holiday periods between when MFA is notified and when VASPs are notified through supervisory channel.

4.2 Immediate Outcome 9 (FT Investigation and Prosecution)

4.2.1 Prosecution/conviction of types of FT activity consistent with the country's risk-profile

247. Moneyval noted that the TF risk in Cyprus, which mostly consists in international TF activities, is heightened due to its proximity to conflict zones and its status as an international financial center. Yet there have been a low number of TF incidents occur in the country, with no prosecutions, few investigations, a negligible number of STRs filed, and no incoming MLA concerning terrorism or TF. Moneyval found no persons identified in EU/UN designated lists to

have assets in Cyprus or to have attempted transactions through the Cyprus system. There has, been one conviction in 2015 for supporting a terror group in return for payment and for ML on the part of an individual.

248. The TF Convention, which is incorporated into domestic Cyprus law by means of the Law to Ratify the International Convention for the Suppression of the Financing of Terrorism 2001 (Law No.29) (“the Ratification Law”), defines “funds” as assets of every kind which can be “however acquired,” whether through legitimate or illegitimate sources. This definition is broad enough to cover VA as a form of asset in connection with TF under Cyprus law. Cyprus authorities did not report any prosecutions or convictions of TF where VA activity was involved or suspected. There have, however, been TF campaigns to raise funds in VA for organizations located in conflict zones geographically close to Cyprus, such as ISIS in Syria. While these campaigns have targeted the international community in general, they have not targeted Cyprus in particular, and there have also been no incidents with ties to such activity reported to the assessment team to have been found to occur in Cyprus.

4.2.2 FT identification and investigation

249. Moneyval noted that general TF investigations customarily take place in Cyprus under established procedures albeit limited resources, noting seven such investigations during its review period. In addition, Moneyval noted that Cyprus has taken widespread actions to improve capabilities for identification and investigation by means of awareness campaigns on TF risks and FATF recommendations, including a conference to reporting entities and training seminars to public and private sector entities. The Cyprus security service, which sits on the Fusion Centre for CTF and collaborates with competent authorities, monitors potential terrorists.

250. The assessors understand the Cyprus police to have taken significant measures toward identification and investigation, which would also provide effective measures to address any cases involving VA. In addition to Moneyval’s observation of 2 EUROPOL officers seconded to the Cyprus police to train and develop expertise to identify and present terrorism threats, the assessors understand the Police to have established significant expertise within the Counter Terrorism Office (CTO) within its Crime Combating Department of the Police. The CTO is dedicated to coordinating actions in accordance with international obligations. Its main task is to receive, analyze, and assess TF related data, as defined by its mission to prevent and combat terrorism under the Police Standing Order 3/39. It maintains a national database on terrorist attacks, organizations, and individuals, and also delivers trainings and seminars. For cases involving a financial element, TF investigators collaborates with the Economic Crime Investigation Office of the Police, which specializes in financial crime. The assessors understand the CTO to have a sophisticated understanding and ability to support TF investigations and provide expertise for other divisions and entities to perform operations and investigations. The CTO may provide information and intelligence to other entities for criminal investigations involving terrorism and TF, including local investigations, and has efficient tools with respect to international cooperation.

251. Nevertheless, despite these extensive measures with respect to overall CTF, the assessors note that there are no targeted capabilities to address VA-specific TF investigations among most supervisory entities, and very limited use of VA specific tracing software. This could represent a gap particularly if there are limited resources for identification and investigation of VA aspects of TF. The assessors observed that the FIU has had little training or experience to deal with TF investigations involving VA. Neither does the Customs Department have VA-specific training or experience for conducting investigations. Its statutory authority is understood to cover checks over physical property or cash currency and does not cover VA inspections or declarations of VA. There has been no training on inspecting VA hardware, such as wallets or related physical devices that may indicate VA ownership.
252. The assessment team found that the Police's cybercrime Sub-Directorate has developed capabilities and has had some experience investigating hardware for VA. The team has collaborated with and attended workshops from Europol and other international agencies, covering matters like the dark web to identify cases involving VA. With respect to VA tracing software, the cybercrime unit of the Cyprus police relies primarily on Europol's use of commercial VA-specific tracing software and intelligence tools for investigations. They also expect Europol to develop additional targeted VA tracing tools which would be made available for its members at some future time, but any such tool is still in development with no known availability date. This lack of direct and immediate access to commercial VA tracing and risk intelligence tools could hinder TF investigations with a VA component, or conversely inhibit investigations of VA activity that could lead to detection of TF activity.
253. Moneyval also identified sectors of the Cyprus economy that are particularly vulnerable to TF risks, noting that Cyprus began to take specific measures to address these vulnerabilities. NPOs were deemed particularly vulnerable to TF risks, with NPOs having the potential to be used for TF campaigns. With respect to NPOs, measures have been taken to increase outreach and amend NPO legislation, requiring all entities to register and submit audited financial statements. However, the assessment team found substantial weaknesses and vulnerabilities with respect to NPOs that could be exploited with regard to TF for VA and VA activities, as discussed in greater detail under IO.10.

4.2.3 FT investigation integrated with -and supportive of- national strategies

254. National strategies for the purpose of counterterrorism are understood by the assessment team not to specifically address VA/VASP TF risks. Therefore, the assessment team was unable to make any direct finding regarding this core issue.
255. Moneyval noted that the 2019 National AML/CFT Strategy sets measures to enhance CFT measures such as specialized training, broadening data collection, and promoting outreach to vulnerable sectors such as NPOs. Moneyval also noted that the National Counterterrorism Strategy adopted in 2014 by Council of Ministers sets a four pillar approach to Prevent, Protect, Pursue, and Respond. Also at a strategic CFT level, with respect to the police, the assessors

found that the police's strategic plan for 2019-2021, which was approved by the Ministry of Justice and Public Order as its supervisory authority and also by the Ministry of Finance, includes fighting terrorism and radicalization as the second of its five main strategic targets.

256. The Cyprus national AML/CFT strategy and the Advisory Authority's AML/CFT Action Plan do not expressly address TF risks arising from VA activities or VASP sector, nor do the five main strategic targets of the Police. There is no suggestion that this omission has impeded application of existing national policies for TF risks to VA/VASP TF risks, so there is no question of any finding of deficiency. Future updates of both the National Strategy and the Action Plan should address these VA/VASP TF risks explicitly where and to the extent warranted.

4.2.4 Effectiveness, proportionality and dissuasiveness of sanctions

257. Moneyval noted that there had been no TF convictions, and therefore no sanctions implemented. However, those sanctions applied for the single conviction case involving terrorism were deemed to be effective, proportionate, and dissuasive. The assessors did not learn of any subsequent sanctions involving VA/VASP TF activity, or failure to impose sanctions, and make no findings with respect to this core issue.

4.2.5 Alternative measures used where FT conviction is not possible (e.g. disruption)

258. Moneyval noted a number of alternative measures aside from conviction applied for TF incidents. In the single conviction case for participation in organized crime, which in practice included involvement in a terrorist group that at the time was not yet proscribed in EU listings, alternative criminal justice measures implemented were deemed to disrupt terrorist activity and led to an effective prosecution. Moneyval also noted that there had been no incoming or outgoing MLA regarding TF, but there have been cases of cooperation across FIUs for TF matters, especially across EGMONT jurisdictions. There was also some degree of LEA cooperation through EUROPOL. However, no examples were provided on the outcomes of these measures, such as cases leading to TF investigations or prosecutions. Aside from criminal justice, authorities did demonstrate a swift response and effective application of sanctions with respect to the TF suspicious activities discovered within the Cyprus bank FMBE, whereby the CBC revoked its license and corresponding banking relationships were blocked.

259. The assessors consider these measures to demonstrate that Cyprus has made use of tools that would also be effective in responding to terrorism cases involving VA, and thus has the ability to implement such measures for VA cases moving forward. Especially given the dedicated office for MLA handling and further harvesting of TF data for investigations, it is likely that MLA may also arise as a common method for responding to cases, including cases involving VA.

260. The assessment team also confirmed that the AML/CFT Bill includes VA as a category of property. As amended in 2020, the AML/CFT Law broadens the definition of property to align with the 2019 FATF Guidelines which include VA. This provides a legal basis to apply both

criminal and non-conviction-based forfeiture (NCBF) provisions to VA as eligible assets. Cyprus also enacted legislation to register NCBF orders made in other jurisdictions. The assessors consider that the NCBF regime in particular enhances the tools available to law enforcement authorities for freezing and confiscating criminal property as VA, especially as it surpasses the minimum requirements established by FATF. Thus, where there are VA assets in Cyprus, it may be practical to use NCBF powers to disrupt terrorist activity.

261. Moneyval also observed that the NCBF regime has been underutilised, partially due to practical restrictions. The NCBF regime applies only when the defendant is outside the jurisdiction or is no longer alive. The prosecutor must also present evidence and establish a prima facie case that the suspect committed the offense, as well as demonstrating reasonable efforts to locate the suspect. Therefore Moneyval found the NCBF regime to be useful only partially and recommended that Cyprus consider amending it. The assessors concur with this recommendation, considering that broadening the applicability of cases under the NCBF regime would be helpful tool for responding to TF cases involving VA. Under current law, however, it is the view of MOKAS that the provisions of the AML/CFT Law regarding domestic court orders for non-conviction based forfeiture (confiscation) can be applied only in very limited circumstances and under very strict specific conditions that make it unlikely that the Cyprus NCBF regime would be highly effective with regard to VA. Therefore, as far as freezing and confiscation of VA is concerned, it is most likely that under current law this should be made on the freezing and confiscation Court orders obtained under the provisions of the AML/CFT Law and not on NCBF Confiscation Orders, unless the legal requirements for NCBF are adjusted in the future.

4.3 Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions)

4.3.1 Implementation of targeted financial sanctions for TF without delay

262. Moneyval observed Cyprus has a framework with a series of mechanisms at its disposal, both at an EU supranational and a national level, to implement targeted financial sanctions (TFS) without delay. The UNSCRs are integrated into EU law, and as such into national legislation of Cyprus as an EU Member State, as well as through domestic legislation Cyprus has enacted. The MFA coordinates with the UN and EU sanctions regimes and provides updates on sanctions imposed on jurisdictions, natural/legal persons, or vessels on its website. Cyprus also was found to have effective domestic communication systems that notify competent authorities and obliged entities of new designations and also any freezing measures applied under the TFS regime.

263. As VASPs will be obliged entities under the AML/CFT Bill, it can reasonably be expected that the designations, obligations and measures communicated to obliged entities would also be effectively communicated to VASPs. To ensure this, CySEC, as supervisor of VASPs designated under the VASP registry, can easily ensure that it adds VASPs to its automated notification lists.

264. Moneyval found shortcomings with respect to screening practices of certain obliged entities. This finding highlights the importance for CySEC as VASP supervisor to monitor practices and protocols as well as written policies of registered VASPs. Although large ASPs and banks were found to effectively screen customers and BOs upon onboarding and through ongoing monitoring, other FIs and DNFBPs were deemed to have less comprehensive TFS controls despite their awareness of screening obligations. It is recommended that CySEC expressly require suitable procedures for TF screening as part of the application and ongoing conditions for the VASP registry, and that CySEC as supervisor continue to monitor practical compliance with registration operating conditions as well as provide guidance to enhance readiness and compliance. These requirements could also include requirements that registered VASPs subscribe to EU and/or other appropriate databases of sanctioned persons and entities.

4.3.2 Targeted approach, outreach and oversight of at-risk non-profit organisations

265. NPOs in Cyprus do not fall under the definition of obliged entities according to Article 2A of the Cyprus AML/CFT Law. NPOs are, nevertheless, subject to a registration procedure that requires them to submit their accounts to the Ministry of Interior, including the original amount or trust that funded the institution and yearly accounts. The role of the Ministry of Interior has been solely to receive the information, with no requirement to perform an in-depth analysis. Thus, both Moneyval and the 2018 Cyprus NRA have noted vulnerabilities in this sector.

266. Moneyval in particular raised extensive deficiencies in the Cyprus framework for NPOs, given that Cyprus had not identified the subset of NPOs most vulnerable to TF risks, or defined the nature of the threats posed by these TF risks. Neither had the sector been subject to risk assessments in this matter, and there were no best practices established to address TF vulnerabilities. Therefore, Moneyval concluded that Cyprus had not developed the capability to apply a risk-based approach to the NPO sector.

267. This absence of a targeted approach may in turn discourage or disrupt legitimate NPO activities. For instance, Moneyval observed that the Cyprus banking sector has been reluctant to serve NPOs, considering them to be a high-risk category. Some smaller banks refuse to do business with NPOs altogether. In this context, Moneyval faulted the methodology of the 2018 Cyprus NRA's assessment of NPOs, because it was largely based on international typologies rather than Cyprus-specific factors, and did not accept the NRA's finding considering the sector to be medium-low risk.

268. While Moneyval did recognize that some measures had been taken to reduce vulnerabilities for NPOs, another deficiency was that none of these measures was deemed to be based on a thorough understanding of the ML/TF risks faced by NPOs, and no aspect of oversight focused on ensuring NPOs would not be abused for ML/TF purposes. Cyprus authorities had begun to strengthen the oversight framework for NPOs, with the 2017 Law on Societies and Institutions and other related matters (LSI) setting the foundation for the development of a risk-based approach. This legislation also established measures envisioned in FATF's Rec. 8 (e.g. registration requirements, publicly available information, etc.) and set

provisions for the development of an NPO register. This register would be managed jointly by the General Registrar, who is the Permanent Secretary of the Ministry of Interior, and the District Officers/Registrars, who as of the time of enactment of the LSI were expected to collaborate to populate it in 2019 and update it on a regular basis.

269. The assessors for this report found that in response to the vulnerabilities exposed by Moneyval regarding the NPO sector, the Ministry of Interior has taken steps toward establishing risk mitigating measures. While it is outside the scope of this assessment to assess these measures broadly, with respect to the register, the Ministry of Interior as the competent authority has maintained the records of approximately 2,000 Cyprus NPOs including societies, institutions, federations, and associations. These records hold data on NPOs' scope, address, Board of Directors, and economic figures. The official gazette of the ministry also publishes the name, address, scope of these registered NPOs, and the name of the head of the Board of Directors. By the second half of 2021, the Ministry of Interior also intends to align its database with the Beneficial Ownership Registers Interconnection System (BORIS) implementation currently being built under the Department of the Registrar of Companies and Official Receiver (DRCOR).
270. The assessors learned that the Ministry of Interior is also working with external consultants to perform a risk assessment on NPOs. The consultants for that project are tasked with evaluating the riskiness of the entire NPO sector and developing a risk based supervisory framework (RBSF), with quantitative and qualitative risk measures and a risk scoring mechanism. The NPO consultants' review is expected to establish measures to identify source of funds and conduct adequate due diligence. Ultimately this process would identify vulnerable NPOs, the threats they are subject to, and tailor the RBSF risk mitigation methodology accordingly. These measures are expected by the MOI to assist it to begin taking action and gathering insights based on the data collected on NPOs.
271. The assessors met with the NPO unit of the Ministry of Interior and discussed the progress of this consulting project, which at this time is yet to be completed. The Ministry of Interior has received initial deliverables, including a project methodology and hands-on analysis of the NPO risks, and with final recommendations yet to be performed.
272. Based on a review of the available materials provided, including the initial deliverables, it did not appear to the assessors that this consulting project has been tasked to consider VA risks pertaining to the NPO sector. The assessors offered to meet with the NPO consultants to identify these VA concerns and were not taken up on this offer, and so were unable to discuss the matter directly with these consultants. Hence their concern persists that while the scope of the consulting project is important, it has a potential blind spot with respect to VA/VASPs.
273. The assessment team found evidence that actions have begun to be taken to evaluate NPO sector vulnerabilities, adopt a risk-based supervision framework for NPOs and adopt risk mitigating measures to address NPOs' existing vulnerabilities. However, the assessment team found that these measures do not appear to have taken into account to any observable degree

the risks of VA or the VA/VASP sector or to incorporate ML/TF VA/VASP activity risks into any such RBSF.

274. Because the approach that intends to provide solutions for the NPO sector in terms of AML/CFT is not considering the role of VA, it appears necessary to modify the scope of the consulting project to include such VA considerations. Broadening the scope accordingly would ensure the project covers areas where existing NPO vulnerabilities can be exploited with VA activities, which may be more likely to arise with the enactment of the AML/CFT Law providing for supervised VA and VASP activities in Cyprus.
275. Among other risks that the NPO sector may be exposing Cyprus to, the assessors made observations with respect to ML/TF in relation to VA/VASP activities. The assessors noted that if the Ministry of Interior has not yet established procedures including source of funds investigations for fiat currencies, they would not have done so for VA either. While the assessors were informed that NPOs are individually audited, they consider that a lack of guidance and checks may not prevent compromised audits from taking place. The overall vulnerabilities of the NPO sector are relevant for VA to the extent that donations in the form of illicitly obtained VA could fund NPOs, or “sham” NPOs could be set up to support terrorist organizations and receive funding in VA.
276. With respect to ML, the assessors note that limited regulations with respect to NPO governance increase the risks of illicit funds entering the system through NPOs. In the absence of source of funds investigations, illicitly obtained VA could be commingled with legitimate funds and reported as charitable receipts, either with or without awareness on the part of NPO managers themselves. With respect to TF, the fact that Cyprus is geographically close to conflict zones increases its vulnerability to risks, and the assessors are familiar with cases of TF in such zones that have launched fundraising campaigns specifically in VA (although these did not specifically target Cyprus).
277. The assessors also observed that even though there have been very few reported instances of suspicious activity in the Cyprus NPO sector, which is likely the reason behind the NRA’s evaluation of its risk level as medium-low, there is no mechanism to check for abuses. For instance, Moneyval noted that there had been only one STR related to TF in the NPO sector and no investigations of TF involving NPOs. The assessors did not learn of any VA activities that had been observed in the NPO sector or reported as suspicious as of the time of the assessment.
278. Ultimately, the assessors found that there may be few to no significant barriers for criminals or terrorists to exploit the existing NPO vulnerabilities by means of VA activities. These factors represent a significant vulnerability if left unattended, not only for overall ML/TF risks but specifically for those posed by VA/VASP activities.

4.3.3 Deprivation of TF assets and Instrumentalities

279. Moneyval found, and the assessors concur, that obliged entities demonstrate awareness of their obligation to establish protocols for freezing assets without delay as a component of TFS implementation. While they demonstrated the capabilities to do so through other measures implemented, obliged entities generally had not had occasion to execute these protocols for the purposes of deprivation of TF assets and instrumentalities. There had been no sanction hits, criminal freezing of assets, or confiscation orders in relation to terrorist activities (e.g. individuals, organizations, or financing) in Cyprus. The assessment team did not receive reports of any such predicates of terrorist activity using VA through any Cyprus obliged entity that would have necessitated their initiation of freezing or confiscation of assets in the form of VA.
280. It is recommended that CySEC expressly require suitable protocols for TF freezing and confiscation of assets as part of the application requirements and ongoing conditions for the VASP registry, and that CySEC as supervisor monitor practical readiness and compliance, as well as provide guidance to enhance readiness and compliance.
281. Although investigative measures are being enhanced with the new Police Office for Handling Mutual Legal Assistance Requests and European Investigation Orders within the Crime Combating Department to focus on MLA requests, and initiatives to harvest additional TF investigations, which may improve capabilities to identify, freeze, and confiscate assets, there are still no targeted measures, implemented or envisioned, for cases involving VA for TF. There have been widely reported instances (outside of Cyprus but arising from conflict zones such as Syria) of TF campaigns in VA targeting international communities of supporters. The specific characteristics of VA infrastructures may require tailored methods to adequately trace, identify, freeze, and confiscate VA, and Cyprus Police have limited direct or immediate access to VA tracing tools, particularly commercial tools and databases, for which they rely principally on Europol's access and subscriptions. It is recommended that Cyprus Police have direct and immediate access to commercial VA database and tracing tools.

4.3.4 Consistency of measures with overall TF risk profile

282. The 2018 Cyprus NRA considered the country's TF risk to be medium, largely due to its status as an IFC and identified ASPs as the second most material sector. The Moneyval report questioned whether the ASP sector had a uniformly adequate capability in TF to identify individuals and entities attempting to conceal their identities through complex structures. This was found to constitute a TF vulnerability. This ASP sector could accordingly pose risk for cases of TF involving the use of VA/VASP means.
283. Regarding the NPO sector, identified by Moneyval as particularly vulnerable to TF, Moneyval found a lack of comprehensive understanding of the sector's specific TF risks, and also a lack of measures in place to identify or respond to these risks. Moneyval noted a new legal/regulatory framework for NPOs and initiatives toward a risk-based approach, and the

assessors were also informed of, and reviewed the scope and current status of, a consulting project that would identify NPO risks including those in relation to TF, and propose risk mitigation measures. There is no consideration of VA risks, including VA TF risks, in the current scope of the consulting project. This constitutes a shortcoming, where a sector recognized as vulnerable to TF is likely to have gaps in understanding, identifying, and mitigating TF risks involving VA due to its failure to consider VA TF risks. It is recommended that the scope of review of the NPO sector be expanded to include VA TF risks arising from the NPO sector.

284. The assessors consider Cyprus's geographic proximity to conflict zones may also constitute a vulnerability for cases involving VA/VASPs. There have been widely reported instances (outside of Cyprus but arising from conflict zones such as Syria) of TF campaigns in VA targeting international communities of supporters. Currently Cyprus has no measures in place reported to the assessment team to identify or understand the VA TF risks posed by these types of campaigns in Cyprus.

4.4 Immediate Outcome 11 (PF financial sanctions)

285. As in the case of TF, Moneyval notes that Cyprus's status as an IFC and its geographic proximity to conflict zones accentuate its risk of PF. Most of the measures in place are common to existing frameworks for TF, such that existing vulnerabilities also carry over to PF compliance. An added vulnerability would be any lack of PF-specific understanding among obliged entities or supervisors. Moneyval found that obliged entities demonstrate shortcomings in their ability to distinguish PF from TF in their risk identification and mitigation measures.

286. As VA was out of scope for Moneyval, and there was not yet a registration framework for VASPs in Cyprus, Moneyval made no findings with regard to PF risks of VA or VASPs.

4.4.1 Implementation of targeted financial sanctions related to proliferation financing without delay

287. Moneyval noted that under the TFS regime, Cyprus relies on both EU supranational and domestic mechanisms to apply TFS for cases of proliferation financing without delay. The UNSCRs are incorporated into EU law through the Decisions and Regulations of the EU Council, and thus incorporated into Cyprus national legislation as an EU member state, as well as through domestic legislation. Cyprus also was found to have effective domestic communication systems that notify authorities and obliged entities of new designations. Supervisors maintain contact lists with which they promptly notify obliged entities of such updates to lists, and also post such notices on their websites.

288. FIs and DNFBPs are required to immediately notify their respective supervisors of any freezing measures applied and report attempted transactions. Under the AML/CFT Bill, as obliged entities VASPs will likewise be required to immediately notify their supervisors of any freezing measures applied and report attempted transactions.

289. As VASPs will be obliged entities under the AML/CFT Bill, it can reasonably be expected that the designations, obligations and measures communicated to obliged entities would also be effectively communicated to VASPs. To ensure this, CySEC, as supervisor of VASPs designated under the VASP registry, can simply ensure that it adds VASPs to its automated notification lists for issues related to PF. Moneyval documented a concern that decisions announced after Nicosia business hours on a Friday may not be communicated by supervisors until the next Business Day. Because VA markets, unlike traditional financial markets, are active throughout evenings, weekends and holidays on a 24/7/365 basis, this could be a meaningful gap with regard to VASPs. While risks from this gap are mitigated because VASPs will be expected to receive updates directly from PF sanctions databases they subscribe to, the supervisory channel of communication is an additional line of defense. Accordingly, CySEC as VASP supervisor should ensure procedures are in place to ensure communications to supervised entities are made without delay – and that CySEC itself receives communications from MFA without delay.
290. Despite the existence of mechanisms to implement TFS for cases of PF, the assessors were not made aware of any incidents related to PF, and thus any occasion for obliged entities to implement measures from the TFS regime. There has not yet been training to supervisory authorities or obliged entities on the specific risks posed by VA in relation to PF. This may represent a shortcoming given the particular dynamics of VA/VASPs in terms of fund movements and traceability. Thus, it is recommended that CySEC expressly require suitable procedures to combat PF as part of the application and ongoing conditions for the VASP registry, continue to monitor practical compliance, and provide guidance to enhance readiness and compliance. These requirements should also include express requirements that registered VASPs subscribe to EU and/or other appropriate databases of PF sanctioned persons and entities.

4.4.2 Identification of assets and funds held by designated persons/entities and prohibitions

291. Moneyval noted that Cyprus relies on a number of tools to be able to identify assets and funds held by designated persons and entities, as well as prohibitions. On a national level, the National Committee for the Implementation of the Convention on the Prohibition of Chemical Weapons and the Committee on Export Control of the Ministry of Trade and Industry coordinate efforts against the proliferation of weapons of mass destruction and some elements of PF. The Coordinating Unit to Combat International Terrorism collaborates with relevant ministries and departments for these purposes as well. Cyprus also has two other bodies that focus on PF-related TFS. Moneyval also noted initiatives to increase awareness of the risks of circumvention of sanctions, and that there had been one investigation of suspected PF relating to possible violations of the UN and EU Sanctions in relation to DPRK.
292. The Customs Department has the power to perform physical checks on exports of sensitive goods, ensuring they are adequately licensed by the Ministry of Energy, Commerce, Industry and Tourism, which licenses exports for dual use goods and military equipment.

However, there has been no consideration identified by the assessment team of the role of VA/VASPs or VA hardware for cases of PF. Neither does the Customs Department have VA-specific training or experience for conducting investigations. Its statutory authority is understood to cover checks over physical property or cash currency and does not cover VA inspections or declarations of VA. There has been no training on inspecting VA hardware, such as wallets or related physical devices that may indicate VA ownership, to mitigate PF risks of VA/VASP.

293. The new Police Office for Handling Mutual Legal Assistance Requests and European Investigation Orders within the Crime Combating Department to focus on MLA requests and European Investigation Orders, and initiatives to harvest additional TF investigations, may improve capabilities to identify assets linked to PF, and eventually freeze and confiscate them as necessary. However, the specific characteristics of VA infrastructures may require tailored methods to adequately trace, identify, freeze, and confiscate VA, and Cyprus Police have limited direct or immediate access to VA tracing tools, particularly commercial tools and databases, for which they rely principally on Europol's access and subscriptions. It is recommended that Cyprus Police have direct and immediate access to commercial VA database and tracing tools.
294. Obligated entities were found by Moneyval to be aware of the need to establish protocols to freeze assets related to PF TFS, and Moneyval also reported that there have been incidents where obliged entities have closed or refused to open client accounts due to suspicions of links to proliferators including DPRK. As obliged entities under the AML/CFT Bill, VASPs would also need to establish such protocols for freezing and screening in regard to PF. While VASPs will already have this obligation, to promote clarity CySEC as supervisor of VASPs should add this to the conditions for registration onto the VASP registry, in order to ensure their ability to take effective steps to identify PF in relation to jurisdictions and persons.

4.4.3 FIs, DNFBPs and VASPs understanding of and compliance with obligations

295. Moneyval noted that FIs and DNFBPs demonstrate an adequate level of understanding regarding their obligations with respect to PF sanctions, to the extent that they are the same as TF sanctions for countries of proliferation concern as for individuals/institutions of terrorism. However, internal procedures have shown a lack of detailed controls to identify TFS measures unique to PF, with the exception of a refusal to serve persons involved in weapons trade. A general lack of differentiation between TF and PF among obliged entities may limit compliance in factors that are unique to PF, such as cases where there may be no geographic link. Obligated entities would be less effective identifying and responding to PF transactions and clients that are not clearly linked to sanctioned countries. Apart from the CBC, which organized PF-specific trainings, other supervisory authorities were found to have performed limited awareness raising measures on PF issues.
296. With respect to the use of VA for matters unique to PF, the assessors conclude that there is a corresponding risk that without clearly targeted registration and operational

requirements VASPs' understanding would also be very limited. Compliance with any targeted requirements that may result from the enactment of the VA/VASP framework, for instance, through either registration and/or operating conditions to registration imposed by CySEC, or secondary legislation from CySEC, would require specialized training and monitoring by supervisors to ensure implementation.

297. In order to mitigate this potential shortcoming in understanding and compliance regarding PF-specific obligations for VASPs, the assessors consider that upon enactment of the AML/CFT Bill, measures should be taken by CySEC to ensure a full understanding of PF-related TFS and adequate compliance. VASPs will be obliged entities under the AML/CFT Bill and as such they would already fall under the same obligations with respect to PF sanctions as other obliged entities. CySEC, as the supervisory authority for VASPs, to promote clarity should establish requirements to ensure full understanding of PF related obligations, as part of VASP registration requirements. CySEC should also issue guidance on compliance and monitor VASPs for compliance with these obligations, applying targeted procedures for monitoring compliance with PF-specific obligations in its supervisory practices.

4.4.4 Competent authorities ensuring and monitoring compliance, by FIs, DNFBPs and VASPs

298. Moneyval found that competent authorities in general understand the distinctions between TFS for TF and PF, and attempt to articulate understandings on PF concerns. Yet supervisory practices to monitor compliance with PF related TFS were similar to those applied for TF and it was unclear whether supervisors' on-site inspections distinguished between TFS for PF and TF, as neither the inspection checklists or the statistics collected distinguish them. There were no offsite supervisory tools found to monitor compliance for TFS specific to PF, except for the CBC.

299. Moneyval found that obliged entities in Cyprus generally did not distinguish between TF and PF as different subjects for which to comply, and neither had they received communications focusing on PF as such. The fact that supervisors had found no major shortcomings among reporting entities with regard to PF related TFS was considered by Moneyval to be inconsistent with this lack of widespread understanding of PF-specific risks.

300. This lack of PF-focused measures could indicate an added vulnerability, which could be magnified in cases involving the use of VA in PF. This may be mitigated by the use of offsite supervisory tools to monitor compliance, such as commercial VA trading and database software tools, and such use by CySEC in supervising VASPs is recommended.

301. Upon the enactment of the VA/VASP framework, the assessors consider it important to for CySEC as the supervisory authority to ensure and monitor compliance regarding PF specific obligations. VASPs would be obliged entities under the AML/CFT Bill and as such by law will fall under the same requirements as other obliged entities. CySEC, to promote clarity, should nevertheless establish express requirements to ensure full compliance of PF related obligations, as part of VASP registration requirements. CySEC should also issue guidance on compliance and

monitor VASPs for compliance with these obligations, applying targeted procedures for monitoring compliance with PF-specific obligations in its supervisory practices. Moreover, VASPs should be included in supervisors' email distribution lists notifying updates on PF sanctions.

5. Preventive Measures

5.1 Key Findings and Recommended Actions

Key Findings:

1. There is very limited VA or VASP (or VASP-type) activity in Cyprus.
2. What activity exists is limited primarily to non-bank FIs supervised by CySEC²⁸ – although these are not registered as VASPs²⁹, nor do they constitute the most material sector of the Cyprus economy, the assessment team treated these (for purposes of applying risk assessment analysis) as highly material and relevant, and assigned them the highest priority from a VA/VASP perspective with regard to preventive measures.
3. VA deposits introduced from customers are regarded as highly risky, and are broadly prohibited, and where permitted are subject to EDD and rigorous preventive measures.
4. There is a general perception by FIs and DNFBPs of the VA and VASP sector as highly risky and outside their risk appetite.
5. Where VA-related activity is detected by CBC-regulated FIs, customers are instructed to cease activity, or accounts terminated, or both. There is a widespread perception that VA-related activity is banned by the CBC for CBC-supervised entities, although the assessment team found there is no actual prohibition.
6. The assessment team found a strong consistent general culture of seeking permission from regulators or other authorities prior to taking on innovative risky activities (rather than acting first and seeking forgiveness).
7. There is a broad desire on the part of FIs to receive amended directives, or at minimum guidance, from CBC and CySEC, before formulating their own policies and procedures. Areas of particular interest include best practices for accepting VA from customers, STR reporting related to VA, VA layering typologies and avoiding tipping when suspicious VA transactions are initiated from customers.
8. The banking sector acts and is widely perceived as a critical line of defense against ML/TF because of its strict controls and practices. With regard to VA, it is widely understood that banks do not accept VA or serve VA activities. Thus funds transmitted from banks or bank customers are not perceived as carrying indirect VA or VASP ML/TF risks. The

²⁸ CIFs can only transact in crypto assets (VA) if they have obtained a permission to provide such services pursuant to article 6(9)(b) of Law 144(I)/2007 [or article 5(5) of Law 87(I)/2007] and such activities are limited to no more than 15% of the total turnover of the CIF in any quarter, and the CIF complies with other conditions, as set forth in CySEC Circular No. C244 (13 October 2017). This circular was replaced in 2018 and CySEC ceased accepting new applications thereunder for VA.

²⁹ Because these entities are already licensed as traditional FIs subject to the Core Principles, there is no deficiency in their not being registered as VASPs, due to the absence of a licensing or registration scheme for VASPs. Interpretative Note to R.15 in the June 2019 FATF Guidelines expressly provides that :“A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.” The assessment team has also considered whether these entities are subject to the full range of obligations applicable to VASPs or in light of their VA activities.

assessment team found this perception reasonable and largely justified. Policies and practices of other obliged entities for interacting with banks and bank customers in the current environment with zero to low tolerance for VA may be challenged if there arises greater activity and adoption of VA in the Cyprus economy, particularly if banks and other CBC-regulated FIs were to lessen restrictions on VA and VASP sectors.

9. The sector generally has not yet formally adopted FATF 2019 updates with respect to the wire transfer rule for transfer of VA, often referred to as the “Travel Rule.” As discussed in R.15, Cyprus has not yet implemented the Travel Rule for VA, and it is not contained in the AML/CFT Bill. Thus there is no legally binding requirement applicable to obliged entities or VASPs in Cyprus. In practice the detrimental impact of the lack of adoption of the Travel Rule for VA is limited, due to the extremely limited to negligible VASP-to-VASP transmission of VA and non-existent transmission of VA involving CBC-supervised FIs.
10. Use of specialized cryptocurrency AML compliance and intelligence/blockchain forensics and transaction monitoring tools and databases is quite limited. There is very limited use of commercial (fee liable) products/services in this category, although a small number of CySEC-regulated firms engaged in VA/VASP activities do so. No CBC-regulated FI do.

Recommended Actions:

1. Firms throughout the sector should expressly adopt written policies and procedures to comply with the wire transfer rule for VA. As the highest priority, FIs already engaging in VASP-type activities (even if not technically required to register as VASPs) should do so.
2. Firms engaging in VA or VASP-type activities involving transfers of VA should monitor (and implement) industry best practices for technological and operational compliance with the Travel Rule for VA.
3. Firms engaging in VA or VASP activities should utilise specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases to monitor risks and deter and detect ML/TF, on a regular basis.
4. Firms that have policies against having customers engaged in VA or VASP activities (whom they classify as high risk) should ensure that they have procedures to confirm those policies are performing as designed. As part of these measures they should periodically utilise specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases to detect whether customers are violating policies undetected.
5. If banks and other CBC-regulated FIs were to lessen restrictions on VA and VASP sectors, policies, practices and preventive measures of obliged entities predicated on VA restrictions of CBC-regulated entities should be reevaluated.
6. Decisions on updated designations for sanctions lists announced outside business hours may not be communicated by supervisors until the next Business Day. Because VA markets, unlike traditional financial markets, are active constantly outside of business hours, and transactions and movements of assets occur 24/7/365 unlike traditional movements of fiat currency, this could be a meaningful gap with regard to VASPs and movement of VA for TF/PF purposes, which could be moved and utilized during these times. Although VASPs as obliged entities will be subscribing directly to

databases that also provide these updates independent of the supervisory notification channel, thus mitigating the risk of this gap, a potential gap remains. VASPs and other firms engaging in VA activities should ensure that they are able to implement updates outside of normal business hours, and utilizing database channels as well as supervisory notification channels.

7. To promote obliged entities' understanding and implementation of preventive measures, it is recommended that
 - a) Supervisory authorities, particularly CySEC, should provide guidance to their obliged entities and supervised firms, for VASPs and other firms engaged with VA/VASPs
 - b) Supervisory authorities, particularly CySEC, should provide guidance to their obliged entities and supervised firms.
 - c) MOKAS should update its GoAML system to add specific predefined fields relating to VA, in order to make it easier for obliged entities to report STRs on VA related issues. This would also make it easier for MOKAS and obliged entities to track metrics on VA/VASP related STR reporting.

5.2 Immediate Outcome 4 (Preventive Measures)

302. Moneyval found the most material sectors in Cyprus to be banking, ASPs, real estate, the casino and MSBs, in descending order. The assessment team considered the overall ML/TF risks of each of these sectors as identified in 2019 by Moneyval, focusing on them solely in relation to the VA and VASP sector. This approach particularly addressed how existing vulnerabilities could be exploited through the use of VA. Hence, when assessing this Immediate Outcome, these sectors were more heavily focused on.
303. As the VASP registration framework has not yet been established under the amendment to the AML/CFT Law, there have not yet been any VASPs registered as such. The assessment team also sought to identify FIs or other entities engaging in VASP-type activities, as well as any VA or VASP activity itself across these material sectors.
304. Some FIs are engaging in VA/VASP activity. The assessment team prioritised those entities and attempted to meet with any of them engaged in substantial levels of activity, based on metrics provided by CySEC, considering that if they were engaging in solely VA activities they would meet the definition of a VASP under FATF Guidelines. These entities are already subject to the full AML/CFT regime under the Cyprus AML/CFT Law as FIs and obliged entities.
305. Of secondary focus were certain key material entities whose policies were not to engage in VA/VASP activity – primarily Banks, EMI, PIs, and MVTs. The assessors considered how these entities ensure the effectiveness of their policies, what measures they take to detect VA activity, and what actions they take if they find non-compliance in the form of undetected or unauthorized VA activity by their customers or within their respective platforms. For firms whose policy is to prohibit VA activity and prohibit servicing the VA/VASP sector, a key

consideration for the assessment team was whether that policy is communicated, whether that policy is succeeding as designed, what steps the firm is taking to ensure the policy is performing as expected, and what measures are taken if breaches of the policy are detected.

306. The assessment team held meetings with obliged entities and supervised firms, focusing on identifying areas where VA/VASP activity was actually occurring, or represented a significant risk. Meetings were held with selected CySEC-supervised firms engaging in more than de minimis VASP-like activity. The assessment team also met with major banks, EMIs, PSPs, the Casino and ASPs. Meetings were also held with trade associations representing Cyprus banks and international banks operating in Cyprus, which strongly reinforced the perception that the assessment team found directly from the largest individual banks, that there was no current appetite from the banks to serve the VA/VASP sector.

307. The assessment team considered the weaknesses identified in the Moneyval report, such as ASP or casino operations, with focus on any aspect that would be material or relevant to the VA/VASP sector.

308. The assessors considered the role of introducers, given that they were extensively addressed in the Moneyval report. However, even when an introducer might be involved in these operations, the customer's onboarding and screening is performed by the obliged entity. Regardless of the role of the introducer, banks' policies with respect to not serving VASPs remain in force, such that any ML/TF risks involving VA are kept at a minimum. Moreover, subsequent to onboarding, detection of VA activities by an introduced client would be effected in the bank's transaction monitoring procedures. Thus the assessors concluded that ML/TF risks for VA activities of introducing does not represent a material independent risk, and as a result, did not focus further on introducers in connection with this risk assessment.

309. The assessors also considered segments of the insurance and betting sectors as potential areas of risk, but after meeting with the respective supervisors and reviewing the supervisory framework, they did not identify any meaningful ML/TF risks involving VA. Thus the assessors did not consider it necessary to meet with the regulated firms. With respect to insurance companies, the assessors' meetings with the Superintendent of Insurance revealed that there is no coverage for VASPs and that VAs are not accepted for payment. The overall AML risk to begin with is extremely low, and reinsurance in the non-life sector would further minimize this risk. Moreover, insurance companies are very conservative in their investment approach and among the least likely to invest in VA.

310. As for betting companies, these would require the regulator's approval in order to accept VAs, and so far none have requested this. There is no evident way to integrate VA into the ecosystem, which is limited to cash and fiat transfers from CBC regulated entities, which in turn adhere to practices not to serve the VA sector.

311. With regard to the Cyprus Investment Program, the assessment team met with the MOI and closely examined any potential risks relevant for this risk assessment, especially given the

recent news coverage on the program and the vulnerabilities that were found to exist. However, no nexus to VA or VASPs was detected. Thus the Cyprus Investment Program was not made an area of focus for the purposes of this risk assessment, and the assessment team also did not focus on the real estate sector.

5.2.1 Understanding ML/TF risks and AML/CFT obligations

312. The general understanding of ML/TF risks and AML/CFT obligations was deemed by the assessors to be strong across the sectors observed. The assessment team focused particularly on ML/TF Risks and AML/CFT obligations associated with VA and VASPs, where the overall level of understanding across entities was also found to be strong.

Banks

313. With regard to banks, the assessment team found a high general level of awareness of ML/TF risks related to VA and VASPs. This consisted primarily of perception of high risks, that existing AML/CFT obligations would mandate the application of AML/CFT measures for high risk activity accordingly, and that any specific AML/CFT obligations tailored to the VA/VASP sector that may arise are yet to be developed, pending issuance of any CBC AML/CFT Directive, Guidance or circular following enactment of the AML/CFT Bill. Banks consistently indicated VA/VASPs as being outside their risk appetite, in part out of concerns that perceptions of riskiness, or of Cyprus banks engaged in a high risk activity, could jeopardize their correspondent banking relationships with international banks outside of Cyprus. Banks showed an awareness of the element of anonymity or pseudonymity in the VA/VASP sector and the inherent risks due to this characteristic, recognizing the importance of identifying UBOs as key. There was also a consistent understanding on the part of regulated firms that the CBC would be highly concerned about the riskiness of VA and VASPs.

314. Because banks have not serviced the VA/VASP sector, there is a general recognition that they are not as familiar with the more specific characteristics unique to the VA/VASP sector, and that this is also a new issue for the regulators both at the Cyprus level and at an EU-wide level. Thus there is an expectation and appetite for guidance specific for Cyprus banks to follow in developing their own understanding of such VA/VASP-specific ML/TF risks and AML/CFT obligations.

Non-bank FIs

315. Among EMIs and PSPs, there was also a consistent understanding of ML/TF risks and AML/CFT obligations, particularly an overall classification of VA/VASPs as high risk, and understanding that that AML/CFT obligations for VA/VASP activities would mandate such treatment. The assessment team found consistent awareness that specific supervisory guidance for the VA/VASP sector in terms of risk and tailored obligations has not been provided by the CBC. Overall the assessment team found limited to no risk appetite in this sector to support VA/VASPs customers or activities, in no insignificant part due to widespread awareness

of the CBC's risk averse stance, where entities that have inquired or shown interest in the space are understood to have been heavily warned about the risks. MVTs also demonstrated a strong understanding of these risks and do not accept VAs.

316. As for securities firms supervised by CySEC - viewed by the assessment team as the highest priority for the risk assessment due to their engagement with the space -- the assessment team found a very strong and highly sophisticated understanding of ML/TF risks and AML/CFT obligations. This spanned beyond a theoretical recognition of high risk. Firms adapted existing obligations to set measures accordingly, in close collaboration with CySEC to develop tailored risk mitigation procedures.
317. The assessment team thus found a very strong understanding of ML/TF risks unique to the VA/VASP sector (e.g. layering, moneypassing, source and traceability of VA). Firms have been monitoring market surveillance and other risks, even while not necessarily required to do so at the time of the assessment, or even as an expected condition to register with the upcoming registration framework under the AML/CFT Bill. There is an advanced awareness of the challenges of identifying the source and destination of VA, and the need to apply rigorous obligations to meet these challenges.
318. Operating under the existing CySEC AML/CFT Directive (which does not specifically address VA), these firms have found ways to successfully apply procedures and controls from other businesses lines adapted for the VA/VASP sector. Nevertheless, the assessment team found that these firms would welcome an updated AML/CFT Directive and further guidance from CySEC when the new AML/CFT Bill is enacted. This guidance would help these entities standardize and streamline the interpretation and application of the already rigorous AML/CFT obligations they have established in-house.

DNFBPs

319. The Casino demonstrated strong awareness of ML/TF risks and AML/CFT obligations and even strong understanding of particular VA/VASP-specific ML/TF risks and AML/CFT obligations. This can be attributed to the measures to improve their overall AML/CFT functions since the Moneyval observations identifying this as a pressing need. The ICR's planned expansion in 2022, which aims to increase gaming operations, introduce foreign junket services, and attract foreign VIP clients, is considered likely by the Casino to increase overall ML/TF risks. Moreover, the assessors observed that the casino's engagement with the supervisor (which since the time of Moneyval's assessment has also recruited experienced supervisory staff with respect to AML) has enhanced the casino's awareness of the risks and obligations through frequent discussions and exchange of information.
320. The ICR broke ground in April 2019 and is planned to open in phases. The initial expected opening for the end of 2021 will likely be delayed due to a pause in construction operations during the COVID-19 lockdown.

321. Until the opening, the licensed operator has been operating a temporary casino in Limassol since June 2018, on a much smaller scale. The licensed operator has also opened four smaller satellite casinos in Nicosia, Limassol, Paphos, and Larnaca, the latter of which has closed. For the satellite casinos, the license permits each to have up to 50 machines.
322. Moneyval observed substantial weaknesses in the casino’s compliance functions, noting that it was operating at or beyond the limits of its AML/CTF risk management and compliance systems.
323. The casino reported having taken the following measures:
- Ramped up its team
 - Recruited an experienced Head of AML Compliance
 - Conducted AML trainings

The assessment team did not independently verify the implementation or assess the effectiveness of these reported measures.

The assessment team also observed a number of factors that it considers could potentially increase the risk of casino activities with respect to VA/VASP activities. The casino’s staff continues to be mostly new to the casino industry, and hence in need of significant training to understand AML risks and requirements for detection and reporting procedures. The casino staff are also new to operating a corporate entity in Cyprus and to the overall EU environment. Neither is there considered to be a significant existing pool of talent with direct experience in this matter in Cyprus, such that expertise is being migrated from similar industries and outside jurisdictions. The ICR is not yet operational and the casino staff has not had any experience with junkets to date, which confirms the need for continued capacity building to adequately manage risks.

324. In conjunction, there has also been an increase in reports to MOKAS by the casino, although the assessment team makes no finding as to the substance or quality of these reports.

Table 5.1: SARs/STRs reported by the casino

Year	2018	2019	2020*
Number of Reports	10	23	10

*year to date as of Nov 3, 2020, and taking into account reduced activity due to COVID.

ASPs

325. The assessment team found a general perception among ASPs that the VA/VASP sector is high risk, and that existing AML/CFT obligations would mandate its treatment as a high risk sector. ASPs are aware that supervisory guidance tailored to the VA/VASP sector is yet to be provided. The assessment team was also informed by the interviewed ASPs that there has

been no meaningful demand from the market for ASP services to clients involved in VAs or VASPs sector. Hence the assessors found no special nexus with VA or VASPs for ASP services.

326. ASPs indicated that they would welcome consistent guidance from their respective supervisors with regard to VA/VASP ML/TF risks and mitigants, so as to tailor their existing policies and practices accordingly. They expressed an interest in working with the VA/VASP sector as a potential line of business. ASPs have an existing framework to apply their current risk-based approach deploying their current understanding of ML/TF risks for high risk businesses and clients. The assessors noted the existence of specific risk assessments where clients assigned a high-risk profile were treated accordingly.

327. With regard to ASPs supervised by ICPAC, their awareness has benefitted from specific provisions relating to VA in ICPAC's 2020 AML/CFT Directive, including typologies that would indicate need for EDD or suggest potential TF activity, and from prior ICPAC circulars identifying risks of VA. ICPAC offered an online seminar to its obliged entities, presented by the Digital Forensic Lab of the Cyprus Police, covering topics of cybercrime, online fraud and cryptocurrencies. ICPAC's General Circular 23/2020 also distributed the Virtual Asset Red Flag Indicators for ML/TF published by FATF in September 2020.

328. ASPs thus were deemed by the assessors to be aware of the importance of their own adherence to adequate AML/CFT obligations.

VASPs - no VASPs licensed yet – VASPs addressed under Non-bank FIs above

329. There are no VASPs licensed as such at the time of the assessment. Those entities engaging in VASP-like activities have been found by the assessors to consist in CySEC regulated entities, which are discussed above under non-bank FIs.

5.2.2 Application of risk mitigating measures

330. While overall use of ML/TF risk mitigating measures has been found widespread in previous risk assessments, the assessment team found widespread use of VA-detecting risk mitigation techniques in customers and transaction monitoring, but very limited use of specialized VA compliance databases and tools.

331. The assessment team found widespread use of techniques such as customer monitoring and transaction monitoring with regard to VA related or VASP activity across the entities observed, in onboarding and due diligence, as well as client monitoring through reporting disclosures and existing procedures. Utilization of financial sanctions database services appeared widespread to universal across FIs, and the assessors noted that this included the CySEC regulated firms engaging in VASP activities. Moreover, the assessment team found a number of firms to take proactive measures with the addition of VASPs and VA entities to standard transaction monitoring databases. Often risk mitigating measures developed in house were found by the assessment team to be robust and rigorous.

332. In general, non-banks have a high reliance on banks as a key line of defense preventing risky payments from entering the system. As banks do not service VA or VASPs, their role as a backstop also applies to substantially remove ML/TF risks with respect to VA and VASPs from the rest of the Cyprus economy. Insurance companies and the casino, for instance, take in clients who are already customers of Cyprus banks. ASPs setting up new legal entities rely on the assurance of the rigor of banks' BO due diligence practices in their own BO due diligence and compliance practices.
333. While the reliance on banks as gatekeepers cannot be bypassed, the implications of non-compliance by any bank could trickle down throughout the system. Banks' mitigating measures benefit non-banks as well, as a back up to provide underlying reassurance for their own AML/CFT practices and overall activities. Clients of Cyprus banks are seen as having been vetted by having undergone the banks' due diligence and risk mitigation measures, as well as ongoing transaction and customer monitoring, which under current bank policies and risk appetites can be expected to mitigate any risks of bank customer ties to the VA/VASP sector.
334. Utilization of specialized VA AML compliance, intelligence and blockchain forensics tools and databases, which are designed to mitigate ML/TF risks specific to the VA/VASP sector, is quite limited. Only CySEC firms which engage in VASP-like activities have either adopted or considered adopting these tools to some extent. For those firms engaging in VA/VASP activities, these tools should be required for use on a regular basis, both for onboarding and due diligence and transactions monitoring and other ongoing AML/CFT procedures.
335. Among those entities whose policies state not to serve the VA/VASP sector, the assessors found these VA-specific tools not to be used at all, although these tools would be useful to detect any such activity and ensure these very policies of not serving the VA/VASP sector are adhered to. Overall it would be advisable for these tools and databases, which are tailored to unique VA/VASP characteristics, to be used periodically by firms that prohibit VA/VASP activity.

Banks

336. Banks do not accept VA or allow customers to transact in them, nor do they accept VASPs as customers. The overall stance toward risk mitigation has been complete prohibition and to refrain from servicing this sector, both directly and indirectly. Banks recognize they have limited direct experience with VA or VA ML/TF risks, and have not received any supervisory guidance with regard to ML/TF risks arising from the VA/VASP sector.
337. For firms whose policy is to prohibit VA activity and prohibit servicing the VA/VASP sector, a key risk mitigation consideration for the assessment team was whether that policy is communicated, whether that policy is succeeding as designed, what steps the firm is taking to ensure the policy is performing as expected, and what measures are taken if breaches of the policy are detected.

338. The stance of not servicing VA activities has been communicated to banking customers and the sector as a whole. The assessment team found that certain systemic Cyprus banks specifically state this in their externally published or internal customer acceptance policies or customer communiques or both, enumerating VA/VASPs as a sector they do not serve. This restriction applies to issuers or dealers of VA, entities involved in conversions between fiat and VA, or related any services (e.g. software providers, payment processing services, card acquirers). Moreover, wire transfers in fiat currency that may be related to buying or selling VA are generally be enumerated as types of transactions that are not accepted or will not be processed by banks.
339. Upon detecting any VA activity on the part of current customers, banks were found by the assessors to demand these customers halt such activities. The assessment team found several examples of banks terminating relationships with clients and closing accounts upon detection of VA/VASP activities within their platform, or any ties to the VA/VASP sector, even if these activities took place outside the banking relationship.
340. Banks were found by the assessors to have standard procedures such as UBO thresholds, requiring proper documentation for source of funds investigations, and frequent screening of negative news and other information and sanctions violations. When negative information or unaccepted activity is identified, procedures are in place to take actions accordingly. There are also ongoing and automated transaction monitoring, with alerts based on riskiness of customers, reviewed on a frequent basis and on an ad hoc basis upon material changes (e.g. changes in directors, country of operations, etc.). VA activity raises red flags in terms of TF and ML risk monitoring measures. Moreover, the assessors found a number of banks to have proactively updated their transaction monitoring systems to capture transactions related to VA (e.g. by updating and adding key words and names of VA-related entities).
341. Banks also monitor card transactions and have policies against their usage for VA or for any purposes related to any VASP customers. Any indication of card usage related to VA appears reasonably likely to be detected under current monitoring practices, and banks provide warnings to such clients to halt these activities. The assessment team has found banks to have blocked VA-related transactions, and in some cases, terminated business relationships with corporate and individual customers for these reasons after providing warnings.
342. Banks generally have dedicated internal teams conducting AML/CFT functions and do not tend to outsource these functions. If bank policies were to evolve to permit any VA/VASP activities, it can be reasonably expected that internal teams would perform the AML/CFT functions with respect to VA/VASP ML/TF risks as well.

Non-bank FIs

343. The CBC believes that EMIS and PSPs under its supervision do not accept VA, and nor do they allow customers to transact in VA, and the assessment team's experience was consistent

with this view. EMIs and PSPs monitor customers and transactions regularly, with the use of indicators that would detect patterns of suspicious activity. There is widespread application of a risk-based approach, with clearly identified measures for high risk clients. Policies appear to be implemented consistently, with appropriate procedures for escalation and response.

344. One major MVTs reported internal policies that agents and partners are prohibited from using VA. To promote effectiveness of these policies, the MVTs tracks indicators that would detect patterns of suspicious transactions such as one to many, many to one, structuring and flipping.
345. EMIs are considered by the CBC as the entities most likely to engage in VA activities and/or serve VASP clients, although none are believed by the CBC to currently be doing so. The EMIs interviewed by the assessment team adhere to rigorous onboarding procedures and well established mechanisms to identify and monitor high risk clients, including a risk-based approach, taking into consideration guidance from FATF and other bodies. In the absence of a regulatory framework, they have refrained from serving VA/VASP activities. The assessors learned of cases where EMI clients engaged in or attempting to engage in VA/VASP activities were terminated.
346. Under the Cyprus regulatory framework, credit institutions under CBC may engage in certain MiFiD-type investment activities that would otherwise be regulated by CySEC. Should these investment activities extend to VA, then such VASP-like activities would fall under CBC and not CySEC. CBC should collect and monitor data regarding VA activity from supervised entities to ensure this is not arising undetected under its remit.
347. The assessors found one CySEC supervised entity authorized and already engaging in VASP-like activities to have expressed interest in obtaining an EMI license to support VA activities and met with the CBC; however in light of discouragement that entity is not seeking such licensing status in Cyprus, and reported that it is evaluating other EU jurisdictions for EMI licensing.
348. The assessors encountered another instance of an EMI that is considering potentially to accept or pay out in VAs; however this is contingent upon the enactment of the AML/CFT Bill as a legal framework coupled with promulgation of supervisory guidance before further action.
349. Across CySEC firms, VA deposits introduced directly from customers are regarded as highly risky and are broadly prohibited. Where permitted, they are subject to EDD and rigorous preventive measures. As the AML/CFT Bill has not yet been enacted and new CySEC guidance not yet provided, the assessors observed these measures to be mostly developed in-house, often in close collaboration with CySEC. The standards and rigor of the risk mitigating measures implemented for these activities was found by the assessors to be robust and effective.
350. For instance, one firm that allows spot trading in VA sources the VA itself, either directly from miners or from reputable vetted exchanges with strong risk controls and ratings, rather

than allowing customers to introduce VA from their external wallets. This is meant to ensure their legitimate origin and that most VA activity remains within its own ecosystem and under its internal monitoring systems that would detect any suspicious activity.

351. In general, entities engaging in VASP-like activities implemented robust client verification measures (e.g. video selfie, passport checks, address checks, IP address checks, ensuring client's country allows VA activity) and other risk mitigation measures for fiat currency deposits (e.g. applying wire transfer methods and ensuring source of wealth investigations with adequate documentation), VA deposits (e.g. deposit limits and confirmations on source of wealth from auditors), and tracking source of funds in VA using blockchain analytics. With respect to tracking these funds, these entities are also developing their knowledge on AML compliance and intelligence and blockchain forensics tools and databases.

DNFBPs

ASPs

352. From interviews with all three ASP supervisors and with selected CySEC supervised ASPs, the assessment team found that ASPs recognize the VA/VASP sector as risky. Because they do not serve this sector -- by not accepting VA and not servicing VASPs -- the opportunity for application of any risk mitigation measures has not arisen. Given their experience servicing already higher risk sectors due to the nature of their business and their exposure to international clients, ASPs already have experience applying risk mitigation measures for other high risk sectors and have indicated they would be willing to apply them to the VA/VASP sector if there were to arise demand for their services upon enactment of the legislation.

353. With regard to ASPs supervised by ICPAC, specific provisions relating to VA are included in ICPAC's 2020 AML/CFT Directive, including typologies that would indicate need for mitigating measures such as EDD or further inquiry into potential TF activity.

Casino

354. With regard to the casino, the assessors also noted that any application of risk mitigating measures with respect to the VA/VASP sector is out of scope because this sector is not being served. Since the concerns expressed in the Moneyval report, steps the casino may take to improve its compliance culture and its understanding of AML/CFT responsibilities should also minimize both the direct and indirect ML/TF risks that may arise at a later stage of the casino's development with respect to VA/VASPs.

355. Regarding direct risks of using VA for buy-in, while there is no official written prohibition policy forbidding VA, the casino has informed the assessors that it is not at this time accepting them and users are not able to fund their accounts or buy chips with VA. Based on the casino's observations, there has been no interest observed from clients wishing to do so, and there is no

supporting infrastructure in place to accept VA because all transactions go through the Cyprus banking system, which expressly avoids servicing this sector.

356. Regarding indirect risks of VA activity, the assessors considered the extent to which the casino's safeguards in place would mitigate the indirect ML/TF risks of VA, which could arise from the use of junkets if clients could transfer funds through that route from the Macau or Manila casino locations. However, junket operators licensed by the Casino Commission so far are prohibited by individual license conditions from managing or controlling customer funds or chips, or deposit money in any way. Their role at the moment is strictly limited to introducing clients to the casino. Therefore, the assessors consider the indirect risk of ML/TF posed by VA to be minimized as well at this point in time. With the expected increase in number of junket operators after the casino becomes operational, their licensing conditions under the Casino Commission may change.
357. The casino reports that both due diligence and funding of client accounts take place in Cyprus, and there is no reliance on other affiliate casinos in the network. Customers are issued their own credit facility based on the due diligence performed solely in Cyprus. Although the casino can grant them credit based on previous play, which is a common practice for casinos around the world, all play must be funded in Cyprus. The casino must ensure customers can pay in Cyprus, which goes through the banking system.
358. As for junkets, the casino's staff recognizes the need to monitor junkets closely and implement all the recommendations on KYC and AML procedures stated by the Casino Commission and their license obligations. While the process of initiating junkets was interrupted due to the COVID-19 lockdown, and the casino has had no experience with junkets to date, the Casino Commission's AML/CFT Directive requires mandatory EDD measures for all customers introduced by junket operators. The casino states it would follow the same procedures for a junket as it would for any high rolling customer (e.g. vetting through KYC, identity verification, source of funds).
359. In the gaming sector, operators under NBA supervision are understood to utilize payment service providers, which must be registered and licensed by the Central Bank of Cyprus. While payments must be in Euros, and users can make payments with cash, debit cards, or credit cards, online betting operators can accept electronic money. The assessors note that the permitted use of electronic money by online operators may create potential vulnerabilities. If users can fund their accounts with e-money through EMIs in the future, and EMIs are able and willing to accept VA, strict controls may be needed lest customers could channel illicitly obtained virtual assets into the system through the online betting industry, either directly or indirectly by converting them into e-money and then using it in these platforms.

According to the NBA, only land-based transactions below the €2,000 threshold are not subject to AML/CFT checks, in accordance with the requirements of AMLD. Online operators are required to conduct CDD on all their customers irrespective of whether the threshold is

surpassed. This includes a source of funds check by the operator. This could assist in the detection of illicit funds, whether in fiat or VA form.

360. One potential avenue to channel virtual assets into the system could be with the use of debit or credit cards based on underlying accounts funded by virtual assets. These cards would conceivably allow users to convert virtual asset holdings into EUR fiat currency in order to pay out winnings in the platform's desired currency. If these transactions are not adequately monitored, they could go undetected. Operators, which are responsible for monitoring transactions for AML, may not be adequately trained or have adequate procedures to identify, report, and respond to virtual asset risks.

361. Nevertheless, there has been no demand detected from industry players to use VA to date, and neither the casino nor gaming operators, to the assessors' knowledge, have received requests from clients seeking to use VA for funding or making payments.

VASPs

362. There are no VASPs registered as such in Cyprus. The only VASP-like activities have been taken up by entities under CySEC, discussed above.

5.2.3 Application of CDD and record-keeping requirements

363. The focus of the assessors in this matter has been on VASPs and VA activities, noting that apart from the selected CySEC securities firms authorized to engage in VASP-like activities, no other entities are servicing this sector. The general assessment team finding among this targeted population was of strong CDD measures applied, including obtaining and retaining BO and UBO information.

Banks

364. Moneyval found that Banks perform rigorous CDD, including obtaining BO information, and maintain records appropriately. The assessors found banks to adhere to strict onboarding policies for both retail and legal entity customers, which must go through screening procedures prior to obtaining accounts. There are also updated KYC and KYB reviews which take place upon onboarding and on a regular basis over time. These reviews refer to set parameters that take into account several risk factors (e.g. geography, country of operation, line of business, industry, country of residence). The assessors found banks to generally adhere to standardized AML/CFT practices of categorizing customers based on risk parameters, generally through risk scoring methodologies that classify clients as low, medium, and high risk.

365. The assessors found that these procedures are designed to detect any high risk activity, including VA/VASP activities on the part of customers, and that these procedures have been effective in deterring or eliminating VA/VASP activities. Banks interviewed by the assessment team reported receiving very few to no applications or inquiries for VA activity.

Non-bank FIs

366. Moneyval found that EMIs perform rigorous CDD including BO investigations. Several EMIs reported heightened BO standards, beyond minimum thresholds for higher risk entities. The assessment team found that while the most recent CBC AML/CFT directive applies to banks, and has not been updated for EMIs, PSPs or MVTs in a considerable time, EMIs nevertheless referred to the AML/CFT Directive for banks and adhered to its standards for their own internal customer onboarding and risk scoring procedures. This included identification of UBOs, directors, signatories, and stakeholders as part of the process of researching client corporate structures. These practices would be implicated if EMIs were to serve the VA/VASP sector.
367. Regarding CySEC-supervised firms engaging in VASP like activities, the assessors found rigorous CDD measures were applied, with standards tailored to customers based on the requirements defined by the CySEC AML/CFT Directive, even though the CySEC Directive has not been updated to cover matters relating to VA activities or customers. These standards were integrated into procedures for electronic onboarding with proof of identification. There was also rigorous screening of BOs implemented across these entities. Thus the assessors concluded that the fully compliant recordkeeping practices already observed by Moneyval would apply to these entities' activities related to the VA/VASP sector as well.

DNFBPs

ASPs

368. ASPs are understood to generally have policies in place to identify high risk clients and activities. The CBA is in process of launching an action plan aiming to increase its obliged entities' awareness with respect to undertaking effective CDD and other preventive measures. The CBA clarifies to its obliged entities that in undertaking these measures, they may rely on third parties subject to the requirements of AMLD. Its December 2019 Guidance expressly states that firms may rely on third parties for all or part of client identification and due diligence procedures, that these third parties must apply record keeping measures consistent with AMLD, and that the firms themselves remain liable in case of breaches.
369. With regard to VA, ICPAC has specifically addressed risk mitigating measures in its 2020 AML/CFT Directive.
370. Regarding BOs, ASPs are obliged to hold adequate, accurate, and current BO information, which is of particular importance with regard to foreign clients. This includes BOs' countries or residence, as well as customers' countries of incorporation (for legal entities), business activities, and total flows in and out of their bank accounts. Due to their role setting up Cyprus companies (usually private limited companies) that are ultimately owned and controlled by non-resident BOs outside of Cyprus, and acting as shareholders & directors on

behalf of them, it is imperative that ASPs ensure transparency for all legal persons involved. Yet Moneyval noted that full compliance with BO-related requirements was not uniformly met across all ASPs. This in turn made other entities' reliance on ASPs' records problematic.

371. These BO-related vulnerabilities are mitigated when ASP clients also hold bank accounts in Cyprus, given that banks were found by Moneyval to adequately adhere to BO-related requirements. However, banks in Cyprus have shown reluctance toward serving the VA/VASP sector. Therefore, the use case may be more likely to arise where a VASP or other entity engaged in VA activities will not have a local Cyprus-based bank account that has benefitted from the screening and recordkeeping performed by Cyprus banks as an additional line of defense. In such cases with respect to VA/VASP activities it is of particular importance for the ASPs themselves to maintain adequate BO records and remain compliant with their obligations.
372. Looking forward, the 2018 amendment to the AML/CFT Law set a legal basis for a BO registry, which is under construction and could further the extent of adequate and transparent BO information. The current AML/CFT Bill provides further legal basis for the BO registry.
373. For the casino, the assessment team reviewed its reported practices with respect to potential risks arising from VA/VASP activity, particularly given the overall AML weaknesses identified in the Moneyval report. However, no exposure to VA has been identified, as the Casino does not accept VA, and only accepts natural persons and not legal persons.
374. Regarding onboarding, the casino reported that it currently implements a threshold-based approach where customers that reach €2,000 in buy-ins or cash outs must provide identification, or their existing gaming card which holds their identification on file. The casino has informed the assessors that it has enhanced its specific procedures for additional due diligence for high-risk customers and high-risk jurisdictions. These procedures have been verbally communicated to the assessors by the casino staff, and the assessors acknowledge there has been no independent assessment or verification of their implementation at the moment. For high-risk customers, once they are identified upon registration or reaching the threshold, the casino requires additional due diligence on source of funds. Any hits in the KYC screening software used would be flagged and raised to the AML department for review. The Casino considers that its CDD measures, as they commence upon such €2000 threshold, are stricter than those required by FATF Recommendation 22.1.(a), which sets a higher threshold. Any suspicions detected are to be raised to supervisors and managers, and thereafter to the dedicated AML team at the corporate office if these concerns persist. These measures would be applicable for VA/VASP activities if they were to arise.
375. Moreover, the AML Law requires the casino to perform its own CDD as the obliged entity ultimately responsible for CDD. Thus, it cannot rely on CDD performed by junkets, and the casino reported that its frontline staff are being trained to understand this distinction. The casino also reported that documentation and buy in procedures for junkets would require an additional monitor or signatory and involve supervisors (at minimum) or managers rather than being left to the general cashiers.

VASPs – none registered – see CySEC firms above

376. There are no VASPs registered as such, so any CDD and record-keeping requirements performed by the VA/VASP sector would be irrelevant for this risk assessment. There are no VASPs registered as such given the framework for registration is still underway. See discussion above for authorized firms under CySEC carrying out VASP-like activities for relevant measures.

5.2.4 Application of specific and EDD measures by FI, DNFBPs and VASPs

New Technologies

377. This assessment of this core issue focused primarily on EDD for VA/VASPs involving New Technologies, particularly VA, and Wire Transfers of VA, due to the targeted scope of this risk assessment. R.15 was substantially expanded in 2019 in conjunction with the expansion of FATF Guidance applicable to VA and VASPs, with the addition of Criterion R.15.3 through R.15.11, and this section should be read in conjunction with the discussion of R.15 in the Technical Compliance Annex. Many jurisdictions are being re-rated under R.15 in light of these expanded and updated requirements.

378. The main deficiency identified in the 5th round MER under R.15.1 and R.15.2 was that only certain types of obliged entities - credit institutions, securities and insurance firms – but not other types of FI were required to identify, assess, and manage the ML/TF risks that may arise in relation to new technologies. A technical deficiency further observed in the MER was that these obligations may be considered to arise indirectly rather than directly³⁰. The AML/CFT Bill rectifies this deficiency with specific new statutory language (Art 66(3)) that expressly requires obliged entities to take appropriate measures to identify and assess ML/TF risks prior to the promotion of any new technology, service or product. This requirement will apply to all obliged entities, including VASPs as well as other types of obliged entities holding other licenses engaging in VA activities (such as the CySEC-licensed securities sector FIs engaging in VA activities).

379. Even prior to enactment of this measure, the assessment team found a widespread practice among entities of checking with the regulator before engaging in any new service or adopting any new technology. This was so notwithstanding the technical deficiency identified in Moneyval report with respect to R.15.1/15.2. The assessment team found this to be the case especially with respect to VA/VASP-like activities performed by the CySEC-regulated firms authorized to operate in the sector under CySEC Circular C244, which set rigorous procedures in-house. Thus, the assessment team found that the technical deficiency identified by Moneyval did not meaningfully reduce the effectiveness of the Preventive Measures in relation to VA/VASPs and new technologies.

³⁰ Under AML/CFT Law Section 64(3) and Annex III par. 2(e) – to be discussed here shortly below.

380. The assessment team considers that Art. 66(3) unambiguously imposes a requirement on obliged entities to identify and assess ML/TF risks prior to the promotion of any new technology, service or product involving VA because of its novelty as a technology as well as its novelty in a service or product offering.
381. The assessment team found that the AML/CFT Law may implicitly be understood to require EDD for VA activities, although VA are not expressly enumerated in the relevant provisions of the AML/CFT Law. Specifically, Article 64(3) provides that EDD measures should be performed for high-risk factors, and in Annex III stipulates a non-exhaustive list of high-risk factors that could readily be understood to apply to VA. These include (b) “products or transactions that might favour anonymity”; and (e) “new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products”. Existing FIs in the securities sector engaging in VA activities, and VASPs once registered (and thus qualifying as obliged entities) are subject to these enhanced EDD obligations for high risk activities that could be read in clauses (b) and (e) to encompass VA. Certain (although not all) VA involve products or transactions that may favour anonymity, or at minimum pseudonymity, and VA products, services and practices plainly fall within the criteria enumerated in (e) at current stage of development and maturity. Certain Cyprus authorities expressed a view that these provisions already applied to VA/VASPs, thus already requiring EDD.
382. These requirements could and should readily be made explicit when CySEC updates its AML/CFT Directives after enactment of the AML/CFT Bill, and/or in the conditions established for registration under the VASP registry. It is recommended that other authorities also make this explicit when updating their AML/CFT Directives or guidance following enactment of the AML/CFT Bill. The assessment team found a general appetite on the part of supervised entities for guidance from the regulator before embarking in any new area, not limited to VA.
383. ASPs supervised by ICPAC are expressly subject to EDD requirements under ICPAC’s 2020 AML/CFT Directive, which (Section 5.7.4) specify “cryptocurrency related activities” as a high risk area in a client profile warranting specified EDD measures. ICPAC has also issued circulars regarding VA identifying that as a high risk area (Section 4.6.4) and has made clear that supervised firms are expected to take high risk areas in their risk assessment design process. ICPAC has also identified “Sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity” as a red flag for suspicious client TF activity for its supervised ASP entities, that would likewise warrant EDD.

Wire Transfers

384. *See also R.15.9 for further discussion with respect to Wire Transfers in the context of new technologies.* There were no entities registered as VASPs at the time of the assessment. CySEC regulated firms engaging in VASP-like activity, however, clearly follow the CySEC AML/CFT Directive and existing obliged entity requirements for conventional fiat wire transfers. The wire transfer rule for transfers of VA by VASPs established by FATF in 2019 has not been

enacted into law in Cyprus, is not included in the AML/CFT Bill and is not accounted for in the existing CySEC AML/CFT Directive or other supervisory directives. CySEC has confirmed that this will be addressed in its upcoming revised AML/CFT Directive.

385. Where transfers for the activities in the VA/VASP sector performed by CySEC supervised firms are from non-VASP customers and not VASPs, the wire transfer rule would be inapplicable. For outgoing transfers in general directly sent to customers and not to other VASPs, the wire transfer rule would similarly be inapplicable. However, there are instances when CySEC-supervised firms send or receive VA to or from VA trading platforms or exchanges that would likely be considered VASPs – although it should be emphasized that many jurisdictions have not yet established a VASP licensing or registration regime and thus these trading platforms or exchanges may not be legally considered VASPs in their jurisdiction of organization. Nevertheless the assessment team regards such entities as plainly functioning as VASPs within FATF definitions. The assessment team did not find general adoption of the wire transfer rule for VA into these entities' written procedures. It is recommended that this rule should be broadly adopted and documented.

386. The assessment team noted that the VASP industry is still developing solutions to comply with the Travel Rule for VA from a technological and operational perspective, and there is not a single approach yet developed on best practices for doing so. Examples of approaches to date at the time of the assessment include the InterVASP Messaging Standard, the Travel Rule Information Sharing Architecture (TRISA), Travel Rule Protocol (TRP), OpenVASP, Tatashi Professional, NetKi, Sygna Bridge, BIP75 Protocol and Nota Bene. Firms should continue to monitor the evolution of these best practices and industry standards for compliance with the Travel Rule, so as to account for them in their own internal procedures.

387. Among CBC regulated firms, none were found by the assessors to allow transfers in VA. Firms generally reported that they are waiting for CySEC and the CBC to update their AML/CFT Directives before creating or updating their own written policies and procedures in relation to VA/VASPs, wire transfers of VA, and any other ML/TF matters relating to VA.

Targeted Financial Sanctions

388. With respect to targeted financial sanctions, see R.15.10 for a fuller discussion (including analysis of c.6.5 and c.7.2). Existing obliged entities including CySEC firms engaging in VASP-like activities have been found by the assessors to generally rely on subscription services, notices from FATF and bulletins from Cyprus regulators in their implementation of procedures for this matter, and VASPs should be required to do so as well as an operating condition of registration. Once VASPs are provided with a framework to register as such, CySEC should ensure it includes them in its information distributions to its supervised entities.

389. Decisions on updated designations for sanctions lists announced after Nicosia business hours may not be communicated by supervisors until the next Business Day. Because VA markets, unlike traditional financial markets, are active constantly outside of business hours,

and transactions and movements of assets occur 24/7/365 unlike traditional movements of fiat currency, this could be a meaningful gap with regard to VASPs and movement of VA for TF purposes, which could be moved and utilized during these times, particular overnight, weekends and holidays. Although VASPs as obliged entities will be subscribing directly to databases that also provide these updates independent of the supervisory notification channel, thus mitigating the risk of this gap, a potential gap remains. VASPs and other firms engaging in VA activities should ensure that they are able to implement updates outside of normal business hours, and utilizing database channels as well as supervisory notification channels.

Higher-risk countries

390. Where banks have offices in higher risk countries, the assessment team found that these tend to be marketing and service centers. Operating as representative offices, these foreign bank branches generally provided no banking services, and merely provided assistance in onboarding or renewals for customers. CDD and AML/CFT functions were found by the assessors to take place in and be managed in Cyprus for all firms the assessment team interviewed. Thus compliance functions were centralized, with onboarding handled at the Cyprus offices. Procedures require approval from compliance departments in order for clients to open an account. While the assessment team considered whether having branches in higher risk jurisdictions could be a conduit for VA risk from those jurisdictions, the above structure should mitigate any such risk. The assessment team also recognizes that both in theory and practice, high risk countries as a source of VA would likely be a clear factor determining firms' application of enhanced risk mitigation measures for high risk transactions.

Cyprus Investment Programme

391. With regard to the recent Cyprus Papers reports in relation to the Cyprus Investment Programme, although there were major weaknesses exposed including AML/CFT, and the program was suspended and subsequently terminated, none of these vulnerabilities have been indicated to be related to the VA/VASP sector or to involve the use of VA.

5.2.5 Reporting obligations and tipping off

392. The assessment team concurs with Moneyval's finding that generally there are well established policies and procedures regarding STRs across all categories of obliged entities, although the specific triggers and filing frequency may vary across entities. Moneyval observed that in the banking sector, at least, there was a convergence toward more consistent filing frequency and filing triggers for STRs/SARs.

393. The assessment team was informed that there has been to date a very limited number of STRs arising from data that would relate to VA or VASPs. Very few firms engage in this sector to begin with. For those few firms that reported filing STRs in relation to VA/VASPs, they also observed that no feedback was provided from MOKAS regarding how to proceed with taking action upon confirming a suspicious case. However, it is not customary for the FIU to provide

feedback on STRs as they are for confidential investigations. MOKAS guidance or feedback is deemed by these firms to be sought after guidance if provided, given the lack of a regulatory framework and the novel issues that the VA/VASP sector presents.

394. There is a general appetite for further guidance from supervisors on STR/SAR reporting for VA/VASPs, especially once the new AML/CFT Bill is enacted. Thus it is advisable for supervisors to provide such guidance to their supervised entities. It is also advisable for MOKAS to update its GoAML system through which firms report SARs/STRs. This would entail repopulating the standard reporting template with additional relevant fields related to VA, and in turn facilitating measures to track VA metrics. SARs/STRs are prioritized by MOKAS as high/medium/low risk based on information from the reports submitted by the firms. Prioritization for reports dealing with VA would depend on the context of the issues reported.

395. Entities interviewed by the assessment team revealed a desire for new guidance targeted to VA regarding when to stop or permit a suspicious VA transaction initiated by a customer in order to avoid tipping off. Such guidance, as indicated by Sections 55 and 70 of the AML Law, is indicated to fall under the statutory duties of the FIU.

5.2.6 *Internal controls and legal/regulatory requirements impending implementation*

396. The assessment team generally found strong internal controls, written policies and procedures, and that firms had a designated AMLCO. The assessment team's specific findings with respect to CySEC supervised VASP-like firms showed strong internal controls, written policies and procedures, and an adequate appreciation of riskiness. Moneyval also found that the secrecy laws do not impede implementation of these measures, and the assessment team found no reason to determine otherwise.

6. Supervision

6.1 Key Findings and Recommended Actions

Key Findings:

FI Supervisors

1. CySEC is the only supervisor with direct experience of supervising VA activities or VASP-like entities. CySEC has developed a substantial understanding of VA. Since 2017, licensed CIFs and an AIFLNP³¹ have been granted authorization to engage in VA activity. CySEC has engaged closely with these entities to mitigate the risks and acquired first-hand experience applying rigorous AML/CFT procedures. This has provided CySEC with insight on the specific novel issues and risks that VA represent. Moreover, CySEC's supervision of VA/VASP activities has been a specific area of focus and support from executive leadership. There is not a mature VA market at this moment, and CySEC is in process of understanding the emerging risks of such a VA market. After the risks are identified, it is expected that they will be evaluated and mitigation measures will take place.
2. All FI supervisors recognize VA as posing substantial AML/CFT risks and novel issues, and uniformly consider VA a high-risk sector. There is a range of degree of awareness of VA-specific characteristics as well as preparedness to supervise VA activities and mitigate risks.
3. The CBC has issued warnings as early as 2014 emphasizing that VA are an unregulated space. These actions, as well as concerns articulated by CBC in meetings with potential actors, appear to have discouraged supervised entities from engaging in VA activities and created a perception that they are banned. There is in fact no CBC prohibition against VA. With no VA activity under its purview, the CBC has not established supervisory measures tailored to VA or addressed VA.
4. FI AML/CFT supervisory resources at CySEC and CBC are strained by existing activities. CySEC has indicated a capability to allocate planned new hire resources to support VASP oversight. CySEC is also evaluating specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases that should promote efficient off-site supervision in monitoring VASP activity, especially VA trading platforms. Other supervisors are not currently using or considering such tools and databases.
5. Apart from CySEC staff directly engaged with or involved in supervising the existing entities engaged in VA activities, and select personnel working on the CySEC Innovation Hub, detailed understanding on this sector is limited. Other than general overview of VA, there has been quite limited training centered on VA ML/TF risks and mitigation measures, either at the level of FI supervisors or from supervisors to regulated entities.

³¹ Alternative Investment Fund with a Limited Number of Partners

6. Other than CySEC, FI supervisors are awaiting the enactment of the AML/CFT Bill before formulating and issuing directives guidance regarding VA activities. CySEC is developing its updated directive and is also developing, but has not yet released, the conditions it will require for entities obtaining and retaining registration under the VASP registry. The first directive will be in regard to the registration process and requirements.
7. VA Kiosks currently fall under a potential regulatory gap that should be discussed between the CBC and CySEC.

DNFBP Supervisors

1. Supervision of ASPs is the critical line of defense against ML/TF. ML/TF risks associated with ASP sector may heighten as VA activities and VASP sector start to develop further in Cyprus, so the role of the ASP supervisors will be of increasing significance in mitigating potential risks or abuses.
2. The ASP supervisors apply market entry measures and a risk-based approach to licensing and supervision, although with different degrees of intensity.
3. CySEC has acquired experience supervising non-ASP entities engaging in VA activities and established data collection and supervision procedures for VA activity for these non-ASP entities that could be applied to ASP supervision with respect to VA/VASP ML/TF risks.
4. ICPAC has established data collection measures to detect VA activity as part of its ongoing monitoring and supervision, though not at the licensing stage. It has also directly addressed VA ML/TF risks in its 2020 AML/CFT Directive, including where EDD is required or heightened TF risks may be indicated.
5. The CBA is in the process of generating guidance and collecting data on VA activity and setting procedures, through a revised questionnaire, and in providing guidance through its revised AML directive.
6. The Casino Commission detects no direct risks at this time from the use of VAs in the casino, since there is no mechanism to accept them as buy-in and all transactions are conducted in fiat currency. There is also no indirect risk of VA arising from the use of junkets, since all funding must occur directly with the casino.
7. The NBA considers that there are no VA being accepted or paid in the betting sector. The NBA does not permit any licensed firms to accept VA as a means to place bets or fund accounts.³²

Recommended Actions:

FI Supervisors

1. FI supervisors should ensure they have regular procedures to share information and evolving best practices with other supervisors in FI and other areas relevant to

³² The NBA has advised the assessment team that it is evaluating establishing a potential innovation sandbox in which it could potentially expressly incorporate VA considerations within their data collection and reporting templates, supervisory procedures and AML/CFT directives without implying permission (see Section 6.2.3 below) As of the date of this assessment such sandbox had not been established nor have its terms and conditions been completed.

oversight of VA activities. This may be achieved through a standing agenda item at Advisory Authority or through initiation of a standing subcommittee including AA supervisor members.

2. FI supervisors should regularly assess the adequacy of resources for supervision with regard to VASPs and VA activities, including training, software tools and staff. CySEC is already in the process of assessing the specific products and will continue the assessment.
3. The regulatory framework for VASPs in Cyprus is a registration regime, not a licensing regime. Cyprus should closely monitor this sector to ensure that its registration framework remains proportionate³³ to the actual ML/TF risks. For example, market supervision including market surveillance and market integrity practices may be needed at a future time to detect and deter money passing.
4. FI supervisors should add VA-specific elements to their existing registration, licensing and supervision practices and written procedures to include VA activities.³⁴
 - a) FI supervisors should increase trainings on VA, going beyond general introductions to VA, particularly ways they can be used or misused for ML/TF, and risk mitigation measures. Training should be delivered to staff, covering best practices for authorization, licensing and supervision procedures, ways to ensure that supervised entities are adequately meeting their requirements, and ways to perform checks during on-site and off-site inspections. Training should also be provided to supervised entities covering best practices to remain compliant and set effective AML/CFT preventive measures for VA.³⁵
5. The CBC and CySEC should update their respective AML/CFT Directives to include measures dealing specifically with VA activities and VASPs promptly after the

³³ The June 2019 FATF Guidance allow equally for a jurisdiction to elect either a registration framework or a licensing one for VASPs, so no deficiency can be found with respect to Cyprus's determination to proceed with registration. However, the Guidance also provides that countries should monitor risks on an ongoing basis to ensure its framework continues to be suitable. (Par. 61): As the VASP sector evolves, countries should consider examining the relationship between AML/CFT measures for covered VA activities and other regulatory and supervisory measures (e.g., consumer protection, prudential safety and soundness, network IT security, tax, etc.), as the measures taken in other fields may affect the ML/TF risks. In this regard, countries should consider undertaking short- and longer-term policy work to develop comprehensive regulatory and supervisory frameworks for covered VA activities and VASPs (as well as other obliged entities operating in the VA space) as widespread adoption of VAs continues.

³⁴ For example: (a) Source of funds analysis during authorizations should expressly query whether any funds sourced from VA; CySEC should adopt a monthly prevention statement for VA transactions modelled after its cash monthly prevention statement. Its supervision handbook should also include typologies for cash transactions that are highly relevant to VAs and can be adjusted to apply to VAs. (b) There should be a review to identify if there are any additional typologies, behaviors, or indicators that are unique to VAs and distinct from those that already exist in cash, and devise procedures accordingly to close any gaps leading to potential ML/TF vulnerabilities; (b) The CBC should update its templates for reporting by regulated entities, including enumerating risk factors that take VA into consideration. Under AML Policy, firms must disclose how much high risk business they process (e.g. metrics collected on profile distribution, geographic distribution, and other data on clients, but no VA section). There is no data collected on whether banks are servicing VA clients, and no evidence-based baseline. (c) VA activity, for instance, should be included as a pre-populated template category under the high-risk business disclosures required from obliged entities under the CBC's AML policy, which will also assist the CBC to start collecting data on whether and to what extent its regulated entities service the VA sector.

³⁵ This is encouraged by the June 2019 FATF Guidance – see pars. 163-165 thereof.

AML/CFT Law amendment is enacted. The revised directives should expressly incorporate the “travel rule” with regard to procedures for transfers of VA. The CBC should update its AML/CFT Directive to refer expressly to VA, and also cover non-bank FIs like MVTs, EMIs and PSPs with regard to AML for VA activities, as a minimum. CySEC is in the process of updating its directive.

6. Supervisors should receive access to and training on specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases. CySEC has reported that it will continue to evaluate products, and depending on the supervisory needs, the choose products accordingly.
7. CySEC should provide guidance to obliged entities with regard to what constitutes suspicious activity or typologies of ML/TF in VA activities and VASP sector. In doing so it may effectively utilise the 2020 FATF Red Flags publication. CySEC should also provide training to obliged entities with respect to suspicious activity in the context of VA activities and VASP sector.

DNFBP Supervisors

1. The three joint ASP supervisors should seek to harmonize their approaches with respect to VA activities and VASPs. CySEC and CBA should add VA/VASP activity to their data collection with respect to ASPs.
2. The three ASP supervisors should share information with each other regarding ASPs under their oversight engaged in VA/VASP activities. Information on rejected applications and withdrawn licenses should be openly available across ASP supervisors
3. The three ASP supervisors should hold trainings for ASPs on VAs, particularly ways they can be used for ML/TF and adequate risk mitigation measures.
4. Following enactment of the AML/CFT Law amendment, ASP supervisors should issue guidance (in the case of ICPAC, further guidance) on how to comply with the primary legislation with respect to VA/VASP activities from ML/TF perspective.
5. The Casino Commission and NBA should expressly incorporate VA considerations within their data collection and reporting templates, supervisory procedures and AML/CFT directives. In doing so, they should make clear that there is no implied permission for supervised entities to engage in VA activities (as NBA has indicated with respect to its potential sandbox under consideration).

6.2 FATF Immediate Outcome 3 (Supervision)

FIs

397. In assessing supervision in Cyprus the assessment team found that there is currently supervised VA or VASP-type activity only under CySEC, barring any undetected activities. The assessment team did not limit its assessment to those areas, however; rather it considered other supervisory sectors to consider risks and vulnerabilities as well as existing controls and mitigants in those sectors. In considering other areas of supervision, the assessment team

focused on whether there were existing VASP or VA activities, whether there were apparent means for VA to enter the supervised sector, and on effectiveness of existing supervisory controls meant to exclude VA.

398. FIs fall mostly under the oversight of the CBC or CySEC, or in the case of the insurance industry, the Superintendent of Insurance.

AML/CFT supervisory authorities for FIs and VASPs are designated as follows:

- (i) CBC supervises credit institutions (including branches of foreign institutions), e-money institutions (including branches of foreign institutions and agents of EU institutions), Payment institutions (including branches of foreign institutions and agents of EU institutions), others (Credit Acquiring Companies, Leasing, Bureaux de Change, MVTs);
- (ii) CySEC supervises VASPs (under the pending AML/CFT Bill), Cyprus Investment Firms (CIFs), External Investment Fund Managers, Internally managed Investment Funds, Undertakings for Collective Investment in Transferable Securities (UCITS), UCITS Management Companies (UCITS MC), Alternative Investment Fund Managers (AIFMs), Alternative Investment Funds (AIFs), and Alternative Investment Funds with a Limited Number of Persons (AIFLNs); and
- (iii) ICCS supervises life insurance companies and intermediaries.

CBC

399. The banking sector, which is the most material in Cyprus, is supervised by the CBC. The banking system is a key backstop to prevent suspicious activity and risky persons from entering the system because much of the economy relies on banking services. Other authorities could be said to rely on banking as a first line of defense because of the reliance by their supervised entities on the banking sector to screen and mitigate risks of banking customers. This creates a significant burden of responsibility on CBC as the banking sector supervisor to establish and ensure the right controls. Other non-bank financial institutions, including PSPs (PIs), EMIs and MVTs, also fall under the CBC. While there is no specific restriction or prohibition or regulatory framework for VA activities, there has been a general reluctance on the part of the CBC to encourage VA activities and a perception that the CBC prohibits VA activities.

CySEC

400. CySEC oversees investment firms and funds. A small number of CIFs have sought and received special permission to engage in VA activities under the Cyprus CIF Law of 2007 and CySEC circular C244, which also provides that VA activities must remain under 15% of turnover. No new permissions under C244 have been granted since 2018.³⁶ An AIFLNP has been authorized to engage in VA investment.

³⁶ The relevant provision that CIFs were granted permission to engage in VA activities was under the 2007 CIF Law and not under the C244. Firms had submitted their applications under the CIF Law as it was considered an “other service” and “(b) it has received the Commission’s permission, which is granted, at its absolute discretion, in exceptional circumstances”

401. CySEC will also oversee the VASP registry, although it has not yet been established under the amendment to the AML/CFT Law nor have the conditions to registration been established. This will be established when the new directive is completed.

402. The VA/VASP activities carried out so far by CySEC have been an area of particular focus and support from executive leadership of the organization. This level of awareness and support is also envisioned for further VA/VASP supervisory activities upon enactment of the framework. CySEC has also demonstrated a high level of engagement and responsiveness with the assessors throughout the risk assessment process.

Superintendent of Insurance

403. The Superintendent of Insurance oversees life and non-life insurance companies and has found VA activities largely irrelevant for this sector. It has observed or identified essentially no use cases for VA activities for the entities it supervises, and thus any VA or VASP ML/TF risks arising from them appear to be negligible.

DNFBPs

ASPs

404. ASPs fall under the supervision of either the CBA, ICPAC or CySEC, depending on the service provider's specific profession and license. ASPs are obliged entities under the AML/CFT Law, and the nature of their business was classified as medium-high risk by the Cyprus NRA. This status makes the role of ASP regulators paramount for ensuring adequate AML/CFT safeguards. The ASL Law obliges all persons providing company services to be regulated and supervised, in addition to lawyers and accountants who are already covered by the AML/CFT Law. While all ASPs fall under the same primary legal and AML obligations, at the level of secondary legislation, each regulator has a different directive.

405. The existence of three separate supervisors can give rise to weaknesses due to differences in directives. In the absence of a unified communication platform to exchange information on ASPs that have been sanctioned, rejected or declined licensing, or stricken off a regulator's registry, they could theoretically be banned by one regulator and proceed to obtain licensing from another. It should be noted that the ownership criteria imposed by ICPAC and the CBA makes the move from one regulator to another difficult as both supervisors only license ASPs that qualify to be their members, i.e., qualified accountants and qualified lawyers respectively.

The 15% limitation on the CIF's total turnover was included in the C244, as the law did not include a provision that applied specifically in DLT services. This was included in a Circular that has now been replaced as in 2018 CySEC stopped accepting any new applications. C244 was published as ESMA/EU had not yet issued their official position determining whether the trading on CFDs relating to virtual currencies falls under paragraph 9, Section C, Annex 1 of MiFID. Following the publication of the EU's bodies re the above determination C244 was replaced.

Moneyval found that in practice, coordination and information sharing among these three joint regulators takes place on a case by case basis, where they may send each other information related to high risk findings. Supervisors reported, however, that exchange of information has been more systematic in the past two years, and have taken extra steps to identify applicants who have been licensed by another supervisor. For example ICPAC has incorporated a section in its initial license application on whether the applicant has applied for or has previously been granted a license from another supervisor triggering thus a communication with the relevant supervisor. Each ASP regulator maintains a separate trust register for those trustees under their respective supervision, with information on the trust's name, date of establishment, date of any changes in governing laws, date of termination, and each trustee's name and address. These registers are made accessible across the three ASP regulators for the purposes of performing supervisory duties under ASP and AML/CFT legislation.

406. Moneyval strongly recommended convergence in procedures across the three ASP regulators.
407. The Moneyval report found all three regulators short on resources and staff, except for ICPAC which was found to have sufficient resources for its on-site monitoring and outsources a number of its tasks to external advisors. Any such shortage would pose risk to the effectiveness of licensing and supervision. For ASPs, the costs of implementing the most effective safeguards represent an important vulnerability as well.
408. Weaknesses and vulnerabilities for the ASP sector are of particular concern for Cyprus because they represent a major sector of the economy. In the realm of VA activity, shortages in resources and staffing could be even more pronounced due to the novelty of the subject matter, need for training and dedicated support, and added risks given that VA activities may be decentralized and/or cross-border.
409. The assessment team found no indication of substantial VA or VASP activity currently taking place in Cyprus on the part of ASPs, nor did the three supervisors indicate that in their perception there is currently any meaningful VA activity in the ASP sector. Supervisors anticipate that when the amended AML/CFT Law is enacted and a regulatory framework for the VASP sector is formally introduced, ASP activity related to VA and VASPs may increase. In the view of the assessment team, any impact of risks or deficiencies in the supervision of ASPs could at that time impact ML/TF risks in the VA/VASP sector involving ASPs.

Casino & Betting

410. The casino and gaming sector is supervised and operated as two separate segments: the casino and the betting sector which consists in online gaming platforms. Each segment falls under its own respective legislation and supervisory authority.

411. Gaming was made legal in Cyprus with the 2015 Law to Regulate the Establishment, Operation, Function, Control and Supervision of Casinos and Related Matters (Cyprus Casino Control Law) and related Regulations. The 2015 Cyprus Casino Control Law also provided for the establishment of the National Gaming and Casino Supervision Commission (Casino Commission), which acts as the single competent authority for licensing, supervision and control of casino operations. The casino is considered by Moneyval to be the fourth most material sector in Cyprus due to the size of the Integrated Casino Resort (ICR) undertaking in construction at the time of the assessment.
412. The Casino Commission was established in 2017 and became operational in January 2018, to supervise the casino with the mission of ensuring casino gaming remains safe and fair, while ensuring adequate understanding and management of potential harms to society, minors, and vulnerable groups. Its responsibilities include assessing applications and granting licenses for casino operations, ensuring the casino operator remains compliant with the obligations under the terms of its license, performing audits and regular supervisory checks, and exercising disciplinary powers (e.g. imposing sanctions, fines, and penalties) as necessary. Online casino services are prohibited in Cyprus under the 2012 Betting Law.
413. The Betting Law established the National Betting Authority (NBA) as the independent supervisory authority with financial independence and autonomy, responsible for regulating, supervising, and monitoring Cyprus betting activities. Cyprus legislation defines betting as any form of bet on sporting or other events, carried out either online or offline, where a number of physical persons participate. Land-based and online betting shops based on sports or other real events with fixed odds, online gaming, and horseracing are popular examples of such activities. These activities are not subject to Cyprus casino legislation but to the Betting Law which legalized them in 2012. This legislation, amended further as the Betting Law of 2019 37(I)/2019, strictly prohibits online casinos and lotteries, with the exception of the National Lottery and charitable purpose lotteries.
414. This sector was not included in the Moneyval report. However, it was covered in the Cyprus National Risk Assessment of 2018.

6.2.1 Licensing, registration and controls preventing criminals and associates from entering the market

415. The assessment team focused for purposes of this core issue on BO/significant or controlling interest or management function in a VASP (or other entity engaging in VASP-like activities). For practical purposes to date this has been limited to FIs engaging in VASP-like activities, such as those already authorized to do so by CySEC. and VASPs seeking registration under the amended AML/CFT law. VASPs under the amended AML/CFT Law will be subject to registration (but not licensing) by CySEC.

FI Supervisors

CBC

416. The CBC has been conservative in setting strict controls in the aftermath of the financial and banking crisis. This is understandable given the importance of the banking sector and the potential adverse consequences of a new ML/TF scandal arising from inadequate licensing or registration controls.
417. Moneyval found CBC to have robust licensing, registration and other controls with regard to management and control persons of CBC-licensed entities. Because under the amended AML-CFT Law VASPs would be licensed by CySEC, not CBC, and because CBC has shown limited appetite for licensing entities under its remit to engage in VA activities, it seems unlikely that CBC's ability to act as a line of defense against unfit or criminal persons holding ownership or management roles in VASPs will be tested in the foreseeable future. The assessment team considers that the CBC could reasonably be expected to apply its rigorous controls to any new VASPs or VASP-like entities falling under its remit and serve as a strong line of defense against unfit or criminal persons holding ownership or management roles in VASPs.
418. Credit institutions of significance are licensed through the EU Single Supervisory Mechanism. The CBC's licensing team currently addresses primarily non-bank licensing, as there have been no new banks being established in Cyprus in the last 5 or more years. CBC has taken the position under PSD2 to require its licensed entities to establish separate legal entities for "other" activities, thus reducing further the likelihood that CBC would be in position to process registration or licensing of aspiring regulated entities engaged in VASP activities.
419. A separate and potentially significant risk, although outside the CBC's control under applicable EU law and treaties, may arise from passported EU firms from other EU jurisdictions, such as EMIs or PSPs, for whom CBC does not have authority or typically receive information regarding BOs or management, particularly if they are solely operating on line or without a branch or legal entity in Cyprus. In this respect CBC and Cyprus are dependent on other EU jurisdictions to carry out their supervisory responsibilities effectively with respect to this core issue.

CySEC

420. CySEC has been granted express statutory authority to consider and ensure fitness of BO, UBO and management for potential VASP registrants, and has demonstrated strong capabilities for existing registrants, including those already engaged in VA activities. CySEC's new registration procedures for VASPs are currently being defined, as are the conditions for VASPs to obtain or maintain registration, so it was not possible for the assessment team to consider those.
421. CySEC has permitted a very limited number of existing supervised firms to engage in VA activities as well as authorizing one new AIFLNP – in each case under its existing supervisory

and licensing framework. CySEC has thus gained hands-on experience to screen out risky persons from becoming BOs, UBOs, or gaining a managerial position or controlling interest.

422. CySEC has approached VA activities in a way that has already applied its rigorous due diligence and controls to the sector to prevent suspicious persons from entering the system. Applying existing strong screening procedures for BOs and management, CySEC uses various tools to check for the character and fitness to ensure these persons are proper for their role and do not have ties to criminal activity.
423. CySEC's procedures for authorization for FIs consist of two steps, first shareholder due diligence, followed by a business model and organizational structure assessment. These are designed to ensure no undesirable entry. The first step is central to this core issue. Under the first step, due diligence procedures ensure shareholders' good reputation, no engagement in criminal activities, and an adequate source of funds. CySEC requires information from the entire shareholder structure, including direct shareholders and intermediate entities if applicable, and tracing back to the UBOs. The process involves a questionnaire, KYC assessments utilizing both specialized software and web searches, and references from any other Cyprus, EU, and non-EU competent authorities supervising the applicant. Source of funds investigations, especially for first time authorizations, ensure the initial capital injection derives from legitimate funds that are sufficient to support operations for at least 3 years. CySEC requires supporting documentation such as tax returns, bank confirmation letters, and audited financial statements for legal entities. These due diligence measures are also applied for approval of changes in control structure, shareholding structure, and license extensions.
424. If CySEC staff is satisfied with the appropriateness of shareholders, the applicant is presented to the Board for pre-approval. Any information that may dispute shareholder appropriateness is listed in a memo with deficiencies and concerns to assist the Board in deciding whether proceed with the authorization or reject it. Existing legal provisions specify that license applications can be rejected upon the competent authority having doubts on the appropriateness of shareholders, such as concerns on their financial soundness, good reputation, etc.
425. The second step for authorizations is to assess the business model and organizational structure of an entity. If CySEC is satisfied that the entity complies with its relevant legal provisions for this matter, it proceeds to grant authorization.

ICCS

426. Both the Moneyval assessment and the 2018 Cyprus National Risk Assessment consider the insurance sector to pose a low ML/TF risk. The Superintendent of Insurance oversees life insurance undertakings and life insurance intermediaries, which make up a small sector, in terms of number of companies and Euro amounts sold. New entrants are few - in general it grants a new license every 1-2 years due to the small number of incoming players.

427. Because insurance companies sell simple products and invest in very conservative assets (e.g. government bonds, corporate bonds, UCITS), there is no apparent material nexus with VA activities, either in their assets held or in their payment terms. Hence the Superintendent of Insurance has not seen a need to establish specific due diligence procedures to screen out risky persons who could become owners or managers of insurance companies engaged in VA or VASP activities, which the assessment team considered reasonable in proportion to a sector already regarded as low risk in terms of overall AML/CTF and of low appetite for VAs.

DNFBP Supervisors

ASPs

428. The assessors concur with Moneyval's observation that all ASP supervisors apply market entry measures. Moneyval found that ICPAC applies comprehensive controls with respect to licensing, which prevent criminals from holding, being beneficial owners of, holding management functions, or acquiring a significant or controlling interest in an ASP. CySEC's procedures have already identified the stage in the existing authorization process where VA activity may be detected. ICPAC has begun measuring VA activity levels through substantial targeted data collection and metrics, and addresses VA AML/CFT measures directly in its AML/CFT Directive. The CBA is in the process of collecting data on VA activity and setting procedures, through a revised questionnaire, and in providing guidance through its revised AML directive.

429. While Moneyval observed one major vulnerability comes from the lack of a routine information exchange among the three supervisors on rejected applications and withdrawn licenses, and the lack of a unified communication platform for such information sharing, supervisors reported, that exchange of information has been more systematic in the past two years, and have taken extra steps to identify applicants who have been licensed by another supervisor. The assessors note the importance of such continued cooperation because the VA space has seen actors seeking to exploit regulatory arbitrage in its early years as global regulatory developments emerged with different approaches across jurisdictions and/or supervisors within the same jurisdiction.

430. It was reported to the assessment team that all three supervisors have exchanged correspondence on the matter during 2020. Furthermore, CySEC publishes any rejections, withdrawals in its website. Furthermore, it should be noted that moving from one regulator to another is not a simple process due to the qualifying criteria relating to the beneficial ownership structure requirements ICPAC and CBA have. CBA for example requires an ownership of 100% qualified lawyers prior to issuing a license and ICPAC requires an ownership of over 50% ownership and control over the board. As a result, for example, a firm licensed by ICPAC would appear unlikely to be eligible to apply to obtain a license from the CBA and vice versa.

431. Regarding BOs, ASPs are obliged to hold adequate, accurate, and current BO information, which is of particular importance with regard to foreign clients. This includes BOs' countries of residence, as well as customers' countries of incorporation (for legal entities), business activities, and total flows in and out of their bank accounts. Due to their role setting up Cyprus companies (usually private limited companies) that are ultimately owned and controlled by non-resident BOs outside of Cyprus, and acting as shareholders & directors on behalf of them, it is imperative that ASPs ensure transparency for all legal persons involved. The same applies for their administration and management of trusts.

432. Moneyval observed that while the overall ASP regulatory and supervisory framework has improved, raising the quality of BO information maintained, there still remained areas in need of improvement. For instance, there was no comprehensive method to verify that all ASPs serving foreign clients were adequately licensed in Cyprus as required by the law. However, there are a number of ways unlicensed ASPs are identified by supervisors as follows:

- Reports to supervisors by competitors when they identify unlicensed entities offering such services.
- When an entity or legal arrangement wants to open a bank account, the financial institution will, as part of its due diligence work, request evidence of the service providers license issued by a supervising authority and hence will identify the unlicensed professional.
- During the on-site monitoring performed by the supervisors, there have been cases where unlicensed professionals have been identified as operating without the appropriate license and have been referred to the relevant licensing department of the supervisor
- Through the monitoring of media and other publications
- Written complaints submitted by the general public directly to each supervisor, complaining of professionals they think should be supervised by said supervisor.

According to the OECD, the Cyprus authorities noted that should an unlicensed person or entity try to perform any of the services subject to license, competitors would immediately notice and report them to the supervisor. Other venues for identifying unlicensed professionals include complaints from the general public or circumstances where an unlicensed person attempted to open a bank account on behalf of a customer, this would raise red flags and the authorities would be made aware. On-site and off-site monitoring by supervisors (including monitoring of media or specific publication) also identified cases where professionals were offering regulated services but did not hold an appropriate license.

Moreover, competent authorities' reliance on BO information maintained by ASPs in their information gathering procedures was perceived as problematic because full compliance with BO-related requirements was not uniformly met across all ASPs. Finally, concerns regarding the effectiveness of ASP supervision could point to gaps in the level of transparency of BO information.

433. These BO-related vulnerabilities are mitigated to some extent when ASP clients also hold bank accounts in Cyprus, given that Cyprus banks were found by Moneyval as well as the

assessment team to adequately adhere to BO-related requirements. These bank accounts serve as an additional layer of defense. However, banks in Cyprus have shown reluctance toward serving VA activities, and the adoption of the AFL/CFT Bill would not necessarily change this stance. Therefore, for envisioned ASP clients engaging in VA activities, there may not be bank accounts in Cyprus whose screening is de facto an additional layer of defense.

CBA

434. The Cyprus Bar Association (CBA) is supervised by the Attorney-General and functions as competent authority for the professional activities of over 4,000 registered practicing advocates in Cyprus. It should be noted, that the CBA is established officially, meaning that it operates based on a statute rather than merely based on private articles of association. Therefore, a parliamentary decision is required in order to amend any procedures, which decreases the flexibility to make such amendments.

The CBA operates as both a regulatory and professional body for members under its supervision, which include lawyers, companies of lawyers (LLC), certain partnerships and LLCs owned 100% directly or indirectly by lawyers (ASPs), and other trusts and administrative services. A firm that belongs exclusively to advocates and/or LLCs may apply for a license as an ASP issued by the CBA on the basis of the Administrative Service Providers Directive. The CBA issues directives, guidelines and circulars and provides training seminars.

435. Approximately 76% of ASPs fall under CBA supervision, which represents a significantly larger portion than those under CySEC or ICPAC oversight. The CBA maintains registries for ASPs and Trusts. As of November 23, 2020, 1318 ASPs were shown listed on CBA's ASP registry.

436. Both Moneyval and the 2018 Cyprus National Risk Assessment detected several weaknesses in the CBA's controls. However, the CBA reported to the assessment team that it has complied with Moneyval's recommendations to a significant extent by revising and ameliorating such controls as follows. CBA also reported that since the Moneyval evaluation, the CBA's onsite inspections have materially increased both qualitatively and quantitatively. CBA is also in process of reviewing and enriching the current AML Questionnaire, aiming to receive more information from the regulated entities which will lead to more effective monitoring and supervision. Through the amendment, the AML Department aims to receive more information from the regulated entities in key topics such as the source of funds and source of wealth, risk assessment, PEPs, internal procedures, exposure to high risk and/or sanction list jurisdictions etc.

ICPAC

437. ICPAC is the only body of accountants recognized by the Council of Ministers and operates as the competent authority for licensing of auditors and audit firms, as well as monitoring its members under the ASL Law and AML/CFT Law. ICPAC oversees 333 ASPs

representing approximately 16%. Moneyval found that all persons in receipt of licenses from ICPAC had been subject to comprehensive suitability checks prior to licensing so as to prevent criminals from holding, or being a beneficial owner of, a significant or controlling interest or holding a management function in ASP.

438. A firm applying for a license under ICPAC supervision has to complete a number of fit and proper criteria. This includes verifying the identity and background of the applicants, confirming their professional competence, assessing their ethical behaviour and their financial stability. The licensing process involves the completion of an application form requesting financial, ownership and management information. It is noted that ICPAC has specific ownership criteria which requires licenses to be granted only to companies owned by qualified accountants by more than 50%. Furthermore, ICPAC requests a clear criminal record for all members, reference letters from two other qualified members and confirmation from the professional accounting body of which the applicant is a member of e.g. the ACCA. Finally, ICPAC renews the license of each firm on an annual basis, confirming the validity of the license.
439. ICPAC also requires that registered entities fill out an annual AML questionnaire. ICPAC has been collecting data on VA activities as part of this questionnaire. The assessment team considers the data collected on VA activity from the questionnaire will be relevant for establishing controls.

CySEC

440. CySEC is responsible for supervising firms offering administrative services which do not fall under ICPAC or CBA supervision. The majority of ASPs fall outside of CySEC's oversight. Approximately 8% of all ASPs are licensed and supervised by CySEC. With regard to ASP controls for registration and licensing, CySEC's procedures along with ICPAC's procedures were recognized by Moneyval as the most rigorous and effective in preventing criminals and their associates from attaining decision making roles. Due to the thorough due diligence measures applied prior to authorization of licenses, ASPs under CySEC were found less likely to pose VA/VASP AML/CFT risks.
441. CySEC's procedures for authorization of investment firms and other CySEC supervised entities consist of two steps, first shareholder due diligence, followed by a business model and organizational structure assessment. Under the legal framework applicable to ASPs, ASPs undergo only the first step. Due diligence procedures ensure shareholders' good reputation, no engagement in criminal activities, and an adequate source of funds. ASPs supervised by CySEC are mostly owned by natural persons, often with 1-2 shareholders, according to CySEC. CySEC requires information from the entire shareholder structure, including direct shareholders and intermediate entities if applicable, and tracing back to the UBOs. The process involves a questionnaire, KYC assessments utilizing both specialized software and web searches, and references from any other Cyprus, EU, and non-EU competent authorities supervising the applicant. Source of funds investigations, especially for first time authorizations, ensure the initial capital injection derives from legitimate funds that are sufficient to support operations

for at least 3 years. CySEC requires supporting documentation such as tax returns, bank confirmation letters, and audited financial statements for legal entities. These due diligence measures are also applied for approval of changes in control structure, shareholding structure, and license extensions.

442. If CySEC is satisfied with the appropriateness of shareholders, the application is presented to the CySEC Board for pre-approval. Any information that may dispute shareholder appropriateness is listed in a memo with deficiencies and concerns to assist the Board in deciding whether proceed with the authorization or reject it. Existing legal provisions specify that license applications can be rejected upon the competent authority having doubts on the appropriateness of shareholders, such as concerns on their financial soundness or good reputation. These provisions apply, in full, to ASPs under CYSEC's oversight.

Casino Commission

443. The Casino Commission, established in 2017 and operational in January 2018, is tasked with assessing applications, granting licenses for casino operations. Moneyval found that the Casino Commission has applied appropriate market entry measures for the Cyprus Casino. The original due diligence, which resulted in the award of the license for the ICR, was completed prior to the Casino Commission becoming operational. Upon becoming operational, the Casino Commission has established licensing and market entry provisions with respect to permissions for the satellite casinos, staff, junkets, suppliers, machinery, etc. The Casino Commission has been closely informed about the casino operator's recent hiring decisions for management positions, including an AML Officer.

444. All junket operators must obtain a license from the Casino Commission in order to operate as such, and the licensing process includes a detailed investigation of the company's beneficial owners, directors, and the suitability of operators and representatives. The assessment team found these procedures and required disclosures adequate for detecting any suspicious ties on the part of management or beneficial ownership with VA activity. Moreover, licenses for junkets can include conditional provisions that the Casino Commission can impose tailored to specific risks such as these.

445. While it is not currently envisioned that either the Casino or junkets will engage in VA activities, the market entry measures are rigorous, and the assessment team expects they would detect improper persons engaging with VA in that sphere.

National Betting Authority

446. The NBA's role includes examining applications, licensing, auditing, and supervising prospective betting shops and online betting operations.

447. The NBA issues Class A (land-based betting) and Class B (online betting) licenses to bookmakers and authorized agents, and maintains a register for each category of licensees.

The NBA has clearly defined market entry due diligence measures in place for the purposes of screening management and beneficial owners. Because no VA activities have been detected as of the time of the assessment, the NBA's controls in this matter have not focused on suspicious ties on the part of management or beneficial owners to such VA activities.

6.2.2 Supervisors' understanding and identification of ML/TF risks

FI Supervisors

448. Although VA were not in scope for the Moneyval MER, the report noted that Cyprus authorities have taken actions to understand the risk of new technologies. These actions deserve particular emphasis, having resulted in issuing public warnings to obliged entities on the risks posed by the VA/VASP sector, attending training seminars to increase supervisory expertise in VA/VASPs, and other forms of ensuring preparedness to take supervisory actions with respect to these activities. In relation to VA/VASPs, supervisory authorities closely monitor international practices, in particular, taking into consideration results of the EU level supranational risk assessment, warnings issued by EU bodies (e.g. ECB, ESAs, EC, etc.) on risks posed by the VA/VASP sector, recent guidance issued by the FATF, etc.
449. The assessment team's findings are consistent with this observation. CySEC especially, given its experience supervising limited VA activity from an ML/TF perspective (but not from a prudential, investor protection or market oversight perspective) and setting controls, has demonstrated the most understanding of these risks. FI supervisors generally consider VA activities to be high risk from an ML/TF perspective.

CBC

450. The CBC regards VA ML/TF risks as high. During the assessment, major VA ML/TF risks identified by the CBC relate to onboarding and source of funds. The CBC has not had opportunities to develop direct supervisory experience that would enhance its understanding on VA-specific ML/TF risks.
451. The CBC has shown interest in enhancing its level of understanding of the ML/TF risks posed by VA, and to benchmark learnings from other jurisdictions with experience in the space. It has held some training sessions for selected staff on VA and VA AML/CFT risks, and plans to continue to do so. It also anticipates participating in VA AML training expected to be provided by EBA in 2021. Enhancing its level of understanding is essential for the CBC to acquire a level of expertise specific enough to issue effective updates to its AML/CFT Directives as well as guidance on risk mitigation with respect to VA activities.

CySEC

452. CySEC displayed the strongest understanding of all Cyprus supervisors with regard to VA ML/TF risks. CySEC's overall understanding of ML/TF risks and controls have established a solid

starting point. CySEC has authorized a limited number of firms to engage in VA activities, in most cases as an extension of their current licenses, and collaborated closely with them to set rigorous controls. Although CySEC has not been directly supervising the VA activities of these supervised firms from a prudential or market conduct perspective, it has displayed a good understanding of the ML/TF risks.³⁷

453. The Authorizations Department recognizes that its existing authorizations procedures can be adapted and implemented for VA activities, and in fact has already envisioned a methodology tailored for the space by taking applicable principles for future authorizations for VASP activity (making it “ahead of the curve”). This would consist in adapting MiFID procedures as applicable, continuing to follow ESMA guidelines for shareholder due diligence as they have already been implemented at CySEC, and embracing a new set of tools designed to trace source of funds for VAs on the blockchain.

454. The AML Department also recognizes the risk of tracing the source of funds, as among the most difficult challenge in transactions involving VAs. It also understands that there are clear risk mitigation measures among its existing procedures (e.g. written policies, included in applications and in supervision standards) that, for instance, supervised VASP and VASP-like entities can apply as preventive or mitigating measures. There is an understanding that as these activities pose novel products and services with particular risks, and that thus further amendments are being considered for the operational directive as well as the registration directive. Examples of other EU countries are being considered.

ICCS

455. Due to the small size of the insurance sector and its assessment of AML risks, the Superintendent of Insurance does not have an AML-specific department, but it does evince a detailed understand of how overall ML risks would pertain to its sector. The two staff responsible for AML also deal with other aspects of supervision and have a holistic knowledge of the companies supervised. Life insurance is under the scope of the AML law, which sets clear stipulations. ICCS has not, however, demonstrated any particular or specialized understanding of ML/TF risks of VA/VASPs, however the assessment team did not find any deficiency in light of the lack of existing or reasonably foreseeable VA activity in this sector.

DNFBP Supervisors

ASPs – Summary

456. Moneyval noted that ASP supervisors demonstrate a suitable understanding of the overall ML risks in this sector, although understanding of TF risks is less sophisticated, partly in conjunction with the rare instances detected of TF activity. The three ASP supervisors are well

³⁷ CySEC is actively monitoring the CIFs that are engaged in VA activities. In addition, Circular [C417](#) has been published in order to facilitate and offer guidelines on the prudential treatment of VAs.

aware of the 2018 Cyprus National Risk Assessment and Moneyval findings, which rated the ASP sector as medium-high risk and identified it as having the second highest potential threat of being used for ML, after the banking sector. Therefore, all three ASP supervisors have a similar overall risk assessment of the ASP sector.

457. There is general awareness on the part of ASP supervisors that non-resident owned or controlled legal entities pose the highest AML risk, and that providing administrative services to a largely international clientele make ASPs a particularly risky sector. Besides ASPs being risky for the nature of their operations, all ASP regulators also fully acknowledged that having three separate regulators without fully harmonized procedures creates additional risk and potential gaps. In this context, fragmentation and variability in size of ASPs also heightens their risk, with the smallest and less well-resourced ASPs being the riskiest. The potential impact of these risks are significant because ASPs represent a substantial sector of the Cyprus economy.

458. The assessment team found that the general approach taken by ASP supervisors to VA risks for ASPs has been to apply overall ML/TF understanding to this emerging space and how it may pose ML/TF risks. While VA are generally considered to represent high risk, there are divergent levels of understanding by the respective ASP supervisors regarding the specifics of these risks. There have also been varying levels of experience and training regarding ML/TF risks of VAs that might form the foundation of understandings regarding risk for ASPs serving clients engaging in these activities.

459. The assessment team found that CySEC demonstrated thorough understanding of VA-specific risks, having both established and envisioned additional risk assessment procedures and metrics for this space. It also has utilized effectively the experience drawn from other areas of CySEC oversight, as a very small number of CySEC-regulated firms are already engaging in limited VA activities (although those activities are not directly supervised in all respects, as discussed elsewhere in this report). ICPAC through its data collection and establishment of relevant metrics measures VA activity at a high level, which demonstrates its awareness of VA-specific risks. ICPAC has issued an AML/CFT Directive that directly addresses specific VA risks and mitigants. The CBA is in the process of collecting VA-related data and preparing guidance. The assessment team thus found a disparity in level of familiarity and understanding among the three ASP supervisors, which can lead to gaps if the current knowledge gaps are not filled.

460. The assessment team also found that once the AML/CFT Bill is enacted, all three supervisors expect to subsequently draft directives or guidance (or, in the case of ICPAC, further directive or guidance) applicable to ASPs and VAs/VASPs ML/TF risks.

CBA

461. The CBA is aware of overall ML/TF risks in Cyprus as they relate to ASPs, both domestically and from international sources. Due to Cyprus being a small country combined with factors that make it an attractive destination for foreign investment, the CBA recognizes that ML risks coming from international sources are of much greater scale. It demonstrated

awareness of Cyprus being used as an international route of moving funds for the purposes of ML/TF. Hence CBA is aware the existing risks from international movements of illicit funds are applicable for Cyprus ASP services offered to both domestic, and mostly international, clients engaging in VA activities. In accordance with the Moneyval and 2018 NRA assessments, the CBA also clearly recognizes the potential disparities caused by having three separate ASP supervisors.

462. Some ASPs engaging in VA activities may function as legal advisors to VA VASPs, which entails providing advice in relation to the law, and is considered by CBA a low risk activity from an ML/TF perspective. The assessment team concurs with this view.
463. Second, ASPs may provide corporate and administrative services to VASPs. This may involve providing corporate directors, trustee services, corporate secretary services, registered office services, etc., leading to direct involvement in a client company and personal responsibility for any criminal violations including ML activities. For instance, when acting as a director for a client dealing in VAs, if an ASP has not done proper due diligence or does not properly understand the risks of these transactions, it will be difficult to comply with AML/CFT obligations. The CBA considers the main VA-related ML/TF risks in relation to the ASP sector would be in this context, where an ASP would provide services to clients which are obliged to comply with the AML law.
464. To date, the CBA had observed only a small number of ASPs involved in low risk legal advisory capacity with respect for clients engaged in VA activities. This observation came from anecdotal experience and no systematic statistics are gathered to measure the extent of such activity. Nevertheless, CBA supervisory staff conducting inspections on ASPs have been trained recently on VA activities and VASPs so as to increase awareness on the specifics of how these risks are manifested in specific scenarios.
465. In order to ensure proper safeguards are taken to reduce the ML/TF risks posed by VA activities in the context of ASP services, the CBA has recognized the need to start by verifying the level of understanding and awareness of VA and VASP activities, both among their own staff and among its member entities. A questionnaire for member entities or similar investigation tool would be envisioned to conduct this verification, and the CBA has reviewed and begun to enrich the current AML Questionnaire accordingly.
466. The CBA reported to the assessment team that its staff is being trained on how VAs could be exploited for ML, and has been planning the relevant procedures to implement in order to address concerns regarding the risks by offering relevant guidance. The CBA has not yet issued warnings on these risks or provided guidance.

ICPAC

467. ICPAC's 2020 AML/CFT Directive already addresses key areas of VA ML/TF risks, including EDD and TF red flags. Moreover, during the field interviews, the assessors also found

a thorough level of understanding of overall ML/TF risks. There is good understanding, which was communicated in the Moneyval report and in the 2018 National Risk Assessment, that the focus of risk of ASPs arises from the recognition of lower levels of transparency regarding beneficial owners, international operations involving investors, links to foreign companies and entities, and complex or deliberately complex corporate structures.

468. Data Collection on VA/VASPs: ICPAC already collects data on whether supervised entities accept or make payments in VAs, and whether they have any clients engaging in such activities. This provides ICPAC with an evidence-based foundation as well as a baseline. The few positive responses ICPAC has received, which pertain to entities with clients engaging in VA activities, are believed by ICPAC to relate to auditors serving such clients and not ASPs. For 2018 and 2019, ICPAC noted that 4 ASPs allow the use of cryptocurrencies as a means of payment from, and/or to their customers. Among these ASPs, 5 and 3 recorded clients involved in holding or mining cryptocurrencies, or engaging in Initial Coin Offerings in 2018 and 2019 respectively, and in each case the number of such clients was less than 10. Over time, as the level of activity for VAs is expected to rise with the onset of the regulated framework, the metrics collected by ICPAC, in combination with adequate training and guidance, will serve ICPAC well in recognizing the scale and riskiness of VA activity.

469. The data collection regarding involvement in VAs on the part of supervised entities and their clients, obtained from the annual offsite evaluation questionnaire, and the fact that this data is taken into account when ICPAC conducts onsite visits, shows a positive level of awareness on this activity, and also awareness of risks specific to VAs.

CySEC

470. CySEC demonstrated a thorough understanding of the ML/TF risks as they relate to VAs in the context of ASP services, considering both VA activities as high risk and ASP services as medium-high risk. Across the board, the main concern regarding VA activities is the AML risk they would represent (e.g. source of funds, beneficial owners, mixers/tumblers, privacy coins that can't be traced). CySEC understands that ASPs could potentially be a target for international funds flowing into Cyprus using VAs, given the existing challenges with international business structures and source of funds at level of BO/UBO or intermediate companies. CySEC reports that it implements a very strict interpretation of the AML law and directive in order to require firms to present a strong economic profile for BO which included source of funds. There is also awareness of the potential for regulatory arbitrage among ASPs supervised by three separate supervisors, although the criteria for qualifying to be supervised by CBA or ICPAC limit this. CySEC observed that reporting of suspicious activity through STRs may go directly to MOKAS from companies, so CySEC may not be fully aware of certain suspicious activity unless informed by MOKAS.

471. CySEC are aware that staffing constraints may hinder the effectiveness of CySEC's AML controls, particularly if resources do not increase commensurate with the growth of the sector once the new regulatory framework is in place.

Casino Commission

472. The Casino Commission now includes experienced AML staff, who have dedicated significant attention to the matter of AML/CFT measures. The Casino Commission issued an AML/CFT Directive in November 2019 that sets forth a risk-based approach for ML/TF. The Directive addresses ML/TF risks in broad aspects of internal controls, the role of AMLCO, internal audit, ongoing monitoring, record keeping, suspicious activities and reporting, reliance on third parties, and the need for adequate education and training of employees. It also addresses CDD for applications, customer relationships, business to business relationships including junkets, identification and verification for natural persons, legal entities, and unincorporated businesses, simplified and enhanced due diligence.
473. The Casino Commission understands that the casino in Cyprus does not support VA activity, and considers VA ML/TF risks arising from it to be very low or non-existent at this time. The assessors found no evidence of direct ML/TF risk for VA because casino operations do not accept such assets for customer buy in, or for any other form of use, and there did not appear to be ways of circumventing these restrictions to introduce VA directly or indirectly into the Casino. Customers generally use cash or cards for buy ins, or make fund transfers, with transactions going through the Cyprus banking system and point-of-sale systems accepting credit cards. Moreover, there is no infrastructure to support any form of VA transactions. In light of the novelty of this matter and due to the fact that it is not an apparent risk, the Casino Commission has not issued guidance for preventive measures in this respect and its AML/CFT Directive does not specifically cover VA ML/TF risks or processes.
474. The Casino Commission demonstrated understanding of the potential risks of junkets, and reasons why they do not appear to pose VA ML/TF risk. Junkets are not obliged entities under Cyprus AML legislation. Junkets are generally foreign entities registering as Cyprus businesses in order to obtain a license from the Casino Commission. Junket licenses can include conditional provisions defined by the Casino Commission if it considers additional measures appropriate upon due diligence findings. Any AML requirements pertaining to junkets would be established by the Casino Commission. The Casino Commission recognizes that there are risks arising from junkets originating from higher risk jurisdictions. The Casino, rather than the Casino Commission, has primary responsibility for ensuring AML/CFT compliance in connection with activities of junket organizers, while junket operators are responsible for complying with conditions of their licenses.
475. A critical mitigant at the moment is that junket operators are not authorized by license condition to transfer funds on behalf of customers – junket customers must introduce funds through the same channels as other casino customers, and are subject to the same controls and limitations, including due diligence performed by the casino. With respect to VA, the assessors find that adequate source of funds investigations, and procedures to trace funds to the UBO, can reasonably be expected to mitigate the indirect risk of VA arising from the use of junkets. At the moment, given the casino's fiat-based infrastructure, reliance on the banking system,

and safeguards established by the Casino Commission discussed in the section below, this risk does not seem apparent or pressing.

476. The assessment team considered whether any potential vulnerability could arise from the fact that the parent company behind the casino manages a portfolio of integrated casinos in Macau and the Philippines, which fall outside the supervisory oversight of the Casino Commission. The Casino states that it does not permit chips or casino credits obtained at affiliated casinos to be deployed or redeemed in Cyprus, and the assessment team understands that if it were to desire to do so it would need to seek permission from the Casino Commission.

National Betting Authority

477. While the NBA was established legally in 2012, it is still a relatively new authority with the first employee hires having taken place in 2019. Yet the NBA demonstrated to the assessment team a broad understanding of both overall AML/CFT risks, and a very proactive stance to enhance its understanding of these risks as they relate to VA activities. At the time of the assessment, the NBA was still currently training and developing its AML/CFT unit, as well as building an automated betting monitoring system with alerts sent directly from betting platforms to the NBA. This level of transparency and visibility could reasonably be expected to greatly enhance its understanding of AML/CFT risks. This system could also be very effective in providing understanding of relevant ML/TF risks if VA activities were to arise, as long as there are mechanisms in the system for recording and tracking VA activities. At present no specific VA-related elements are planned or expected.

478. The NBA is also responsible for adopting AML/CFT measures and issuing relevant directives. The NBA advised the assessment team that it had prepared a draft of a secondary legislation in the form of an AML/CFT Directive as a response to the recommendations established by the 2018 Cyprus National Risk Assessment. However, this was not made available to the assessment team so it was not possible to evaluate it or include it in this assessment.

479. The NBA also informed the assessment team of plans to undergo a consultation with industry participants in or about October 2020 with respect to the draft AML Directive prior to being finalized, with the intention to be ready to enact as soon as the Cyprus AML primary legislation is finalized. However, the assessment team was not advised of or provided with any such consultation, nor has it been indicated on the NBA web site.³⁸

480. Currently the NBA's belief is that there are no VAs being accepted or paid in the betting sector. This lends itself to a baseline of zero regarding risk at the moment. Moreover, to further minimize the ML/TF risks that could arise from VA activities, the NBA does not permit licensed firms to accept VA as a means to place bets or fund accounts.

³⁸ Last visited 12 December, 2020

481. The NBA has begun a collaboration with the University of Nicosia, which is currently conducting a risk assessment on non-fiat forms of betting payment under a range of potential scenarios. At the time of this assessment the UNIC risk assessment had not been completed and thus could not be considered by the assessment team.

6.2.3 Risk-based supervision of compliance with AML/CFT requirements

FI Supervisors

482. Risk based supervision of compliance with AML/CFT requirements has been widely adopted by Cyprus FI and VASP supervisors. In practice, only CySEC has actual experience applying this to VA activities or firms engaged in VASP-like activities. The assessment team considered the risk-based methodologies of other supervisors to identify any evident gaps with respect to VA, however its principal focus was on risk-based supervision and monitoring of VA/VASP AML/CFT by CySEC.

CBC

483. The CBC has no direct supervisory experience with either VASPs or other CBC-supervised entities engaging in VA activities or providing services to VASPs or VA customers. The CBC believes, and the assessment team found no evidence to the contrary, that no CBC-supervised entity is engaging in VA activities or knowingly providing services to customers engaged in VA activities. Supervised entities are required to disclose any high risk business they engage in, and must obtain approval from the CBC prior to engaging in new activities or services, thus any initiative to commence VA activities by a supervised entity would be expected to be brought to the CBC's attention and reviewed carefully for risks and controls prior to moving forward. However, CBC written supervisory procedures and reporting templates do not currently refer expressly to VA (or classify VA activities as high risk from an AML/CFT or prudential perspective) nor do they provide specifically for collection of VA metrics or data.

484. Generally, as found by Moneyval, CBC takes strict measures to avoid any AML/CFT weaknesses. There is zero tolerance toward anonymous accounts or transactions, which can be seen as an element of its caution toward VA activities. The CBC's approach to VA is highly cautious. CBC has not encouraged supervised entities to engage in VA activities or attempted to promote innovation in VA. It may be observed that CBC has more pressing priorities, including the COVID pandemic, impact and response; historical AML weaknesses in the banking sector and negative perceptions of Cyprus resulting therefrom that CBC has worked hard to combat (successfully, per Moneyval's findings); non-performing loans in the banking sector; as well as the weaknesses in the Cyprus Investment Programme disclosed as part of the "Cyprus Papers" scandal; and of course the aftermath of the 2013 Cyprus banking crisis. In 2014 CBC published an advisory with respect to the risks of VA, though the risks identified did not include or focus on AML/CFT risks.

485. The assessment team found a widespread perception, across industry as well as other governmental and supervisory authorities, that VA activities are banned by the CBC, as well as a degree of inability even within the CBC to state definitely whether that was actually the case. After a number of meetings and inquiries, the assessors found the CBC has no official policy against licensing or authorizing its regulated entities to service VASP customers or engage in VA activities themselves, nor does it consider there to be a legal basis for declining to do so. Ultimately the assessment team found that there is a very strict risk-based analysis of controls around any proposed VA activity, and in practice none have been sufficiently fashioned to withstand the scrutiny from the CBC to gain approval.
486. For instance, within the six months prior to the assessment interview, a PSP interested in applying for licensing to offer VA services, after considering the CBC's enumeration of the risks, did not proceed with the application. Neither did a previous entity interested in licensing for the purposes of minting bitcoins for shipment abroad proceed with the authorization of its venture. The CBC informed the assessment team of one EMI approached by a VA exchange seeking to open an account, that engaged with CBC to review this activity before proceeding. This was not implemented due to concerns regarding the VA exchange's customer due diligence procedures. Finally, the assessors separately observed a CySEC supervised entity that had initiated discussion with the CBC to obtain an EMI license to do business with VA and reported to the assessors a strong level of discouragement from proceeding with an application and has not moved forward.
487. While CBC recognizes that it will be necessary to update its AML/CFT Directives to cover VA after the AML/CFT Law is amended, it does not appear to the assessment team to be planning or readying itself for supervision of increased VA activities that would bring increased AML/CFT risks. The assessment team found that CBC has not forecast or planned for an increase of supervised activity or increased monitoring after the AML/CFT Law is amended, nor has it determined, allocated or prepared resources in the event VA activity under its remit were to increase.
488. The CBC has 3 supervision teams: the AML team (under the Banking Operations Division), the prudential supervision team for banks, and the prudential supervision team for non-bank financial institutions including EMIs and PSPs (both under the Supervision Division). For banks, the European Central Bank is the primary prudential supervisor for major banks under the EU SSM, and the CBC is the primary prudential supervisor for less significant banks which fall indirectly under the EU SSM, as well as branches from non-EU banks. In recent years, both the ECB and the EBA have extended their functions to set up an AML section and expand information exchange between prudential and AML supervisors, in order to support this objective. During the period of the assessment, the CBC AML function underwent a partial reorganization, removing it from the Supervision section and placing it under the Banking Operations Division. The Assessment team understands that this was unrelated to any anticipated or potential rise in or other development related to VA activity.

489. EMIs and PSPs are supervised by CBC with regard to both AML/CFT and prudential aspects. PSPs offer 8 categories of services under the PSD2 law, including money service businesses. PSPs cannot issue e-money, but EMIs under EMI legislation can offer various services and can use payment services in their business. EMIs are required to provide the CBC with robust monthly and annual statistics.
490. For any supervised entities engaging in VA activities, the CBC would expect them to apply their existing AML/CFT procedures. The AML/CFT manual also requires regulated entities to perform client risk categorizations, under which VASP customers could be treated like any other high-risk customer type.
491. The CBC perceives that, out of its supervised entity categories, EMIs may be the most likely and open to serving VASPs. Given the difficulties VASPs encounter in accessing banking services, they may seek EMI services or apply for EMI licenses themselves. EMIs currently do not formally need permission from the CBC to onboard VA exchanges as customers. The CBC's AML/CFT Directive requirements and principles of Know Your Customer and Know Your Customer's Customer would apply.
492. Under the authority of PSD2 as transposed into Cyprus law, the CBC has also exercised its authority to decline the approval of "hybrid" business models that offer both regulated and unregulated services. In this respect the CBC has legal authority to require regulated entities seeking to engage in VA activities to separate their lines of business through two separate legal entities. In practice this is likely to push any VA activity by a CBC supervised PSD2 entity outside the CBC's regulatory perimeter into a non-CBC-regulated affiliate.
493. CBC has taken the position that VA kiosks, also referred to as VA ATMs, are outside its jurisdiction, leaving a potential supervisory gap. The CBC views VA ATMs as falling outside the scope of its licensing because they involve an "exchange" between VAs and fiat currencies, while typical ATMs under the CBC's oversight and jurisdiction involve accessing funds in a payment account. When an entity interested in setting up a bitcoin ATM met with the CBC regarding potential licensing, it was advised that the CBC has determined that it had no regulatory authority for such activity, as typical ATMs are regulated under PSD2 but VA ATMs are not. This regulatory gap should be rectified through Cyprus assigning responsibility for VA kiosks/ATMs to a competent authority supervisor.
494. CBC AML supervision is conditional upon entities having a physical presence in Cyprus, such as a branch or a Cyprus-domiciled legal entity. It has limited to no visibility over passported entities offering services with no physical or legal entity presence in Cyprus. Although EU-wide discussions are reportedly underway that may eventually allow the CBC to collect statistics from foreign passported firms currently operating in Cyprus, under the oversight of their respective home supervisors, these have not been realized. This represents an important vulnerability at an EU-wide level, particularly with respect to VA activities whose core operations unfold within online platforms. Unregulated and unsupervised VA activity may arise in Cyprus through this channel, potentially undetected as well.

495. While the CBC expects to detect and monitor VA activity arising among its supervised entities by means of its mandatory supervision reports and questionnaires required as part of the licensing process for new entities, the assessors found gaps in relation to measuring VA activities. CBC supervision currently does not collect any data or metrics on whether or to what extent regulated entities are servicing the VA sector, although this data could be included in the KYC and economic profile of customers and their transaction monitoring activity. Under the AML Policy, firms must disclose the amount of high-risk business they process (e.g. metrics on risk profile distributions, geographic distribution, and other data on clients). However there is not an explicit section for VAs and it is recommended that this be expressly included.³⁹

CySEC

496. CySEC has developed effective supervisory procedures to mitigate AML risks posed by VA activities and firms engaging in VASP-like activities. CySEC's experience with the limited number of firms authorized to date to engage in VA activities have also served as a pilot to prepare CySEC for more extensive supervision and monitoring once the amended AML/CFT Law is enacted, the VASP registration framework is put in place and VA activities under CySEC's oversight are expected to increase. The procedures CySEC has developed to supervise VA activities are integrated with the existing supervisory framework regulated entities, which sets high standards for AML controls. CySEC is already collecting relevant data on VA activity.

497. CySEC provided data to the assessment team with regard to VA activity by certain of its regulated entities, which enabled the assessment team to develop an understanding of the relatively low level of such activity; however this data has been redacted from this report at CySEC's request due to confidentiality and sensitivity considerations.

498. CySEC is tasked with responsibility for carrying out investigations, entering and inspecting supervised entities' physical premises, and sharing findings with foreign regulators. It has a designated Supervision Department tasked with monitoring compliance as well as educating of supervised entities on AML, capital adequacy, and compliance with any relevant new legislation. The supervisory role conducts onsite and offsite inspections for medium/high to high risk CIFs. Although none have arisen with respect to VA activities, any cases where further investigation is required would be raised to the Investigations Department, which would

³⁹ The CBC should update its templates for reporting by regulated entities, including enumerating risk factors that take VA into consideration. Under AML Policy, firms must disclose how much high risk business they process (e.g. metrics collected on profile distribution, geographic distribution, and other data on clients, but no VA section). There is no data collected on whether banks are servicing VA clients, and no evidence-based baseline. VA activity, for instance, should be included as a pre-populated template category under the high-risk business disclosures required from obliged entities under the CBC's AML policy, which will also assist the CBC to start collecting data on whether and to what extent its regulated entities service the VA sector.

collaborate closely with the AML Department. If needed CySEC can draw on outsourced resources using private sector entities.

499. The Risk and Statistics Department has developed a Risk Based Supervision Framework ('RBSF') to set procedures to standardize inspections and the collection of metrics. RBSF incorporates FATF guidelines and requirements of AMLD4, focusing on areas and entities with the highest ML/TF risks and allocating resources accordingly (it is expected to be updated to apply AMLD5 once that is transposed into Cyprus law by enactment of the AML/CFT Bill). All CySEC-supervised firms are subject to the RBSF. The AML Department is responsible for supervising with respect to AML/CFT requirements and collaborates closely with the Supervision Department. RBSF is applied to Cyprus firms, and not passported firms from other EU jurisdictions. VA activities cannot currently be passported, which prevents them from arising outside the scope of CySEC's jurisdiction. A cross border risk is considered by CySEC when a supervised entity by the CySEC provides cross border activities. However, if VASPs registered or licensed in other EU jurisdictions (e.g. they are not entities supervised by CySEC) are able to passport into Cyprus under the amended AML/CFT Law, such firms could potentially operate outside the RBSF framework.
500. With the adoption of the new supervision framework, the AML Department has adopted a targeted methodology where it determines risk scoring and provides categorizations under the revised control framework. The assessors found that CySEC's AML Department has incorporated rigorous controls to ensure compliance.
501. Moneyval had observed that the risk data collected by CySEC could be enhanced to be more detailed and refined. In 2019, a revised risk evaluation approach was implemented by the Risk & Statistics department, and in 2020 it was adopted by the AML department. The improved framework, which measures Impact, Inherent Risk, and AML Controls for supervised entities, also includes new questions to measure VA activities of supervised entities. The latter section was included in the previous RBSF after the 2018 gap analysis was completed.
502. With respect to VAs, under "Inherent Risk" measurements, there are two questions related to VA activity.
- The first question asks whether the supervised entity offers complex products or services that allow VA uses, either directly or indirectly ("Complexity" - product mix and crypto funding). This is a risk measure that is incorporated into the overall CySEC RBSF model. The second question, regarding the category of "Value and size of product," asks to what extent a supervised entity would allow the use of VA as a method of payment to and/or from clients. Entities that respond "yes" would receive a higher risk scoring and closer monitoring and may be subject to further investigative actions if this activity expands.
503. In conjunction with the overall RBSF revisions, the new AML methodology now incorporates 7 AML internal controls for CIFs that include:
- AML policies and procedures,
 - AML officer suitability and competence,

- effectiveness of internal auditor on AML issues,
- AML monitoring activities,
- Staff training,
- Board involvement in AML, and
- Risk based approach.

504. Ratings for each control are scored numerically and classified as

- Weak
- Needs Improvement
- Acceptable
- Strong

505. AML quantitative risk measures are calculated through applying point scorings to the 7 controls categories.

506. The AML department uses a confidential staff handbook (AML Procedures Manual) that explains how to assess and weight these items and ensures clear standards and consistency across firms and examinations. This AML Procedures Manual guides officers to perform the same tests across these items for each firm, promoting consistency. The AML Department sends its final ratings to the Risk & Statistics department to be included in the overall RBSF results.

507. The cycle for examining firms is based on their risk profile. After Moneyval's evaluation, CySEC subsequently increased its amount inspections as part of an internal initiative to evaluate all high-risk companies at least once or twice a year. Medium to high risk companies have a 5-year inspection cycle, medium to low risk companies have close to a 7-year inspection cycle, and low risk companies have an ad hoc inspection cycle that depends on information gathered about them and whether they are added to CySEC's audit program.

508. One additional tool used by CySEC is an AML Questionnaire. CySEC's monthly AML questionnaire requiring supervised entities to report cash transactions above €10,000 could also be applied for VA transactions. The typologies for cash transactions from the internal handbook are also being considered by CySEC for adjustment and adoption for VA.

509. Both the 2018 National Risk Assessment and Moneyval observed that CySEC's limited amount of human resources hindered the effectiveness of supervision because the number of on-site inspections was deemed to be low. The introduction of VASPs as CySEC-regulated entities in 2021 can be expected to place additional demands on the CySEC AML unit. The assessment team anticipates this would require additional resources for training and staffing; stretching these resources too thinly could exacerbate existing vulnerabilities. CySEC has indicated, however, that it anticipates adding significant additional staff in 2021 across the organization. In addition, CySEC has begun to familiarize itself with specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools and databases, which it believes

could assist it in performing off-site supervision more efficiently as VA and VASP activities increase.

ICCS

510. The Superintendent of Insurance is able to maintain close oversight over its supervised entities due to the small size of the sector. At the time of the assessment, there were only 9 insurance undertakings under its oversight. Examinations are conducted internally by the supervision team and cover governance and other issues as well as AML. Insurance undertakings are subject to the EU's Solvency II Directive, which is based on a risk-based approach for setting capital requirements, supervisory review, and market discipline. This directive ensures consistent valuation and sets overall very strict procedures that include mandatory internal audits.
511. The current reinsurance structures establish considerable barriers to ML/TF activity. For any type of non-life insurance, there are insurance treaties with very well-known reinsurers. The marine insurance sector, for instance, is not deemed by the Superintendent of Insurance to be vulnerable to ML/TF because claims are reinsured, and reinsurers would make every effort to challenge any claims, especially when they are large. Any ML/TF activity seeking to make fictitious claims would have to go through these reinsurers. For any ML/TF activity to occur undetected, both sides of a transaction would have to be fraudulent in order to accept fictitious claims and issuances, which is regarded as very difficult to do in practice and also extremely unlikely to involve VAs.
512. The reporting requirements of Solvency II provide a detailed picture of all investments of each undertaking including funds, unit-linked funds, etc. Procedures require quarterly, semiannual, and annual reporting, with annual reports involving external auditors. Insurance companies must fill a specific form where they must include details on their investments. The Superintendent of Insurance closely reviews these reports to examine all the investments of each undertaking, in order to calculate service and capital requirements (e.g. rating, concentration) based on Solvency II. The assessment team was informed that none of these investments have shown indication of VAs.
513. Under Solvency II investments must be made based on a prudent person principle, which is understood to exclude investments in VA. The assessment team found that no undertakings have proposed to the Superintendent to make VA investments, nor are these expected in light of the conservative investment approach of insurance companies.

DNFBP Supervisors

ASPs – Summary

514. ASPs are obliged entities under the AML/CFT Law, and engage in business activities considered to be higher risk. While ASPs are supervised by the applicable one of the three

supervisors with respect to ML/TF, at the time of the assessment only ICPAC has addressed directly VA risks in its specific framework regarding AML/CFT. Other ASP supervisors have not yet issued guidance or set standards for AML/CFT compliance specific to VAs, although the assessment team received indications that they anticipate doing so after the AML/CFT Law is enacted.

515. The level of VA activity detected by ASP supervisors and ASPs themselves is minimal. This is reinforced by the data collection performed by ICPAC. The assessment team did not find any deficiency in supervising activity that is not yet taking place.
516. There exist differences in their respective risk assessment methodologies and in their level of intensity and rigor. ICPAC has been observed by Moneyval to have the most adequate level of resources allocated to AML/CFT supervision for on-site inspections, in part because they have availed themselves of outsourced resources that can be calibrated. For the CBA and CySEC, the number of on-site inspections were considered very low by Moneyval. The CBA has, however, increased significantly the number of on-site inspections ever since, but due to COVID-19 pandemic measures, has recently amended the methodology of on-site inspections to allow remote access and self-checks through questionnaires.

CBA

517. Regarding overall supervision, a team of 7 CBA employees conducts online and onsite inspections and perform supervisory functions over regulated entities on a day to day basis. Over the course of its supervisory activities, the CBA also cooperates frequently and shares information with other authorities, on a day to day basis and at various levels. This maintains open channels of communication with the other two ASP supervisors, other Cyprus supervisory authorities, members of the Advisory Authority and other entities.
518. Since 2010, the CBA has been conducting onsite visits to its regulated entities based on their risk classification: the assessment team was informed that these intervals are 1 year to 2 years for high risk entities, every 3 years for medium risk entities, and every 4-5 years for low risk entities. Since 2013, its AML/CFT Supervision Department has adopted a risk-based methodology to set specific procedures for both on-site and off-site inspections, in order to ensure regulated entities' compliance with their obligations.
519. Inspections differ in their comprehensiveness and rigor depending on the size and risk level of the supervised entity. They make use of specific checklists such as a Trust Checklist, Client Accounts Checklist, and Third Persons Checklist, none of which have yet incorporated metrics or controls for VA activity, and there is not yet a VA or VASP checklist.
520. Taking into consideration the Moneyval findings, the CBA has increased its on-site inspections. Moreover, in an effort to improve the quality of onsite inspections, the CBA hired two (2) external expert professionals in order to train, support and assist the supervisory staff. An independent certified fraud examiner (member of ACFE) accompanies the AML officers

during the onsite visits to regulated entities aiming to guide and assist them during the audit on targeted cases under examination on a need-to basis. In addition, an independent AML specialist has been hired to provide continuous training to the officers of the CBA AML Department, focusing on specific topics of the audit so as to enable the officers to identify any potential breaches of the AML law and/or regulations and/or directives. As mentioned above, due to the COVID-19 pandemic measures, the CBA has recently amended the methodology of general inspections to allow remote access and self-checks through questionnaires.

521. Looking forward to the expected context where VAs would be regulated in Cyprus, the CBA should continue to apply the newly introduced VA supervisory procedures. This could accordingly be mitigated by classifying ASPs that service VA or VASPs as high risk, and the CBA should consider adding a VA or VASP checklist as well as data collection similar to that performed by ICPAC.

522. While there is need for further improvements in its supervisory capabilities, which the CBA interviewees fully recognized, the assessors were advised that the CBA is currently taking measures to improve its supervisory controls. Measures to improve supervision, accompanied by rigorous training on AML/CFT compliance related to VA/VASPs, should be deployed for ASPs serving clients engaging in VA activities once these become regulated.

523. The CBA has reported to the assessment team that is in the process of producing guidance for member entities regarding specific VA standards in order to detect suspicious activity. It plans to establish specific VA procedures for detecting suspicious transactions involving VA during member entity inspections. It also plans to enable CBA staff to check whether member entities are performing appropriate VA activity checks by detecting suspicious transactions from these activities, conducting regular inspections, and particularly conducting inspections when suspicious activities are detected.

To date, the CBA has not provided guidance or obligation for member entities to look for patterns specific to VAs in order to detect suspicious activity. There are no VA-specific procedures to identify suspicious transactions involving VAs during inspections of member entities.

ICPAC

524. For ICPAC, both the 2018 NRA and the Moneyval assessment found no serious deficiency findings but rather suggested improvements. The assessors concur that ICPAC and other ASP supervisors should coordinate toward a more uniform approach and framework. The recommendations from the assessments were translated in to an ICPAC action plan.

525. Regarding VA activity by ASPs, ICPAC's supervision reflects its 2020 AML/CFT Directive which expressly addressed key VA ML/TF risks and mitigants, including EDD and TF red flags.

526. ICPAC was observed by Moneyval to have an adequate number of inspections to supervised entities, which places it in position with regard to supervision of ASPs serving clients engaging in VA activities. As part of its off-site monitoring procedures, ICPAC also requests basic information from all its licensed and supervised entities regarding their involvement in VAs, as well as that of their clients. This includes entities holding ASP licenses, as well as audit licenses and general practitioner licenses. ICPAC administers a yearly questionnaire that includes a question on whether these supervised entities make or accept payments in VAs, and how many of their existing clients are involved in VA activities such as trading.
527. Few supervised entities have reported making or accepting VA payments, and only a small number have reported having clients involved in the space. For 2018 and 2019, ICPAC noted that 4 ASPs allow the use of cryptocurrencies as a means of payment from, and/or to their customers. Among these ASPs, 5 and 3 recorded clients involved in holding or mining cryptocurrencies, or engaging in Initial Coin Offerings in 2018 and 2019 respectively, and in each case the number of such clients was less than 10.
528. For those entities that have reported involvement in VAs on the part of their clients, ICPAC takes into consideration whether there may be an upcoming onsite assessment scheduled, where this data is taken into account. The two questions in the questionnaire relating to VA activities, whether obliged entities use cryptocurrencies as a means of payment, and whether they have clients involved in VA activities, carry an extra risk weight which is added to the overall risk and is reflected in the risk categorization of the obliged entities that answered accordingly. The increased risk due to VA can push an obliged entity to a 'High' or 'Medium-High' categorization which is attached to a more frequent monitoring cycle. ICPAC's monitoring cycle is of 1-2 years for high risk entities, 2-4 years for medium/high risk entities, 3-5 years for medium/low risk entities, and 6 years for low risk entities. The risk weights applied to each risk factor are documented in ICPAC's Risk Based Approach Manual which is updated on an annual basis.
529. The data collected by ICPAC to date regarding VA payments on the part of supervised entities, and any VA activity on the part of their respective clients, would be relevant to setting measures to ensure compliance, conduct inspections targeted to ASPs serving clients engaging in VA activities, and monitor their effectiveness. This would logically start with VA-specific guidance once the legislation becomes enacted. ICPAC data collection does not survey whether supervised entities would use specific tracing tools to detect VA activity in their own operations or those of their counterparties or customers. However, ICPAC demonstrated a willingness to include these factors in future questionnaires if provided with further background to assess whether supervised entities could be asked for such information. They consider the state of progress to be in early stages for this sector, which will eventually unfold in the future, which is why they're currently observing it. They have not seen much activity overall in Cyprus, especially in the sectors they supervise.

530. CySEC Risk and Statistics Department RBSF incorporates FATF guidelines and requirements of AMLD4, focusing on areas and entities with the highest ML/TF risks and allocating resources accordingly. The AML Department is directly responsible for end to end examination of ASPs, determining their risk scoring, and providing categorizations under the revised control framework. Unlike investment firms under CySEC's oversight, ASPs fall outside the oversight of the Supervision Department, which carries out RBSF's procedures for prudential supervision, conduct for fair treatment of clients, and governance. Under RBSF, ASPs are evaluated by CySEC solely for AML/CFT purposes.
531. In 2019, a revised evaluation form was implemented by the statistics department, and in 2020 it was adopted by the AML department. The improved framework, which measures Impact, Inherent Risk, and AML Controls for supervised entities, includes new questions to measure VA activities of supervised entities. Hence this supervision approach is designed to apply to ASPs serving clients in the VA space, and in fact it has already begun to gather metrics on VA activities for these entities. One tool used by CySEC is an AML Questionnaire.
532. The assessors found that CySEC's AML Department has incorporated rigorous controls to ensure its own supervision procedures can uphold adequate AML/CTF standards for ASPs, including ASPs serving clients engaged in VA activities. Under "Inherent Risk" measurements, there are two questions related to VA activity as part of the supervision program. The first question asks whether the ASP under evaluation offers complex products or services that allow VA uses, either directly or indirectly ("Complexity" - product mix & crypto funding). This is a risk measure that is incorporated into the overall CySEC RBSF model. In 2019, 1 ASP responded "yes" and as such would receive a higher risk scoring and closer monitoring in this new space, and further investigative actions if this activity expands. The second question, regarding the category of "Value and size of product," asks to what extent an ASP would allow the use of VA as a method of payment to and/or from clients. All ASPs were found to answer "no."
533. In conjunction with the overall RBSF revisions, the new AML methodology now incorporates 8 AML internal controls (new control factors), plus a governance control specific to ASPs (because the AML department is the only department that supervises ASPs). The governance section is applicable for ASPs only. CySEC AML department officers in formulating their assessment of governance take into account their interviews with AML compliance officers of supervised entities.
534. There is also an internal handbook that the AML department uses in conducting onsite and offsite supervisions, whose results feed into the ratings. This confidential staff handbook (AML Procedures Manual) explains how to assess and weight these items and ensures clear standards and consistency across firms and examinations. This staff handbook guides officers to perform the same tests across these items for each client, promoting consistency. The typologies for cash transactions from the internal handbook are being considered by CySEC for adjustment and adoption for VA. The final results are inputted into CySEC's template which produces the final output, which the AML Department sends to the Risk & Statistics department to be included in the overall RBSF results.

Casino Commission

535. As a response to the concerns expressed in the Moneyval report about the risks posed by the casino, the Casino Commission has made a series of enhancements and taken noticeable steps to improve the compliance culture of the casino. These actions set important safeguards that are relevant for VA ML/TF risks as well. Hence both the direct and indirect risks of ML/TF involving VAs are significantly minimized with the existence of these safeguards.
536. The casino legislation provides for a license for a single land-based casino operator to run a largescale casino and four smaller 'satellite' casinos. From the point in which the Casino Commission became operational, the assessment team found it to have conducted thorough due diligence and rigorous procedures.
537. The Casino Commission has issued licenses to two junket operators that are not yet operational. Junket licenses can include conditional provisions defined by the Casino Commission if it considers additional measures appropriate upon due diligence findings. The assessment team understands these procedures to be rigorous and can be adequately tailored to any specific risks that may arise, including risks related to VA activity.
538. The Casino Commission's AML/CFT Directive requires the casino to submit an annual AML report, the first of which was submitted by the casino in February 2020. In December 2019, the Casino Commission also issued a reporting directive which sets reporting requirements and a format for the casino to submit regular monthly and daily reports. This Casino Regulatory Return is a monthly reporting form that the casino must submit, including specified AML data. With these measures in place, the Casino Commission has started to implement a risk-based approach to supervision, aiming to improve the quality and content of information submitted.
539. The assessors consider the Casino Commission's safeguards to be effective at minimizing the direct and most obvious ML/TF risk of VA, which could emerge from their use as buy-in; this is because VA are not accepted as a means of buy-in. The Casino Commission at this point of time is not aware of any intention and plans of the casino to start accepting VAs. Neither are VAs considered as a part of the action plan that the casino operator adopted.
540. Most importantly, accepting VAs would require notifying the Casino Commission and obtaining official permission. There is a formal procedure that for any innovative projects, the casino would have to submit a proposal for review and approval by the Casino Commission. All proposals require an AML risk assessment and measures to be put in place to address the risks. At the moment the Casino Commission will not approve of any VA projects until it can fully understand the risks and develop the capacity to supervise them with adequate controls.
541. Finally, while junkets are not obliged entities under AML legislation and not under the direct controls of the Casino Commission, the potential for risks or gaps surrounding them is

minimized through licensing. All junket operators must obtain a license from the Casino Commission in order to operate as such, which requires them to first register as businesses in Cyprus. The licensing process includes a detailed investigation of the company, its business model, beneficial owners, directors, suitability of operators and representatives, and AML policies. Applicants are asked about their intended money management expectations, so the Casino Commission would expect to be informed if they plan to use VAs over the course of this investigation. Second, junket licenses are meant to ensure that the casino subjects them to scrutiny and oversight. For each junket license, the Casino Commission can impose conditional provisions and safeguards depending on the nature of customer fund management they intend to engage in. For the two licensed junkets to date, the Casino Commission has imposed a condition that they are not allowed to manage customer funds or credit, so transactions can only occur directly between the customer and the casino. Conditions can be tailored relative to each license and the specific risks involved, restricting the types of financial transactions licensees could use. With respect to VAs, the Casino Commission will not license junkets engaging in this activity until it is confident in its supervisory capability to manage the risks. This does not appear to present meaningful VA ML/TF risk.

National Betting Authority

542. While the NBA overall is a new agency, it has demonstrated significant preparedness in supervising AML matters and has taken proactive measures to the extent that AML risks relate to VAs. The AML unit is expected to expand once the automated monitoring system is launched, producing reports that will require additional staff to analyze and operate the system. Should betting platform operators not be adequately trained or have adequate procedures to identify, report, and respond to VA risks if these were to arise through increase use of VAs, the NBA would have access to the data on their transactions through its automated system, and perform its own due diligence and procedures to mitigate these risks.
543. The NBA conducts on-site inspections, supervises licensees, and drafts and issues Directives to facilitate implementation of the legislation over time. Inspections are meant to betting activity is conducted in a legal, transparent, fair, and compliant manner with respect to the law and regulations. This entails fair practices regarding profits paid to players, taxes paid to the government, contributions paid to the NBA, and ensuring licensees remain compliant with the terms of their respective licenses. The NBA is also responsible for taking preventive measures to protect youth and vulnerable groups from potential gambling addictions.
544. The NBA conducts oversight under a matrix system that pulls people from across several departments to perform AML functions and conduct related research. Roles are still being defined overall, but the assessment team was advised that there are staff that focus exclusively on the AML unit. The NBA is still currently training and developing its AML unit, as well as building an automated betting monitoring system with alerts sent directly from betting platforms to the NBA. This level of transparency and visibility is deemed to streamline compliance processes significantly. While betting operators are responsible for monitoring transactions, the automated system provides the NBA with access to all relevant data which will

be useful in establishing further effective supervisory measures and detecting patterns or anomalies that could reflect typologies of ML/TF.

545. At the time of the assessment, the NBA does not permit licensed firms to accept VAs from any users seeking to place bets or fund their accounts. Moreover, licensed firms are required to use payment service providers, which are authorized by the Central Bank of Cyprus to fund accounts in Euros only. These measures minimize or eliminate the risk of VA activities arising, and with them the inherent ML/TF risks.

546. The NBA also reported to the assessment team that it is considering the inclusion of a cryptocurrency sandbox environment exception within its AML Directive, which it has asserted would serve the purpose of incorporating VA considerations within its data collection and reporting templates and supervisory procedures. If approved and implemented, the sandbox environment, as well as its requirements and conditions, would be delineated in a separate Directive, pending the completion of the research conducted by the University of Nicosia regarding the adoption and use of cryptocurrencies as a means of payment. Moreover, all licence applications are required to include the operator's KYC and AML policy. These have to be compliant with the national Law and cannot be amended by the operator without the NBA's prior approval.

6.2.4 Remedial actions and effective, proportionate, and dissuasive sanctions

FI Supervisors

547. To date there have been very limited VA/VASP activities in this sector, existing only in the sectors supervised by CySEC and not by any of the other supervisors. There have been no remedial actions or sanctions with respect to VA/VASP ML/TF risks applied in practice. Given the limited activity, the assessment team did not find this a deficiency.

CBC

548. The AML/CFT Law and the CBC AML/CFT Directives establish clear legal authority for the CBC to impose remedial actions and sanctions, including financial sanctions, for the purposes of preventing and combating ML/TF. CBC's AML/CFT Directives for its respective supervised entity types require updating to cover VA activities. CBC staff have indicated an intent or desire to update its AML/CFT Directives to cover VA in 2021 and it is recommended that this occur.

CySEC

549. CySEC has withdrawn licenses and issued fines of a size that made them dissuasive, as part of its overall supervisory actions. While these remedial actions have been effective, they have not yet been taken for VA activities, which for now are limited to very few entities and remain under close oversight with CySEC staff. The degree to which CySEC has collaborated

with these supervised entities to develop rigorous AML/CFT procedures for VA activity have to date deterred situations that would trigger any existing sanctions framework.

ICCS

550. To date there have been no VA/VASP activities in this sector, and there have been no remedial actions or sanctions with respect to VA/VASP ML/TF risks applied in practice.

DNFBP Supervisors

ASPs – Summary

551. The assessment team found no remedial actions applied to date by any of the supervisors with respect to VA ML/TF. Based on the principle of proportionality there is no finding of any deficiency however, given the low level of VA activity to date and the lack of a regulatory framework in advance of its adoption.

552. Moneyval found that there is also no standard platform where the supervisors could share information regarding those ASPs that have been sanctioned or undertaken other remedial actions. Establishment of such a platform with respect to sanctions applied for ASP AML/CFT and VA activities would mitigate risk of inconsistency across supervisors or regulatory arbitrage in this emerging area.

CBA

553. An area of concern identified in the 2018 Cyprus National Risk Assessment was the lack of effective, proportional, and dissuasive sanctions imposed by the CBA in cases of non-compliance on the part of supervised entities. Although the CBA had imposed sanctions to its supervised entities during the period of the Moneyval assessment, with measures to make them effective and dissuasive, the framework to impose such sanctions was limited in its effectiveness. Moneyval also noted a lack of clear criteria to determine the level of administrative sanctions based on the seriousness of a breach.

554. Based on the points from the above paragraph, the CBA has appointed a new Disciplinary Committee and has assigned different sub-groups in order to be able to proceed with simultaneous examination of disciplinary cases in a faster and more efficient manner, and has increased fines accordingly. This was done to enhance the effectiveness of the disciplinary procedures and sanctions. Furthermore, it was decided to publish every conviction of regulated/obliged entities by the Disciplinary Committee, in an effort to prevent both individual lawyers and/or legal entities from future wrongdoing. This measure aims to act as a tool which will incentivize regulated entities to adapt and implement the relevant AML laws and directives to avoid reputational damage in case of conviction. Furthermore, the CBA is re-assessing the effectiveness, categorization and proportionality of its sanctions, especially in cases where a repetitive tendency is observed.

555. In its strategic plan for training, licensing and a risk-based approach, the CBA's objective includes establishing a policy for sanctions. CBA staff interviewed mentioned measures being taken for the last 10 years to improve its supervisory controls, as an ongoing and continuous process that is still in need of improvements. Given the heightened risks that ASPs in particular under CBA supervision represent, as well as the recognition that VAs are a high-risk activity, the CBA reported to the assessment team a number of improvements with respect to its remedial actions, including sanctions, for these particular supervised entities as a component of the CBA's ongoing improvement initiatives.

ICPAC

556. ICPAC has translated the recommendations from both the 2018 NRA and the Moneyval assessment into an action plan that sets remedial actions for ASPs as well as accountants and auditors as supervised entities. With regard to sanctions in specific, it was observed by Moneyval that ICPAC has not imposed enough measures or set clear criteria to determine the level of administrative sanctions based on the seriousness of a breach, although it must be acknowledged that ICPAC has in place an AML/CFT Directive addressing VA activities. Failure to require remedial actions (where warranted) in the future context of supervision of ASPs serving clients in the VA sector would be a potential weakness.

CySEC

557. Moneyval found that CySEC imposed sanctions to its supervised entities during the period of the Moneyval assessment, with measures to make them effective and dissuasive, although the absolute number of sanctions imposed for AML/CFT infringements was considered significantly low relative to the number of infringements detected. Moreover, the more common consensual approach where supervised entities are tasked to remedy their own deficiencies and demonstrate their actions, as contrasted to the supervisor imposing the penalty and. Remediation measures, called into question the effectiveness, proportionality and dissuasiveness of CySEC's regime for sanctioning, in Moneyval's view. To date no sanctions have been imposed relating to VA ML/TF noncompliance.

Casino Commission

558. There have been no remedial actions or sanctions imposed for VA activity because there is no such activity taking place.

National Betting Authority

559. The NBA has not applied sanctions or any remedial actions related to VA activities because such activities have not arisen at the time of the assessment.

6.2.5 Impact of supervisory actions on compliance

FI Supervisors

CBC

560. In the aftermath of the 2013 banking crisis, the CBC's high degree of caution to prevent AML risks from arising has led to a strict level of compliance throughout the banking sector, as well as a thorough awareness of these risks among non-bank financial institutions, as set forth in Moneyval's findings.
561. The CBC's supervisory actions regarding VA have involved closely scrutinizing risks and controls of any proposed VA activities. The assessment team found that supervised entities have largely avoided VA activities or providing services to VASPs or even retail customers purchasing VA due to a low risk appetite for what they perceive as high-risk VA activity that might put their correspondent banking relationships at risk
562. The CBC's approach has led to the perception, on the part of supervised entities, other authorities and among internal staff as well, that VA activity is altogether banned by CBC, although this is not the case.
563. Under PSD2 supervisors may permit regulated entities to engage in "other" activities within the same legal entity or to require it to occur in a separate legal entity. The CBC has elected to require supervised firms to utilize a separate legal entity to conduct "other" activities, thus reducing the potential risks within the supervised entities.

CySEC

564. CySEC's supervisory actions for those selected firms engaging in VA activities involve close cooperation and frequent communication between supervisory staff and supervised entities. The supervisory staff have been very involved in the development and implementation of rigorous AML/CFT procedures tailored to VA activities. The impact of this supervisory approach has been a high degree of compliance while at the same time allowing for VA activities to unfold in an adequately supervised manner (from an AML/CFT perspective).

ICCS

565. The Superintendent of Insurance has not taken any actions focused on ML/TF risks related to VA or VASPs. However, the assessment team did not consider this a deficiency because of the lack of apparent nexus or entry point of VA or VASPs into this sector.

DNFBP Supervisors

CBA

566. The CBA is in process of setting VA-specific supervisory measures to impact compliance through a legislative and legally binding regulatory framework for VA activities. The CBA is in process of launching an action plan aiming to increase the awareness of its obliged entities to undertake effective CDD and other preventive measures. In this context, the CBA is currently revising its AML questionnaire to incorporate recent trends, as well as adding a section for targeted collection of data on the VA market.

The CBA informed the assessment team that the reason that this has not been done in the past is because the legal society generally has not provided any services in this respect, with perhaps some minor exceptions. This is consistent with the assessment team's general observation that there is very limited VA activity in Cyprus at the moment.

For those minor exceptions of obliged persons who do offer such services related to VA activity, the CBA considers their services still do not remain unregulated because they fall under the scope of the CBA Guidance. More precisely, as provided for in the Guidance-December 2019, which states that enhanced due diligence should be carried out for clients determined to be of higher risk, it is expressly provided that cryptocurrency activities are an area that poses higher risk. Therefore, obliged entities engaging in these activities should follow the designated procedures for EDD and apply the Risk Based approach designated in the guidance.

ICPAC

567. ICPAC's VA-specific supervisory measures are set forth in its 2020 AML/CFT Directive. It has also offered an online seminar to its obliged entities, presented by the Digital Forensic Lab of the Cyprus Police, covering the topics of cybercrime, online fraud, and cryptocurrencies, as well as disseminating the FATF Virtual Asset Red Flag Indicators for ML/TF from September 2020, in its General Circular 23/2020.

CySEC

568. There have been no VA-specific supervisory measures to impact compliance in the absence of an enacted, legally binding regulatory framework for VA activities.

Casino Commission

569. Not applicable

National Betting Authority

570. Not applicable

6.2.6 Promoting a clear understanding of AML/CFT obligations and ML/TF risks

FI Supervisors

571. Both CySEC and the CBC have binding AML/CFT Directives, which they have clearly communicated to supervised firms and made readily available on their respective websites. Both have yet to update their AML/CFT Directives to include measures dealing specifically with VA activities and VASPs. They have clearly indicated to the assessment team their intent or desire to do so in 2021 once the amendment to the AML/CFT Law is enacted. CySEC performed a public consultation in 2019 on how the Cyprus AML/CFT Law should be amended to address VA, which has the effect of educating the industry as well as enhancing the supervisor's understanding.

CBC

572. Moneyval observed, and the assessors concur, that the CBC has undertaken efforts to promote overall AML/CFT understanding and effective risk mitigation practices since the aftermath of the financial crisis. However, these have not focused broadly on VA activities. The assessment team found that CBC-supervised entities consistently perceived VA activities and VASP customers as high risk from an ML/TF perspective and have been eschewing them completely. Should VA activities start to take place in this sector, a more nuanced view tailored to specific risks and mitigants may be needed.

573. The CBC must update its AML/CFT Directive to include measures specific to VA/VASPs. In addition, the CBC has not updated its AML/CFT Directive to include non-bank FIs like EMLs, PSPs and MVTs, which may be more likely than banks and credit institutions to engage with VASP or VA customers. The CBC is considered a thematic update to its AML/CFT Directive to cover all types of supervised entities in respect of measures specific to VA/VASPs.

574. Once CBC has updated its AML/CFT Directive to include measures specific to VA/VASPs, it should consider further steps to communicate and promote clear understanding of the new measures.

CySEC

575. The assessment team met with the main entities authorized by CySEC to engage in VA or VASP-like activity under CySEC Circular C244 or as an AIFLNP, and found that CySEC has promoted a clear understanding of the specific VA ML/TF risks and mitigants through its direct interactions with these entities. CySEC has actively engaged with the sector as a ML/TF supervisor and has both gained and promoted a more sophisticated understanding of risks and mitigating measures as they pertain to VA. CySEC has not, however, offered broader industry training and should consider doing so once its VASP registration framework is in place. Once CySEC has updated its AML/CFT Directive to include measures specific to VA/VASPs, it should also consider further steps to communicate and promote clear understanding of the new measures.

ICCS

576. The Superintendent of Insurance has not taken any actions focused on ML/TF risks related to VA or VASPs. However, the assessment team did not consider this a deficiency because of the lack of apparent nexus or entry point of VA or VASPs into this sector.

DNFBP Supervisors

ASPs – Summary

577. All three ASP supervisors have provided training and issued guidance on compliance with the provisions of the AML/CFT Law to promote supervised entities' clear understanding of their obligations. ICPAC's AML/CFT Directive has provided highly specific guidance on VA ML/TF risks. Moneyval also observed the level of understanding of general AML risks is high among supervised entities. Most ASPs are thus trained in this respect and able to detect suspicious activity. There is knowledge and experience on what suspicious activities to look out for and what actions to take upon detection of unusual activity.
578. Because ASP supervisors have not detected substantial VA activities on the part of their supervised entities, and in advance of the adoption of the regulatory framework tailored for this sector, they largely have not been in a position to disseminate knowledge on VA-specific ML/TF risks and AML/CFT obligations.
579. Although there are no reported ASPs currently serving clients in the VA sector (other than as advisors), there is interest in VA-specific training with the expectation that once these activities become regulated, ASP services will increase in demand. The three ASP supervisors all indicated plans to organize the provision of training in this respect, in coordination with issuance of guidance and secondary legislation. There is general awareness, both on the part of supervisors and ASPs themselves, regarding the need for both training and guidance for compliance with AML/CFT obligations regarding VA activity.

CBA

580. With regard to VAs, the CBA has begun to provide ASPs and all of its members with specific continuous training and knowledge sharing regarding AML/CFT, as no such activity has been detected previously and therefore it was not considered a priority.

ICPAC

581. In addition to licensing and supervision, ICPAC is also tasked with ensuring continuous professional development among its members. This includes updating members regarding new developments and issues that may impact the accounting profession, auditing, and related

matters. In this respect, ICPAC provides technical support and training for relevant issues. This responsibility is relevant for developments in VAs as they concern ASPs supervised by ICPAC.

582. ICPAC has offered an online seminar to its obliged entities, presented by the Digital Forensic Lab of the Cyprus Police, covering the topics of cybercrime, online fraud, and cryptocurrencies, as well disseminating the FATF Virtual Asset Red Flag Indicators for ML/TF from September 2020, in its General Circular 23/2020. While the assessors have not been made aware of any other training delivered on VAs to date, the novelty of the issue and the low level of activity could support treating this as a less pressing issue to hold industry-wide trainings on. However, with the envisioned regulatory developments in progress for this space, and the expectation that they would lead to heightened VA activity, effective professional development in this space should become much more relevant.

CySEC

583. There has been no training to date targeted to ASPs seeking to serve clients engaging in VA activities, but the assessors note that any VA-specific training and collaboration that has taken place between CySEC and other CySEC-supervised entities could be adapted and applied for ASPs.

Casino Commission

Not applicable

National Betting Authority

584. The NBA's supervisory measures have also promoted an adequate understanding of supervised entities' AML/CFT obligations and ML/TF risks although the focus to date in light of existing conditions has been on non-VA obligations and risks.

585. Performance of the consultation and publication of the AML/CFT Directive would greatly promote clearer understanding when it occurs.

7. Legal Persons and Arrangements

7.1. Key Findings and Recommended Actions

Key Findings:

1. Cyprus is a company formation and administration center, which increases the materiality of ML/TF vulnerabilities with respect to the misuse of legal persons and arrangements created in the country. Any such vulnerabilities would also be vulnerabilities that apply to legal persons and arrangements engaging in the VA/VASP sector, which would also carry the risk of being misused for ML/TF purposes.
2. Moneyval found, and the assessors were advised of no steps to rectify, a failure by Cyprus to track metrics on percentage of companies under non-resident ownership/control, percentage of companies without Cyprus bank accounts, and percentage of companies under ASP management or part of corporate chains. The DRCOR does not record metrics on the legal persons and arrangements listed on its registry, including entities planning to engage in VA activities.
3. This may limit authorities' ability to detect potential patterns or typologies of ML/TF risk arising from abuses in companies that are non-resident owned/controlled, do not hold Cyprus bank accounts, and/or are under ASP management or part of corporate chains. This could also limit the ability to detect patterns of ML/TF risk or abuse in VASPs or entities engaging in VA activities.
4. Cyprus has taken measures to improve the accuracy, availability, and transparency of information related to legal persons and arrangements by means of BO registers. These improvements should enhance the quality of record information from legal persons and arrangements engaged in the VA/VASP sector.
 - a. The DRCOR has made progress striking off companies and updating its existing register, although there still remains outdated and inaccurate information that has been retained due to ongoing creditor claims and claims from the Tax Department for pending tax payments. The DRCOR is also building a BO register for corporate entities to be populated by March 2022. Additional functionality for access by the general public is expected to be implemented by Q3 2022.
 - b. CySEC is developing a BO register of trusts.
 - c. The MoI is updating its current NPO register and aligning it with the DRCOR register.
 - d. The CBC has developed a bank account register with BO information, which has gone live and operational since the enactment of the AML/CFT Bill.
5. Adequate BO registers stated above may serve authorities as an effective alternative to their prior reliance on ASPs as the primary repository of BO information.
6. Although not referenced by Moneyval, Cyprus has very strict sanctions for breaches regarding basic and BO information on legal persons and arrangements. Cyprus criminalizes the act of providing false or misleading information on BOs. As part of CDD procedures, entities that knowingly provide false or misleading identification or

other information on customers or BOs are considered guilty of an offense. This can lead to conviction, with imprisonment for up to two years, a fine of up to €100,000, or both.

7. CySEC will establish a VASP registry upon enactment of the AML/CFT Bill, with full authority to collect all necessary information regarding legal structure and arrangement, BO and management it deems necessary.
 - a. CySEC will not just collect this information, it will verify the information on this registry, which procedures (based in current CySEC processes) are expected to be far more rigorous than the basic checks for form and completeness that the DRCOR applies for its records.
 - b. The specifications and registration conditions for the VASP register are yet to be established at the moment of the assessment, although the statutory basis is established in the AML/CFT Bill.
8. VA activities may operate under a range of legal arrangements, which could present novel issues and could present heightened risks in Cyprus.
 - a. The decentralized fashion in which certain VA/VASP entities are established, outside of legal persons, is an important feature currently evolving.
 - b. Trends toward decentralized finance (DeFi) and emergence and growth of stablecoin arrangements may also result in novel structures and legal arrangements for VA/VASP entities.

Recommended Actions:

1. Ensure BO registries of legal persons and arrangements adequately record and update relevant information for entities in the VA/VASP sector. In conjunction with the recommendations in Section 6 toward harmonization across ASP supervisors regarding VA activities, requirements for recording information on legal persons and legal arrangements and implementing monitoring and auditing practices should also be harmonized across ASP supervisors.
2. Consider whether it would be desirable for the DRCOR to record designated metrics on legal persons and arrangements listed on its registry, specifically metrics on percentage of companies under non-resident ownership/control, percentage of companies without Cyprus bank accounts, and percentage of companies under ASP management or part of corporate chains. This would assist allowing the Registrar to flag suspicious activities or patterns and collect metrics on companies engaging in VA activities so as to assist regulators in monitoring unregulated activity.
3. When CySEC establishes the specifications for its VASP registry, it should ensure all necessary information regarding legal persons and arrangements and BO is provided and maintained, as conditions for VASP registration.
 - a. To further transparency and public availability of information, CySEC should consider what basic and BO information to make public on VASPs in the registry.
 - b. CySEC should ensure in the registration conditions that it receives the necessary information for legal arrangements engaging in VA/VASP activities. This is particularly important due to the emerging trend for VA/VASP activities

to fall under novel legal arrangements outside of a legal entity, as in the case of DeFi.

4. CySEC should monitor issues with respect to the evolving and novel structures and legal arrangements that VA/VASP entities are likely to operate under due to their decentralized nature, outside of legal persons, including trends of decentralized finance (DeFi) and stablecoin arrangements which may continue to evolve in novel structures and legal arrangements for VA/VASP entities. CySEC should communicate its findings to other authorities such as DRCOR to ensure record collection corresponds to evolving requirements.

7.2 Immediate Outcome 5 (legal persons and arrangements)

586. Cyprus is a center for trust and company formation and administration. A significant proportion of legal persons and arrangements form part of international corporate structures and are managed by ASPs on behalf of foreign residents. Moneyval found this entails a certain degree of ML/TF risks to the extent that illicitly obtained funds from abroad may enter the system in Cyprus. These same vulnerabilities of misuse of legal persons and arrangements could be misused by entities operating in the VA/VASP sector. Legal persons and arrangements engaging in VA activities, using international structures, and serviced by ASPs, could therefore pose ML/TF risks.
587. With respect to legal persons, Moneyval noted that private companies, which may be administered by ASPs or not, are the most common form, and also most preferred by non-residents, to structure and manage their assets. The structure where the legal owner and the beneficial owner are not the same person poses heightened risks, especially where the non-residents make up the BO and have control. ASPs hold roles of directors/secretaries in these structures, and BO information is available through the registers held by the ASPs serving these private companies. In cases where these entities hold Cyprus bank accounts, the records of these banks also hold BO information. BO information from Cyprus bank records has been found by Moneyval to be more reliable and accurate than that held by ASPs.
588. Moneyval also noted that the second most common type of legal person in Cyprus makes up entities engaged in commercial, trading, and entrepreneurial activities, where the legal owner and beneficial owner are the same person. In such entities, ASPs do not take the role of directors/secretaries. The director/secretary owns at least 25%, and share capital is not held on behalf of third parties, and there are no nominee shareholders. BO information is available from the entities themselves, from the registry maintained by the Department of the Registrar of Companies and Official Receiver (DRCOR), and also from Cyprus bank records in cases where these entities hold Cyprus bank accounts.
589. With respect to legal arrangements, of which the business of trusts is the most material type, the sector is less developed in Cyprus in comparison to company formation and

administration. Thus, it is considered by Moneyval to pose less material ML/TF risks. Trusts are required to obtain and hold BO information. They are generally set up by ASPs and most have an international component in the form of a non-resident settlor, beneficiary, etc. These trusts are required to have at least one licensed Cyprus resident trustee. For the few remaining trusts, generally family trusts, there is no need for a licensed trustee. Similar procedures and vulnerabilities would hold for legal arrangements in the VA/VASP sector.

590. Company registration in the existing registry managed by the DRCOR takes place through lawyers, providing a memo stating company registration and documents are in accordance with Cyprus law, European law, and international law. VA companies or VASPs are subject to the same procedures, where they would provide a memo stating their activities are in accordance with the law.
591. In addition, the existing AML/CFT legislation in Cyprus sets provisions for a BO registry for legal persons. In accordance with FATF best practices for beneficial ownership, this registry will be managed by the DRCOR and would cover all entities including VA/VASP entities registered as legal persons. The Registrar would check for basic form and completeness in adding and updating its records, however it would not collect additional metrics. There is also a BO registry for trusts under development to be managed by CySEC, a bank account registry has been developed and is managed by the CBC, and an updated NPO registry to be aligned with the DRCOR BO registry and managed by the MoI. All of these registries would presumably include relevant legal entities engaged in VA/VASP activities. The assessors consider that maintaining BO records accordingly is an important step to ensure transparency and control ML/TF risks for VA/VASP legal persons, arrangements and activities.
592. Furthermore, the AML/CFT law also grants powers to CySEC for registration of VA/VASP entities, where CySEC will examine applications and can deny registrations. Based on these powers and procedures, CySEC will be putting together an additional registry of VASP entities. Thus, VASPs would have a file in the overall company registry as well as this CySEC registry, which will include additional controls and reviews to verify the information, beyond basic checks for form and completeness. CySEC will review VA/VASP legal entities' disclosures as provided according to existing requirements for all legal persons and arrangements. At the moment of the assessment, CySEC has not yet defined the requirements for this registry, which would include BO information and other information on legal persons and arrangements operating in the VA/VASP sector. The assessors find this VASP registry to be an added source of transparency and critical safeguard to mitigate abuse of legal entities engaging in VA/VASP activities.

7.2.1 Public availability of information on the creation and types of legal persons and arrangements

593. The assessors find that the existing level of public availability of information on the creation and types of legal persons and arrangements in Cyprus would apply for VASPs and

entities engaging in VA activities. Therefore, the assessors consider there to be no incremental ML/TF risks with respect to the VA/VASP sector in this respect.

594. Moneyval noted that details on the creation and types of legal persons in Cyprus is made public on the Cyprus government website, which also contains the forms required to create legal persons and make changes (e.g. directors, shareholders, registered address, etc.), as well as the entirety of Cyprus legislation. English translations of several laws, including incorporation and registration of legal persons and arrangements, are publicly available on the Office of the Law Commissioner's website. The MoI data also releases information publicly on its website regarding its respective registered entities, and the MoF's website has public information on approved charities. With respect to trusts as legal arrangements, however, information on their creation is not public but can be obtained directly from the respective trust providers. Information on trust types may be publicly available through Internet searches.

595. At the moment of the assessment, the DRCOR manages and updates a company registry, with publicly available information on current directors, registered addresses, and pending changes free of charge on its website. Access to full information requires a fee which is waived for the Police, FIU, CBC, and Tax Department. The DRCOR merely records and posts the information and does not collect metrics or statistics on it. The DRCOR is also taking active steps to address the deficiencies found by Moneyval with respect to outdated information and pending strike-offs of a substantial number of companies, which will improve the quality, transparency, and reliability of the data available on its registry.

596. Looking ahead, the assessors found that the DRCOR is working to launch a BO register for corporate entities, denoted the Beneficial Ownership Registers Interconnection System (BORIS). As per the provisions of AMLD5 which has been transposed into the new AML/CFT law, this registry will be openly available to the public. The upcoming AML/CFT Bill incorporates provisions from AMLD5 which extends the access provisions for a BO registry to be made publicly available, rather than restricted to supervisory authorities, law enforcement, and obliged entities when conducting CDD. Until the final register is implemented by Q3 2022, the DRCOR has developed an interim solution, which is only technically feasible to make available upon request to competent supervisory authorities, the FIU, and law enforcement (police, tax authorities, customs). DRCOR has released a circular in December of 2020 requesting companies to provide BO details starting in February of 2021, with intended completion date by June of 2021 currently extended up to March 2022. The interim solution will be launched with this information until the software is developed to launch the final registry publicly.

597. There are a number of additional specific BO registers that are also being developed in Cyprus, which will add to the availability and accessibility of data on the creation and types of legal persons and arrangements. Also under the provisions of AMLD5 and the Cyprus AML/CFT Bill, a BO register of trusts administered in Cyprus is expected to be launched in January 2022, and will be managed and updated by CySEC. CySEC will therefore be the single authority holding BO information on trusts and legal arrangements administered in Cyprus, rather than having 3 registries managed by CySEC, ICPAC, and CBA. This register will not be available to the

general public but to supervisory authorities, law enforcement, and any parties with legitimate interests in advancing AML/CFT measures. This is in accordance with international practices and provisions from AMLD5. The legitimate interest will be established by CySEC on a case by case basis, as provided in the AML/CFT legislation.

598. There is also a bank account register developed by the CBC under the provisions of the AML/CFT Law, which has gone live and operational since the enactment of this legislation. Moneyval has noted that the BO information currently provided by banks from their existing records is more accurate and reliable than records held and provided by ASPs. This registry will include information on the name of the individual or company, bank account number, and UBO. It will be available to the FIU and police, and is also available to law enforcement entities, such as the Tax Department and Customs, for use in criminal cases that would require access to that data.

599. With respect to NPOs, the existing BO register of NPOs managed by the MOI is being adapted to better align with the larger BORIS system. There is a small number of such NPOs, approximately 2,000, already registered by the MOI as legal persons that generally don't have shareholders. The registry will make the names of management publicly available.

600. Finally, with respect to the VASP registry to be managed by CySEC, the specifications are yet to be established. Critically, CySEC would not just gather information but would examine the substance of applications and the information provided therein rigorously, unlike DRCOR, verifying their accuracy and taking extra steps to assess character and fitness. In furtherance of promoting transparency and public availability of information, CySEC should consider to what extent it will make the data public regarding BOs and UBOs of VASPs seeking registration.

7.2.2 Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal persons

601. The assessors found there to be a generally acceptable level of understanding of ML/TF risks and vulnerabilities of legal persons in Cyprus, particularly given its status as an international center for company formation and administration. There is widespread awareness that BOs who are not legal Cyprus residents pose heightened vulnerabilities of misuse of legal persons for ML/TF. Authorities understand that complex structures with an international component, several countries of residence or incorporation, nominee shareholders and several layers of intermediary BOs are all factors that increase vulnerabilities of ML/TF.

602. However, Moneyval noted that Cyprus has not conducted a risk assessment to formally identify and assess the ML/TF risks and vulnerabilities of legal persons. There remain gaps in understanding the specifics of the existing vulnerabilities of legal persons, the corporate landscape, and how legal persons created in Cyprus could be abused for ML/TF. There is no knowledge on the types of legal persons most frequently used in criminal schemes, or the extent to which nominee shareholder agreements have been subject to misuse historically.

603. The assessors note that these gaps in understanding would carry over to legal entities operating in the VA/VASP sector. They concur with Moneyval's conclusion that this represents an important shortcoming that hinders the ability to implement targeted risk mitigation measures based on specific risk identification, especially given the materiality of Cyprus legal persons and the range of legal arrangements that VA/VASP entities can take beyond trusts. The number and proportion of legal entities with non-resident BOs and control is also unknown, as well as the types and nationalities most represented in these structures. Out of these entities with foreign BOs and control, the number of entities that do not hold Cyprus bank accounts, the number of entities under ASP management, and the number of entities that form part of a corporate chain or use bearer shares or warrants, are also unknown. There are no procedures or statistics specific to VA/VASP activities in these matters.
604. The assessors also found that there is very limited focus on or awareness of the implications of these weaknesses and deficiencies as applied to VASPs, or specific understanding that these risks would likely apply to VASPs from abroad starting operations in Cyprus.
605. Offsetting these weaknesses is the VASP registry to be established by CySEC, including rigorous conditions expected to be imposed and enforced by authority provided under the AML/CFT Bill to CySEC in establishing the registry. CySEC has demonstrated an adequate and sophisticated level of understanding of the relevant risks for legal persons engaging in VA/VASP activities.

7.2.3 Mitigating measures to prevent the misuse of legal persons and arrangements

606. Moneyval expressed a number of concerns with respect to basic and BO information on legal persons and arrangements. With regard to basic information, Moneyval noted weaknesses arising from the fact that the company registry managed by the DRCOR held substantial outdated and inaccurate information.
607. With respect to BO information for legal persons, the Administrative Services Law of 2012 (ASL), which sets the ASP regulatory and supervisory framework for prudential and AML/CFT issues, is designed to ensure transparency of non-resident owned and controlled legal entities which pose highest ML/TF risks. ASPs must be licensed in order to provide their services. Non-resident owned and controlled legal persons engaging the services of ASPs are also required to engage only with Cyprus licensed ASPs, which must be natural persons residing in Cyprus. AML/CFT requirements for ASPs require them to gather BO information of their legal entity clients. Yet Moneyval noted, and the assessors concur, a need for improvements in the registers of ASPs and their clients maintained by the three ASP supervisors (CySEC, ICPAC, CBA). Moneyval also noted that apart from on-site visits by ASP supervisors, which cover only a sample of entities at a time, there is no mechanism to verify that the requirement to engage services of only Cyprus-licensed ASPs is met by all non-resident owned and controlled legal

persons. This may present a significant gap for the VA/VASP sector given the likelihood that these operations may be foreign owned or operated. The assessors also note that the availability of BO information would depend on the quality of CDD performed by ASPs.

608. With respect to BO information for legal arrangements, ASPs managing and administering trusts are required to maintain BO information on them under the ASL and AML/CFT Bill. The ASL and International Trusts Law also require Cyprus trusts to have at least one trustee be licensed and a resident of Cyprus. Yet Moneyval again finds that there is no mechanism to ensure implementation of this requirement. Moneyval concludes that because trusts are less material than legal persons, this vulnerability is also less material. Yet the assessors also find it important to consider that VA activities have potential to utilize a range of legal arrangements which could heighten the risk of this type of legal entity. One of the emerging and evolving features of the VA/VASP ecosystem is the decentralized fashion in which entities are established. Moreover, the existing trends of decentralized finance (DeFi) and stablecoin arrangements may result in novel structures and legal arrangements, which presents a level of ML/TF risk that should be monitored.

609. Moneyval also noted that the banking sector has adequately and reliably recorded and held BO information, even more so than the ASPs, as part of its standard CDD procedures. An additional safeguard performed consistently by banks has been to establish direct contact and meet BOs personally. Yet however transparent and accurate the BO information held by Cyprus banks may be, it is only beneficial to the extent that legal persons and arrangements actually hold Cyprus bank accounts and have been screened through that screening process. With respect to the VA/VASP sector, in the event that VASPs turn out to be primarily foreign owned and operated, there would be a greater likelihood of them holding bank accounts outside of Cyprus, especially given the general reluctance of the Cyprus banking sector to engage the VA/VASP sector, thus reducing the mitigating effect of this control factor.

610. Ultimately, the assessors found that Cyprus has taken significant measures to address Moneyval's concerns and also taken additional steps to further improve transparency and availability of information on legal persons and arrangements. These improvements consist in mitigating measures that the assessors consider can effectively prevent the misuse of legal persons and legal arrangements in Cyprus.

611. The assessment team learned of substantial improvements to address Moneyval's concerns regarding the company registry, with the DRCOR taking action to implement its reform and enhance the Registrar's powers. This involved taking steps to clean up and update the company registry by striking off companies and making necessary updates. It also adopted a new IT infrastructure and fully migrated its records to an electronic format, with an electronic file for every company.

612. Moreover, the assessors found additional and substantial steps have been taken to improve transparency and accessibility of BO information. The existing AML/CFT legislation in Cyprus criminalizes the act of providing false or misleading information on BOs, establishing

conviction, imprisonment, and pecuniary fines. This serves to further promote transparency in BO records, setting a basis for the creation of additional registers specifically recording BO information which the assessors were informed to be in development at the moment of the assessment.

613. The DRCOR has begun to undertake the task of creating a new BO registry for corporate entities, currently being populated with the relevant information, with a deadline for full compliance by companies March 2022. The system with full online functionality and public access is expected to be implemented by Q3 2022, which the assessors consider would significantly improve the transparency of BO information available. The upcoming Beneficial Ownership Registers Interconnection System (BORIS) will comply with provisions of the AML/CFT Bill transposing AMLD5. An interim solution has been developed thus far by the DRCOR, in conjunction with a circular issued by CySEC on December 21, 2020, which provided companies until July of 2021 (later extended to March 2022) to meet their obligation to provide data. The FIU, law enforcement authorities, and competent supervisory authorities will have access to this interim solution upon request. Moreover, the MoI is updating its register of NPOs for better alignment with the overarching BORIS implementation by the second half of 2022.
614. An additional BO register of trusts is also under development, to be managed and updated by CySEC. This register is expected to become operational by January 2022. The assessors also found that the CBC has developed a bank account register under the provisions of the AML/CFT Law, which has become live and operational since the enactment of this Law by Parliament.
615. The assessors consider that these factors that improve transparency of basic and BO information for legal persons and arrangements in general would also apply to legal persons and arrangements engaging in VA/VASP activities. Thus, the assessors find that the improvements being implemented in this respect as mitigating measures would also serve as useful measures to control ML/TF risks of legal persons and arrangements engaging in VA/VASP activities. The impact of these measures on the VA/VASP sector consist of greater transparency of basic and BO records, which FATF recognizes to be an effective measure to mitigate ML/TF risks arising from misuse of legal persons and arrangements.
616. Finally, as an additional and crucial safeguard for the VA/VASP sector, the VASP registry to be managed by CySEC is considered by the assessors to be a key measure to mitigate potential misuse of legal persons and arrangements engaging in VA/VASP activities. It will add to the level of transparency of both basic and BO information, in a verified and vetted manner, with records on the registry having undergone CySEC's controls for company registration. While the specifications for the VASP registry are yet to be established at the moment of the assessment, the assessors consider that the application of CySEC's verifications, which go beyond the basic checks for form and completeness applied for the DRCOR registry, will likely make the VASP registry a source of more robust and reliable information.

7.2.5 Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons and legal arrangements

617. Moneyval noted that competent authorities have direct and full access to the records held by the DRCOR. However, Moneyval also noted important shortcomings with respect to the consistency of access to information and reliability of records. While these shortcomings persist, the assessors consider they would also apply to records of legal persons and arrangements engaging in VA/VASP activities.
618. The DRCOR's company registry was found by Moneyval and by the assessors to contain a substantial amount of outdated information. Any outdated information that may persist in this registry would not be reliable for competent authorities to rely on for setting AML/CFT risk mitigation measures or taking action upon ML/TF concerns arising. Outdated information may also imply outdated and inaccurate BO information, and an overall lack of transparency.
619. Until the launch of the BO registry, records from ASPs would continue to be the primary source of BO information. However, reliance on ASP records was deemed by Moneyval to be problematic due to inconsistencies in the application of BO requirements and concerns on the effectiveness of licensing and supervision. These factors could call into question the validity of basic and BO information held by ASPs. Moreover, for those legal persons not administered by ASPs, where the BO is the same person as the legal owner, there may be no consistent and reliable source of BO information. BO information could be accessible directly from the legal entities which may not be adequately verified, from the DRCOR registry which still holds outdated records, or from Cyprus banks if accounts are held with them.
620. While Cyprus bank records on BO information were deemed by Moneyval to be more reliable due to their stringent CDD procedures, they wouldn't always be applicable because Cyprus legal persons and arrangements may hold foreign bank accounts. Thus, reliance on Cyprus bank records as a better source of information than ASP records would only be possible for cases where legal persons and arrangements would hold Cyprus bank accounts. This may exclude non-resident owned and controlled legal entities, which are also considered the most vulnerable to ML/TF risks.
621. Moneyval also noted a lack of metrics, where there are no statistics or insights gathered from the records. There is no data on the proportion of legal persons and arrangements that are non-resident owned/controlled, the proportion that has no Cyprus bank account, or the proportion that falls under ASP management or forms part of corporate chains.
622. However, the assessors note that Cyprus is taking significant measures to improve the timely access to adequate, accurate, and current basic and BO information, which would also benefit the level of transparency for legal persons and arrangements in the VA/VASP sector. Looking forward, the assessors found that in addition to the DRCOR's measures to clean up its company records, the BORIS implementation for a company BO registry and additional BO records under development would eventually provide a better alternative to access more

reliable basic and BO information on legal persons and arrangements. Upon the full implementation of the BORIS registry of company BO information under the DRCOR, the MoI's parallel update to its NPO register, the BO register of trusts under CySEC, and the CBC's bank account register, the assessors note that BO information will be more easily accessible and more consistently reported to facilitate access and transparency.

623. Moreover, the assessors consider that CySEC's register for VASPs would ensure access to all material information on legal persons and arrangements operating in the VA/VASP sector. They note that CySEC should ensure in the VASP registry's registration conditions that it receives the necessary information regarding legal arrangements engaging in VA/VASP activities. This is particularly important in light of the emerging trend for legal arrangements to be used for VA/VASP activities outside of any legal entity, as in the case of DeFi.

7.2.6 Effectiveness, proportionality and dissuasiveness of sanctions

624. Although not referenced by Moneyval for this matter, the assessors noted that Cyprus has very strict sanctions for breaches regarding basic and BO information on legal persons and arrangements. The Cyprus framework sets important safeguards for effective, proportionate, and dissuasive sanctions. Moneyval had noted elsewhere that the existing AML/CFT legislation in Cyprus criminalizes the act of providing false or misleading information on BOs. As part of CDD procedures, entities that knowingly provide false or misleading identification or other information on customers or BOs are considered guilty of an offense. This can lead to conviction, with imprisonment for up to two years, a fine of up to €100,000, or both. Moneyval also noted that both ASPs and banks are subject to serious repercussions for failure to provide BO information upon request, or failing to uphold the confidentiality of the requests by competent authorities.

625. With respect to basic information, Moneyval noted that the DRCOR implemented effective and dissuasive sanctions for failure and delays in submitting legal persons' annual returns. These sanctions included striking off companies that failed to submit their annual returns and imposing fees for late filing by active companies. Ultimately, these sanctions would result in improving the quality of records held by the DRCOR. The assessors consider that these sanctions would also be applied for registered legal persons and arrangements engaging in VA/VASP activities, improving the reliability of their records.

626. However, apart from the DRCOR's company registry, Moneyval found weaknesses in the application of effective and dissuasive sanctions. This is particularly concerning because they relate to shortcomings in the implementation of the sanctions established by the legal framework stated above. Thus, violations of the AML/CFT law's provisions, such as FIs and DNFBPs failing to obtain and verify BO information, may not be adequately sanctioned. This was considered by Moneyval to be a significant shortcoming that does little to incentivize compliance, particularly for ASPs. With respect to the ASL requirements, Moneyval found there had been no sanctions applied. Thus, any violations such as failure to appoint an ASP as a

director/company secretary, registering a trust and appointing a trustee, or providing false/misleading BO information would not have been sanctioned.

627. The assessors note that the weaknesses in implementation of sanctions, particularly those established by the Cyprus legal framework through the AML/CFT Bill and ASL legislation, would also imply vulnerabilities with respect to legal persons and arrangements operating in the VA/VASP sector. Failure to uphold legal requirements with respect to records of basic and BO information of entities engaging in VA/VASP activities may not be adequately sanctioned. The assessors consider that this shortcoming would make present added challenges for authorities seeking to find accurate information when needed for AML/CFT purposes, either for preventive measures or in response to suspicious activity detected. Apart from these concerns, the assessment team did not find any relevant additional concerns specific to the VA sector.

628. *Overall conclusions on IO.5*

629. Weaknesses persist in the overall framework for legal persons and arrangements, and these weaknesses could readily translate to heightened risks and vulnerabilities for VASPs and legal persons and arrangements engaged in VA activities. In and of themselves these weaknesses would have resulted in a rating of low or moderate effectiveness. However, any such weaknesses should be substantially mitigated by the requirements imposed, monitored and enforced by CySEC in its VASP registry, which for purposes of this risk assessment is the most germane to this IO. While requirements have not yet been promulgated, statutory provisions already suggest a substantial level of effectiveness for VA/VASP legal persons or arrangements, which should outperform other legal persons and arrangements with regard to ML/TF risks and vulnerabilities. Implementation of the registry by CySEC should be monitored on an ongoing basis to ensure this potential is achieved.

8. International Cooperation

8.1 Key Findings and Recommended Actions

Key Findings:

1. Cyprus has well established procedures for international cooperation with countries at an EU level, as well as outside the EU, as well as strong ties with relevant authorities. These procedures have shown to be effective and can be utilized for cases involving VA or VASPs.
2. Authorities collaborate frequently and effectively with their counterparts abroad, with dedicated units for international cooperation in place.
3. Cyprus is in process of enhancing its repositories of basic and BO information of legal persons and entities, including CySEC's VASP registry which is expected to hold robust information and should greatly benefit information sharing as to VASPs.
4. There has been no significant activity to date requiring international cooperation involving VA or VASPs.

Recommended Actions:

1. It would be advisable to collect statistics specific to VA and VASPs, which would facilitate detecting if this sector represents a growing area warranting further attention.
2. Cyprus should apply its already existing strong channels of international collaboration to cases involving VA/VASPs.
3. Cyprus could leverage its collaboration with other jurisdictions that have had additional and complementary experiences with the VA/VASP sector, drawing from these relationships across supervisors to identify lessons and best practices. Such International cooperation could be an important channel for Cyprus with respect to the VA/VASP sector.

8.2 Immediate Outcome 2 (International Cooperation)

630. As an IFC, Cyprus has heightened cross-border ML/TF vulnerabilities. Therefore, international cooperation is a material component for addressing these vulnerabilities. In this context, Cyprus has been found to have developed highly effective procedures, forged strong relationships with relevant entities abroad, and has played a critical role cooperating and assisting other jurisdictions for the purposes of identifying and responding to cross-border ML/TF instances. Moreover, efforts to enhance these systems have been found to have shown positive results to address any shortcomings in operational aspects. The assessment team considers that these strong existing procedures should establish a constructive foundation for the purposes of VA/VASP cases, although authorities should monitor for situations where gaps arise due to the innovative and evolving nature of VA technologies and activities.

631. There have been very few cases of international cooperation involving VA. The MJPO, which plays a central role processing incoming and outgoing requests, has reported identifying fewer than 5 MLA involving BTC. All of these were incoming requests, and existing standard procedures were applied, consistent with best practices for international cooperation. The MJPO does not keep specific track of cases involving VA, although it would consider tracking VA if these cases were to increase. The assessment team requested but was not provided with further details on these cases.

8.2.1 Providing constructive and timely MLA and extradition

632. Moneyval found Cyprus to have generally effective procedures, particularly for freezing, confiscation, and extradition, both with EU member states and non-EU jurisdictions. While cases within the EU are subject to more standardized procedures, with specific manuals for implementing EIOs and EAWs, non-EU cases apply less formalized procedures, and no guidance has been provided to proceed consistently with such cases. The assessment team was informed of one particular incident from a local police report involving BTC. The assets in the form of VA to be frozen were identified but quickly transferred to a different wallet that authorities were unable to access. Although authorities did not succeed in freezing VA, they were able to freeze other alternative assets of equivalent value. Authorities reported that this experience provided lessons learned to better identify and freeze VA for future cases that may arise.

8.2.2 Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

633. The assessors note that there have been no instances involving VA as funds or VASPs where Cyprus sought legal assistance with respect to ML on a domestic level, or TF. Existing procedures would be utilized to pursue such cases if they were to arise. The use of tailored tools for VA, such as tracing software and other commercial intelligence tools, could enhance the effectiveness of existing procedures when applied to cases involving VA/VASPs.

8.2.3 Seeking and providing other forms of international cooperation for AML/CFT purposes

634. Moneyval observed that supervisory authorities in Cyprus have effective mechanisms in place to exchange information and collaborate with counterparts in other jurisdictions for AML/CFT purposes, with dedicated units for international cooperation and MOUs in place. They have sought and received resources through international cooperation effectively through various tools. There is also a high degree of dependence on procedures from international bodies such as Interpol/Europol, with which communication has been deemed to be well aligned with the Cyprus risk profile. Reliance on both EU and global bilateral and multilateral agreements also serves to further standardize and ensure the effectiveness of cases that involve EU member states.

635. The assessors' findings concur with Moneyval's observation that the FIU, the Police, the CBC, and CySEC all have effective mechanisms to collaborate with their respective foreign counterparts. The Customs Department also has well established relationships through which it exchanges intelligence on a daily basis with foreign counterparts. While not targeted or designed for the VA/VASP sector, these existing mechanisms would be very relevant, and even beneficial, for cases involving VA/VASPs.

636. The FIU, an active member of the Egmont Group, utilizes its systems and principles to provide and seek intelligence in its frequent collaborations with other FIUs. Its proactive forms of seeking of information, including cooperation with Police channels of international communication, have enhanced STR analysis and increased spontaneous disseminations. The Asset Recovery Office within the FIU, which identifies and traces proceeds in collaboration with its EU counterparts, would particularly benefit from learnings and experiences from tracing VA outside of Cyprus.

637. In 2018 and 2019, the FIU received the following requests from counterpart FIUs and Asset Recovery Offices:

Table 8.2.3: FIU Requests from Financial Intelligence Units and Asset Recovery Offices

	2018	2019
Requests from Financial Intelligence Units	478	468
Requests from Asset Recovery Offices	54	49

638. The Police also actively collaborates with international counterparts, under the European Union and International Police Cooperation Directorate (EUIPCD), which handles all EU relevant issues concerning the Police and is responsible for the development of international police cooperation, ensuring timely and mutual exchange of information concerning the prevention, investigation and detection of criminal offences committed in Cyprus, having links with another country or countries, or committed in another country and in any way connected with Cyprus. In particular, this Directorate promotes the implementation of the national strategy for international police cooperation, hosts the National SPOC (Single Point of Contact), monitors the alignment with and implementation of the EU acquis in the field of justice and home affairs, including the Schengen acquis, with respect to police practices. The Directorate also coordinates the preparations of the Cyprus Police for joining the Schengen area, monitors the participation of police officers to Working Parties of the Council of the EU in the field of home affairs, Comitology meetings and other EU and international fora and monitors the secondment of Liaison Officers abroad and the enhancement of European Police Missions.

The Police Cooperation Office of the Directorate serves as the point of contact with police liaison officers from several countries, including those that Cyprus collaborates most frequently

with. The Cyprus Police's National Strategy for international cooperation comprises the EUIPCD manual, as well as a related protocol to handle information through its communication channels with Europol, Interpol, and the upcoming SIRENE cooperation yet to be made operational. The Strategic Planning for 2019-2021, which includes combatting cybercrime in relation to AML/CFT purposes, also serves to enhance international police cooperation channels by setting five targets. For the purposes of VA/VASP related information exchange, the 24/7 services of SPOC (covering Europol, Interpol, and SIRENE channels) would be extremely relevant given that VA markets operate on a 24/7 basis as well that is also real-time. This would necessitate immediate action that could take place outside of normal business hours.

639. The CBC is under a number of established bilateral relations and MOUs in alignment with the Basel Committee on Banking Supervision which aims to strengthen cross-border banking supervision, in addition to a multilateral agreement with the ECB setting practices for information exchange. The CBC frequently shares its findings regarding Cyprus subsidiaries of foreign banks with the respective home supervisors. In the event that EMIs domiciled elsewhere in the EU engage in VA or VASP activities in Cyprus or support VASP customers or customers engaging in VA activities in Cyprus, CBC will have reliance on their home supervisors and communication channels will be tested.

640. As designated supervisor of VASPs under the upcoming framework, CySEC has been found to have shown a particularly sophisticated degree of international cooperation procedures, particularly exchanging mutual assistance and information across authorities, through the Strategy, International Relations, and Communications Department. It makes frequent use of IOSCO and ESMA MMoU channels, having been ranked as a top 10 user of IOSCO MMoU channels and also having been internationally acknowledge for the quality of assistance delivered to foreign entities, according to Moneyval observations.

641. The assessors observed that all relevant entities in Cyprus have extremely limited experience due to the lack of cases having arisen involving VA as assets and VASPs as entities. Cyprus supervisors would therefore have much to gain from international cooperation with international entities which have had a greater level of experience with VA as a form of funds and VASPs as entities. The existing channels of communication and collaboration, in their several forms, could be effectively leveraged to promote capacity building and staff training by means of shared experiences across supervisors. Cyprus has forged strong international relationships and uniquely strong channels of information exchange to rely on for the purposes of capacity building with respect to the VA/VASP sector. Where warranted, these channels of information exchange can be further enhanced with targeted measures for VA as funds or VASPs as entities.

8.2.4 International exchange of basic and beneficial ownership information of legal persons and arrangements

642. Moneyval found existing procedures provided for regular and timely provision of basic and BO information of legal persons and arrangements. With a strong framework in place, Cyprus authorities not only effectively exchange this information with relevant counterparties in other jurisdictions, but the additional BO registries under construction are expected to further enhance the quality of information available to draw from. As referenced in Section 7 on Legal Persons and Arrangements, these enhancements include a BO registry for corporate entities to be managed by the DRCOR, the MoI's alignment of the existing NPO register with the DRCOR, the CBC's bank account register which includes BO information, and CySEC's BO register of trusts. The DRCOR has also made progress to strike off companies and update its existing company register with basic information.
643. With respect to the VA/VASP sector, CySEC's comprehensive VASP registry is to include basic and BO information of registered VASPs under the upcoming framework. This registry is expected to include more robust and material information than the DRCOR's listings, given that CySEC will implement additional procedures to verify the records beyond basic checks for form and completeness. Although, the assessment team did not learn of any incoming or outgoing requests for basic or BO information involving VA as funds, or VASPs as entities, the VASP registry should enable CySEC to adequately respond to requests from foreign authorities with respect to VA/VASPs using the established procedures.

TECHNICAL COMPLIANCE ANNEX – R.15 NEW TECHNOLOGIES

R.15 was broadly expanded to address VA and VASP ML/TF risks in the 2019 FATF Guidance and the 2019 updates to the FATF Assessment Methodology. Accordingly, a full analysis of R.15 in relation to VA and VASPs is provided here.

R.15 New Technologies.

In its 5th round MER, Cyprus was rated **Largely Compliant** with R.15.

In October 2018 FATF revised R.15 and in June 2019, the FATF adopted the Interpretative Note to Recommendation 15 to address obligations related to virtual assets (VA) and virtual asset service providers (VASPs). These new requirements include: requirements on identifying, assessing and understanding ML/TF risk associated with VA activities or operations of VASPs; requirements for VASPs to be licensed or registered; requirements for countries to apply adequate risk-based AML/CFT supervision (including sanctions) to VASPs and that such supervision should be conducted by a competent authority; as well as requirements to apply measures related to preventive measures and international cooperation to VASPs. The 5th round MER⁴⁰ did not assess Cyprus's compliance with revised R.15 because, at the time of the on-site visit, the FATF had not yet revised its assessment Methodology, adopted in October 2019.

Taking into account that R.15 was rated as LC in MER, this assessment considers the progress made by Cyprus to comply with R.15 with respect to VA and VASPs and the revised and new elements of R.15 that relate to VA and VASPs. This risk assessment in this sense performs a re-rating of Cyprus under R.15 in relation to VA and VASP elements.

Cyprus has taken substantial steps to comply with the new requirements of Recommendation 15. It has caused this risk assessment to be performed, and it has submitted to Parliament the proposed AML/CFT Bill which, in addition to transposing 5AMLD, also includes key elements of the 2019 FATF Guidance with regard to VA and VASPs. In particular, the proposed AML/CFT Bill clearly and expressly includes VA in the statutory definition of "property", includes VASPs within the statutory scope of obliged entities, provides for the establishment of a VASP registration scheme and VASP registry, designates CySEC as the supervisor responsible for operating the registry with statutory authority to establish conditions to registration for VASPs and their management and BOs, and ensures that unfit persons cannot become BO or managers of VASPs. It provides for penalties for engaging in VASP activities without registering as a VASP. It also expressly requires obliged entities to take appropriate

⁴⁰ Although VA were not in scope for the Moneyval MER, the report noted that: Cypriot authorities have taken actions to understand the risk of new technologies. That has resulted in issuing public warnings to the obliged entities on the risks posed by virtual currencies, attending training seminars to increase supervisory expertise in virtual currencies and other FinTech related products, examining features of FinTech-related products by closely engaging in consultations with the private sector entities, etc. In relation to virtual currencies, supervisory authorities closely monitor international practices, in particular, taking into consideration results of the supranational (EU level) risk assessment, warnings issued by EU bodies (such as ECB, ESAs, EC, etc.) on risks posed by virtual currencies, recent guidance issued by the FATF, etc.. [emphasis added]

measures to identify and assess ML/TF risks prior to the promotion of any new technology, service or product, thus addressing a deficiency identified in the Moneyval report. Cyprus also completed a public consultation regarding the proposed amendment to the AML/CFT Law.

However, the amendment to the AML/CFT Law did not incorporate VA within the scope of R.16 for wire transfers. While partial compliance with R.16 with respect to VA is achieved through existing legally binding requirements to scrutinize and document the source of funds, further express legally binding provisions are required. The assessment team understands that the necessary legally binding provisions may be accomplished through secondary legislation, and CySEC has confirmed that it will implement the Travel Rule for VASPs and other entities under its supervision in its revised AML/CFT Directive to be issued in 2021, although this will not cover entities outside its scope. EU Reg. 2015/847, upon which Cyprus generally relies for compliance with R.16, has not expanded the definition of funds to include VA, however, and is limited to “currency” which under EU Reg. 2015/847 does not include VA.

In addition, Cyprus has not expressly designated the authority responsible for detecting unregistered VASPs.

New technologies

Criterion 15.1: R.15.1 as to Countries is met because Cyprus is conducting this risk assessment with respect to VA/VASPs, with the authorization and support of the Advisory Authority and Parliament.

R.15.1 as to Financial Institutions is met. The main deficiency identified in the 5th round MER under R.15.1 was that only certain types of obliged entities - credit institutions, securities and insurance firms – but not other types of FI were required to identify, assess, and manage the ML/TF risks that may arise in relation to new technologies. A technical deficiency further observed in the MER was that these obligations may be considered to arise indirectly rather than directly.⁴¹ The AML/CFT Bill

⁴¹ The Moneyval report found that Cyprus obliged entities are all under an indirect obligation to identify and assess the ML/TF risks that may arise in relation to new technologies. They are required to undertake enhanced customer due diligence in situations that present a high risk of ML/TF, and in assessing situations that pose high risks they are required to consider, among other things, “new products and new business practices, including new delivery mechanism[s], and the use of new or developing technologies for both new and pre-existing products”. AML/CFT Law, Sec. 64(3) and Annex III, para. 2(e). Banks are also subject to a more direct requirement: credit institutions must apply policies, procedures and measures to identify, assess and manage ML/TF risk during the day- to-day operations of the credit institution in relation to (a) the development of new products, services, new business practices, including new delivery channels (b) the use of new or developing technologies for both new and existing products and (c) possible changes in the business profile of the credit institution (e.g. penetration to new markets by opening branches/subsidiaries in new countries/areas). CBC AML Directive, para. 13(xi). Securities firms are specifically required to comply with the European Supervisory Authorities’ Risk Factor Guidelines, which requires that they understand the risks associated with new or innovative products or services, particularly where this involves the use of new technologies. CySEC Circular C276, ESA Risk Factor Guidelines paras. 30, 67. Insurance companies are required to evaluate risks arising from “new customers, new products, and updating and amending systems and procedures.” ICCS Revised AML Orders, sec. 4.2(xii). There is no similarly explicit requirement for other types of obliged entities. Apart from the requirements under Sec. 64(3) of AML/CFT Law, there are no more detailed

rectifies this deficiency with express new language (Art 66(3)) which expressly requires obliged entities to take appropriate measures to identify and assess ML/TF risks prior to the promotion of any new technology, service or product. Even prior to enactment of this measure, the assessment team found that both the supervisors as well as regulated firms under CBC and CySEC considered such firms to be subject to such a requirement to identify, assess, and manage the ML/TF risks that may arise in relation to new technologies and that such requirement would apply to ML/TF risks related to VA or VASP activities or technologies. The assessment team specifically found this to be the case with respect to existing CySEC-regulated firms that are engaging in VA activities as currently permitted under MiFID, AIFMD or other applicable regulation and/or under special permission from CySEC under Circular C244.

Because VASPs are obliged entities under the AML/CFT Bill this requirement will apply to them as well (It should be noted that R.15.1 applies to FI but not VASPs).

Regarding R.15.1 as to FIs, the assessment team found that the AML/CFT Law may implicitly be understood to require EDD for VA activities or circumstances where a customer of an FI is a VASP or engaging in VA activities, although VA/VASPs are not expressly enumerated in the relevant provisions of the AML/CFT Law. Specifically, Article 64(3) provides that EDD measures should be performed for high-risk factors, and in Annex III stipulates a non-exhaustive list of high risk factors that could readily be understood to apply to VA. These include (b) “products or transactions that might favour anonymity”; and (e) “new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products”. Certain Cyprus authorities, including CySEC, expressed a view that these provisions clearly applied to VA/VASPs, thus requiring EDD. Nevertheless, the assessment team found that FI obliged entities were applying EDD with respect to customers engaging in VA activities under their own internal policies. These requirements could and should readily be made explicit when CySEC and CBC update their respective AML/CFT Directives after enactment of the AML/CFT Bill.

Criterion R.15.2: R.15.2 is met. The main deficiency identified in the 5th round MER under R.15.2 was the lack of a sufficiently explicit requirement for FI other than credit institutions to perform a “pre-launch” risk assessment and mitigation to take place before launch of a new technology, product or service.⁴² The AML/CFT Bill rectifies this deficiency with express new language (Art 66(3)) which

requirements for payment institutions, for e-money institutions, credit acquiring companies, bureaux de change. However, these sectors are not material in Cyprus.

⁴² Moneyval Findings: Criterion 15.2 – (Mostly Met) For credit institutions, the risk assessment must be conducted prior to the launch of the new products, business practices or the use of new or developing technologies and there must be measures in place to manage and mitigate the risks, see section 13 of the CBC directive. Entities regulated by CySEC, Securities Firms, similarly, must specifically undertake “measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for money laundering and terrorist financing.”, see CySEC AML/CFT Directive, para. 9(1)(a). Other obliged entities more generally must take measures to prevent the use of products or transactions that may favour anonymity and must apply reasonable measures and procedures to address the risks of technological developments and new financial products. See AML/CFT Law Sec. 66(3). This obligation does not clearly extend to new business practices in general, or to new delivery mechanisms in particular, and does not require that risk assessment and mitigation take place before launch of a new technology. Apart from the requirements under Sec. 64(3) of

expressly requires obliged entities to take appropriate measures to identify and assess ML/TF risks prior to the promotion of any new technology, service or product. Even prior to enactment of this measure, the assessment team found that both the supervisors as well as regulated firms under CBC and CySEC considered such firms to be subject to such a requirement to undertake a risk assessment prior to the launch or use of new products, practices and technologies, and that such risk assessments are in fact being performed by supervised firms. This requirement also applies to ML/TF risks related to VA or VASP activities or technologies.

The assessment team found, with respect to existing CySEC-regulated CIF firms that are engaging in VA activities as currently permitted under special permission from CySEC under CySEC Circular No. C244, that such firms are already subject to these requirements under CySEC's AML/CFT Directive.⁴³ The assessment team found that there is a difference of legal interpretation within CySEC as to whether the regulated entities are formally required to engage in enhanced CDD if a customer is solely a customer with respect to the currently unregulated businesses. Notwithstanding this difference, however, CySEC and the supervised firms have confirmed that in practice the regulated financial institutions are performing enhanced CDD.

Virtual assets and virtual asset service providers

Criterion R.15.3: R.15.3 (a) is met by the performance of this risk assessment with respect to the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs.

R.15.3(b) is partly met. Cyprus is already applying a risk-based approach based on its pre-risk assessment understanding of the risks of VAs and the VASP sector. Cyprus authorities have evinced an intention to apply further risk-based measures once risks and measures are identified by this risk assessment. In the one area identified by the assessment team of actual VASP-type activity, in the form of VA activities conducted legally by firms supervised by CySEC under special permission provided by CySEC under C244, the ML/TF risks of such firms (including those activities) are subject to the legally binding framework of the CySEC AML/CFT Directive, although as noted in R.15.2 there is a matter of differing legal interpretation within CySEC as to the extent to which specific measures of the CySEC AML/CFT Directive apply to customers of such entities engaged solely in VA activities. This can readily and should be addressed when CySEC updates its AML/CFT Directive following enactment of the AML/CFT Bill.

AML/CFT Law, there are no more detailed requirements for insurance firms, payment institutions, for e-money institutions, credit acquiring companies, bureaux de change. However, these sectors are not material in Cyprus.

⁴³ The Interpretative note to R.15 in the 2019 FATF Guidelines provides that "A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations." These firms are already licensed as FIs in Cyprus.

However, the CySEC AML/CFT Directive does not currently expressly incorporate VAs or VASPs, and thus does not specify measures for VASPs or firms engaged in VA activities, does not expressly refer to VAs or VASPs, does not enumerate as high risk or risk factors matters relating to VA, and does not clearly treat VA as funds or property thereunder.⁴⁴ It is recommended that these omissions and other matters be promptly and specifically addressed in revision to the CySEC AML/CFT Directive after the AML/CFT Law amendment is enacted.

Regarding R.15.3(b) as to VASPs, the assessment team found that the AML/CFT Law may implicitly be understood to require EDD for VA activities, although VA are not expressly enumerated in the relevant provisions of the AML/CFT Law. Specifically, Article 64(3) provides that EDD measures should be performed for high-risk factors, and in Annex III stipulates a non-exhaustive list of high-risk factors that could readily be understood to apply to VA. These include (b) “products or transactions that might favour anonymity”; and (e) “new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products”. As an obliged entity a VASP would be subject to these enhanced EDD obligations for high risk activities that could be read in clauses (b) and (e) to encompass VA. Certain Cyprus authorities including CySEC expressed a view that these provisions applied to VA, thus already requiring EDD. These requirements could and should readily be made explicit when CySEC updates its AML/CFT Directives after enactment of the AML/CFT Bill, and/or in the conditions established for registration under the VASP registry.

Moreover, CySEC has indicated that based on the pending results of the NRA, which will indicate priorities and implementing measures including the allocation of resources, it will prioritise and allocate required resources to prevent and mitigate money laundering and terrorist financing, including the necessary changes to the legislative framework for implementing the required measures to mitigate the risks identified.

R.15.3(c) is met as VASPs, under the amendment to the AML/CFT Law, are included in the definition of obliged entities. As obliged entities VASPs will be required to take appropriate steps to identify, assess, manage and mitigate their ML and TF risks under Art. 66(3). Moneyval’s findings under criteria R.1.10 and R.1.11 with respect to obliged entities support this finding.⁴⁵

⁴⁴ Under paragraph 12(4) of CySEC’s AML/CFT Directive, all obliged entities should take into account, among others, the Joint Guidelines and the Guidelines issued by the Financial Action Task Force (FATF) when assessing money laundering and terrorist financing risks, as well as when applying risk-based measures and procedures. In which case this includes the Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

⁴⁵ These findings were: Criterion 1.10 – Obligated entities are required to take appropriate steps to identify and assess ML/FT risks, taking into account risk factors, including factors which relate to their customers, countries and geographical areas, products, services transactions or delivery channels. The risk assessment should be proportionate to the nature and size of the obliged entity, be documented, kept updated and made available to the relevant supervisory authorities. (Sec. 58A, AML/CFT Law) Further detailed requirements are set out in the binding directives issued by supervisory authorities. Criterion 1.11 – Obligated entities are required to have adequate and appropriate policies, controls and procedures in place, which are proportionate to their nature and size, to mitigate and manage ML/FT risks effectively (Sec. 58, AML/CFT Law). These measures should be approved by senior management, monitored and, where appropriate, enhanced (Sec. 58C, AML/CFT Law). Enhanced measures are required to be taken as noted under c.1.7.

Criterion R.15.4: R.15.4(a) is at least mostly met because the AML/CFT Law as amended requires VASPs to be registered. The assessment team understands the definition of “person” in the AML/CFT Bill to apply to either a legal or natural person engaging in VASP activities. The assessment team further understands that the registry scheme allows for a VASP to be registered in another member state without specifying the relationship to the jurisdiction where it is created (legal person) or where principal place of business is located (natural person). Although all VASPs are required to be registered, it is not clear if all VASPs that are: (i) legal persons created in Cyprus and (ii) natural persons with a place of business in Cyprus must be registered. This should be clarified in the implementing regulations and conditions for VASP registration to be issued by CySEC.

CySEC has indicated that it will enforce a register under section 61E of the AML/CFT Law, which requires all VASPs, either that being a natural person or a legal person that operate in the Cyprus Republic to register with CySEC. CySEC has the power to approve or reject the registration application based on the conditions to be laid down in the applicable laws and CySEC’s Directives.

R.15.4(b) is met because under the amended AML/CFT Law Art. 61E Sections 9 and 10 CySEC as operator of the registry will screen for these matters with respect to beneficial owners of a significant or controlling interest in, or persons holding a management function of, a VASP. Thus competent authorities take the necessary measures 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.

Criterion R15.5: This criterion is mostly met. While there is a clear legal obligation under the AML/CFT Law for any such entity engaging in VASP activities to have the requisite registration, there are not yet express provisions whereby Cyprus has designated responsibility to a specific authority for monitoring to detect and identify unregistered activity.

Section 59(1)(b)(vi) of the AML/CFT Law provides that CySEC is the supervisory authority for VASPs. Sections 61E (2),(3),(4) provides that all VASPs that provide services in Cyprus Republic must be registered to CySEC’s Register. Thus, a failure to do so (register with CYSEC) may lead to the administrative sanctions based on the powers provided under Section 59(6) of the AML/CFT Law. The AML/CFT Law has been amended to include section 61E, thus VASPs are obliged entities under the supervision of CySEC. VASPs are obliged to comply with the regulatory framework that is applicable to all CySEC's regulated entities, which includes among others the AML/CFT Law, CySEC’s AML/CFT Directive and Circulars issued by CYSEC.

The sanctions for acting as an unregistered VASP are specified in Article 59(6) of the AML/CFT Law and include substantial civil and administrative sanctions. No criminal penalties are prescribed in the AML/CFT Bill and there is not a separate VASP law providing criminal penalties for engaging in VASP activities without registering as a VASP. It is recommended that Cyprus consider prescribing such criminal penalties for engaging in VASP activities without registering as a VASP by statute in future amendment to the AML/CFT Law.

With regard to monitoring for unregistered VASP activity, it is recommended that CySEC as operator of the registry could readily undertake this, and could also include this in its whistleblowing/customer portal, and supplement this with appropriate communications to the public, to industry stakeholders and to the Police, FIU and members of the Advisory Authority, making clear that CySEC is monitoring for this, and is the appropriate authority to notify when unregistered activity is seen. This would also ensure, for example, that the information provided to MOKAS in STRs could be screened to identify unregistered VASPs and help promote appropriate cooperation in this regard. The designated authority should also consider what other tools, resources and procedures it could apply for detecting unregistered VASP activity.⁴⁶

Criterion R.15.6 is met.

Moneyval rated Cyprus as **Largely Compliant** with R.26 and **Compliant** with R.27. With regard to R.26, a deficiency was identified as to whether CySEC's oversight adequately reached managers other than key function holders, and this potential gap should be considered in CySEC's preparation of secondary legislation as it updates its AML/CFT Directive in connection with VASP registration.

R.15.6(a) Under the amended AML/CFT Law, VASPs will be subject to registration and monitoring that they comply with the terms and conditions of their registration. The AML/CFT Law has been amended to include section 61E, thus VASPs are now obliged entities under the supervision of CySEC. VASPs are obliged to comply with the regulatory framework applicable to all CySEC's regulated entities, which includes among others the AML/CFT Law, CySEC's AML/CFT Directive and Circulars issued by CySEC. A failure to comply will lead to the disciplinary and administrative sanctions based on the power of section 59(6) of the AML/CFT Law. Furthermore, Section 32 of the CySEC Law provides for the powers of CySEC, to collect information, Section 33 of the CySEC Law provides for the power of CySEC to carry out inspections. In addition, Section 34 provides for the power to enter and investigate to the obliged entities' premises. Finally, Section 36 provides for the power to appoint an investigating officer.

The assessment team thus found that Criterion 15.6(a) is met. CySEC has demonstrated to the assessment team its capabilities in the strength and effectiveness of its risk-based supervision for AML/CFT with respect to the (non-VASP) entities it currently supervises, including CIFs and Investment Funds as well as ASPs. A registration and monitoring scheme does not equal a licensing and supervision framework. The FATF Guidance allow equally for a jurisdiction to elect either a registration framework or a licensing one for VASPs. However, the Guidance also provides that countries should

⁴⁶ The June 2019 FATF Guidance provides at Par. 84: "In order to identify persons operating without a license and/or registration, countries should consider the range of tools and resources they may have for investigating the presence of an unlicensed or unregistered VASP. For example, countries should consider web-scraping and open-source information to identify online advertising or possible solicitations for business by an unregistered or unlicensed entity; information from industry circles (including by establishing channels for receiving public feedback) regarding the presence of certain businesses that may be unlicensed or unregistered; FIU or other information from reporting institutions, such as STRs or bank-provided investigative leads that may reveal the presence of an unlicensed or unregistered natural or legal person VASP; non-publicly available information, such as whether the entity previously applied for a license or registration or had its license or registration withdrawn and law enforcement and intelligence reports; as well as other investigative tools or capabilities."

monitor risks on an ongoing basis to ensure its framework continues to be suitable.⁴⁷ Cyprus should closely monitor this sector to ensure that its registration framework remains proportionate to the actual ML/TF risks.

R.15.6(b) is met. Section 59(9) of the AML/CFT Law provides for the necessary powers of the Supervisory Authorities in order to perform their supervisory duties effectively. Section 59(9)(b) provides that Supervisory Authorities in order to verify the compliance of persons under their supervision, to carry out inspections, to request and collect information, to enter the premises of the supervised persons and to inspect documents, records and accounts and any data stored in computers or other electronic means and to receive copies or extracts of these data. The AML/CFT Law has been amended to include section 61E, thus VASPs are now obliged entities under the supervision of CySEC. VASPs are obliged to comply with the regulatory framework applicable to all CySEC's regulated entities, which includes among others the AML/CFT Law, CySEC's AML/CFT Directive and Circulars issued by CySEC. A failure to comply will lead to the disciplinary and administrative sanctions based on the power of section 59(6) of the AML/CFT Law. Furthermore, Section 32 of the CySEC Law provides for the powers of CySEC, to collect information, Section 33 of the CySEC Law provides for the power of CySEC to carry out inspections. In addition, Section 34 provides for the power to enter and investigate to the obliged entities' premises. Finally, Section 36 provides for the power to appoint an investigating officer.

CySEC clearly has the power to withdraw, restrict or suspend the registration of a VASP registered in Cyprus under the amendment to the AFL/CFT Law. CySEC also has authority to initiate other civil and criminal penalties, because ML offenses are subject as a matter of law to civil and criminal penalties.⁴⁸ The assessment team understands that CySEC can also initiate other sanctions or penalties to VASPs or their managers or BOs (see R15.8 and R.35) such as criminal, civil or administrative penalties because ML offenses are subject as a matter of law to such range of sanctions.

It is however unclear what recourse if any Cyprus as a host jurisdiction has with respect to a VASP registered in another (home) member state that is operating in Cyprus to impose disciplinary or financial sanctions or cause them to be imposed.

Criterion R.15.7 is partly met. VASPs will be obliged entities subject to CySEC's AML/CFT Directive. However, the AML/CFT Directive has not yet been updated to contain specific guidelines for VASPs or VA activities. Achievement of this criterion may also be met or furthered in practice through the conditions and the organizational and operational requirements for VASP registration to be imposed by CySEC under 61.E(5) and (7) of the amended AML/CFT Law. The assessment team notes that Cyprus was rated **Largely Compliant** by Moneyval under R.34, and its report reflects a considerable track

⁴⁷ The June 2019 FATF Guidance provides (Par. 61): As the VASP sector evolves, countries should consider examining the relationship between AML/CFT measures for covered VA activities and other regulatory and supervisory measures (e.g., consumer protection, prudential safety and soundness, network IT security, tax, etc.), as the measures taken in other fields may affect the ML/TF risks. In this regard, countries should consider undertaking short- and longer-term policy work to develop comprehensive regulatory and supervisory frameworks for covered VA activities and VASPs (as well as other obliged entities operating in the VA space) as widespread adoption of VAs continues.

⁴⁸ ML offence is punishable by up to fourteen years' imprisonment or by a pecuniary penalty of up to Euro 500.000 or by both of these penalties.

record by CySEC of providing guidance and feedback to supervised entities in various forms, which could reasonably be expected to extend to VASPs in the future.⁴⁹ The assessment team has found an intention by relevant authorities to issue guidance in areas relevant to VASPs and VA once the AML/CFT Law is enacted. The assessment team strongly recommends provision of guidance by the competent authorities and supervisors in this area, including guidance to assist obliged entities with respect to SAR/STR reporting with respect to VAs, and updating the GoAML system used for STR reporting to include preset fields that relate to VA.

In the event that a VASP is structured as an entity by an ASP supervised by ICPAC, the assessment team takes note that ASPs supervised by ICPAC are expressly subject to EDD requirements under ICPAC's 2020 AML/CFT Directive, which (Section 5.7.4) specify "cryptocurrency related activities" as a high risk area in a client profile warranting specified EDD measures. These could provide an additional line of defense or clarity. ICPAC has also issued circulars regarding VA identifying that as a high risk area (Section 4.6.4) and has made clear that supervised firms are expected to take high risk areas in their risk assessment design process. ICPAC has also identified "Sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity" as a red flag for suspicious client TF activity for its supervised ASP entities, that would likewise warrant EDD.

Criterion R.15.8: Criterion R.15.8(a) is met. Under the amendment to the AML/CFT Law VASPs fall within definition of Obligated Entities and are therefore subject to a range of sanctions, including civil and criminal penalties applicable to ML offenses under applicable law.

⁴⁹ CySEC has issued an AML/CFT directive for its supervised entities. In addition, CySEC has issued a number of circulars, concerning, inter alia, guidance on new provisions of the AML/CFT Law; guidance on legislative changes at an EU level; serious tax offenses; and guidance on the content of the annual report of the compliance officers in relation to issues which have arisen in relation to preventing money laundering and terrorist financing. Furthermore, CySEC has issued feedback (in the form of circulars) to supervised entities in relation to common and recurring weaknesses and/or deficiencies and best/poor practices identified during the onsite and offsite inspections. The CySEC provides guidance to its regulated entities by addressing enquiries of legal nature on the application of the AML/CFT Law and CySEC's AML/CFT Directive. Circulars issued for AML/CFT purposes are addressed to all entities under the supervision of CySEC and are publicly available on CySEC's website. CySEC's AML/CFT Directive provides specific guidance on various matters arising from their AML/CFT obligations, including the application of appropriate measures and procedures on a risk-based approach, customer identification and due diligence procedures (along with enhanced due diligence measures on specific types of high-risk customers) and recognition and reporting of suspicious transactions and activities to MOKAS (paragraph 26 and PART VI). CySEC provides seminars regarding the Continuous Professional Development, primarily to persons registered in the public register (i.e. certified persons that have passed CySEC's written examination with the obligation of completing CPDs annually to remain in the public register) for the purpose of compliance with paragraph 17(2)(a) of the [Directive regarding the certification of persons and the public register](#). In addition, CySEC issued a number of circulars to inform and guide the regulated entities on issues, concerning inter alia, guidance on new provisions of the AML/CFT Law, guidance on legislative changes on an EU level, serious tax offenses and guidance on the content of the annual report of the compliance officers for the issues of preventing money laundering and terrorist financing. Finally, CySEC provides guidance to its regulated entities by addressing enquiries of legal nature on the application of the AML/CFT Law and CySEC's AML/CFT Directive. Circular C276 states that obliged entities must apply the Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 for the purposes of complying with the requirements set out in Articles 58(a), 58(d), 58(h), 58A, 61(2), 62(2), 63 and 64 of the AML/CFT Law.

R.15.8(b) is met. Under the amendment to the AML/CFT Law VASPs fall within definition of Obligated Entities and are therefore their senior management and directors and control persons are therefore subject to a range of sanctions, including civil and criminal penalties applicable to ML offenses under applicable law.

Section 59(1)(b)(vi) of the AML/CFT Law provides that CySEC is the supervisory authority for VASPs. Section 59(6) of the AML/CFT Law provides for the measures by the Supervisory Authority in cases where a person falling under its supervision fails to comply with the provisions of this Part of the Law or with the Directives issued by the competent Supervisory Authority in accordance with paragraph (4) of this section or the provisions of EC Regulation no. 847/2015. In addition, section 4(1) of Law 58(I)/2016 on the provisions of the UNSCR and EU sanctions provides that any person in violation of these sanctions is guilty of an offence and in case of conviction is subject to (a) if a natural person, imprisonment not exceeding two years or a pecuniary fine not exceeding €100.000 or to both (b) if a legal person, to a pecuniary fine not exceeding €300.000. Section 4(2) of the same Law provides that criminal prosecution of any person can only be exercised upon the approval of the Attorney General of the Republic. Sections 59(6)(a)(iv) and (v) of the AML/CFT Law provides for applicable sanctions that may be imposed on natural persons. These include the imposition of a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities and the imposition of an administrative fine to a person discharging managerial responsibilities in an obliged entity or to any other person whenever it is established that the failure to comply was due to their fault, intentional omission or negligence. Furthermore, Section 59(6)(a2) of the AML/CFT Law provides that a legal person may be liable for breaches, which are committed for its benefit by any person acting individually or as part of an organ of that legal person and having a leading position within such legal person. Additionally, Section 37(3)(b) of the CySEC Law provides that CySEC may impose an administrative fine to an advisor, manager or officer or any other person in case it is established that the violation is a consequence of his fault, willful omission or negligence.

Criterion R.15.9: R.15.9(a) is met. VASPs will have the obligations of obliged entities with regard to the Preventive Measures under the AML/CFT Law under R.10-R.21 (including R.16) with regard to transactions involving fiat currency, including obligations under Title II of the Risk Factors Guidelines of the ESAs. In addition, the AML/CFT Bill expressly requires VASPs to perform CDD on occasional transactions that exceed the €1000 threshold (Art. 60(g)). Section 60 of the AML/CFT Law was amended to include VASPs as obliged entities. They are obliged to follow all obligations of CDD under the AML/CFT Law, CySEC's AML/CFT Directive and Circulars as all other CySEC's regulated entities. According to section 60(g) of the AML/CFT Law, VASPs should apply CDD, when carrying out an occasional transaction which amounts to an amount equal to or higher than one thousand euro (€1,000) whether the transaction is carried out in a single operation or in several operations which appear to be linked. However, a technical argument could be made that for FIs engaged in VA activities under CySEC (as is the case today) or under CBC (as may arise in the future) an occasional transaction in VA which exceeds EUR 1,000 would not be subject to this obligation because the above statutory provision relates specifically only to VASPs, and A) Cyprus has not defined all VA transfers as non-domestic wire transfers and B) the relevant underlying EU regulation, EU Reg. 2015/847, refers only to "funds" which are limited to fiat currency and have not been extended to encompass VA.

These potential technical gaps may (and should) readily be addressed in AML/CFT Directives of CySEC and CBC, as these FIs are in certain respects functionally equivalent to VASPs but may not be required to register as VASPs since they are already licensed as FIs. Because R.15(a) as written applies only to VASPs and not to other entities engaging in VA activities that are lawfully entitled to do so without registering as VASPs, the assessment team did not find any deficiency under this criterion.

R.15.9(b) (i) and (ii) are not met. This is a significant deficiency in that the so-called Travel Rule or Wire Transfer Rule for VA has not been included in the AML/CFT Bill.⁵⁰ This is partially mitigated by the general obligation of obliged entities to ascertain source of funds, along with recordkeeping obligations and a general obligation to deter and prevent money laundering from which a duty associated with obtaining the requisite information regarding the destination of VA may be inferred. However, at most this obligation as to beneficiary information for VA transfers is implied rather than explicit. The assessment team recommends strongly that this be made explicit and legally binding in the VASP registry framework and/or the CySEC AML/CFT Directive, as well as in AML/CFT Directives of the CBC and other supervisory authorities, until such time as the AML/CFT Law is next amended.

R.15.9(b) (iii) is partly met. With regard to freezing, this criterion is met as the AML/CFT Law clearly extends the definition of property to include VA, thus clearly enabling legal basis for freezing of VA. The Combating of Terrorism and Victims' Protection Law N. 75(I)/2019 applies to VASPs as an obliged entity under the AML/CFT Law. The law N. 75(I)/2019 covers a number of issues, including the definition of terrorism felonies, the responsibilities of legal persons, responsibility of entities obliged under the AML/CFT Law to confiscate property belonging or controlled by persons engaged in terrorism and the responsibility of supervisory authorities for ensuring that obliged entities abide with the relevant provisions of this law. However, other elements of R.15/9(b)(iii) are not met. This is a deficiency in that the so-called Travel Rule or Wire Transfer Rule for VA has not been included in the amendment to the AML/CFT law. On R.16 Moneyval found Cyprus **Largely Compliant** primarily on the basis of EU Reg. 2015/847.⁵¹ VA are outside the scope of this regulation, which refers only to "currency", as VA are not legally recognized as or considered currency under EU law. This EU Regulation has not been amended to cover VASPs or transfers of VA, nor have its threshold amounts been amended to reflect FATF June 2019 Guidance. Moreover, there is no provision establishing that transfers of VA are all considered international wire transfers, as required under the FATF 2019 Guidance, not domestic transfers (even if effected within the EEA or within a single member state/Cyprus).

⁵⁰ According to the FATF Plenary statement following the June 2021 FATF Plenary, the majority of reporting jurisdictions have not yet implemented the Travel Rule for VA. <https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2021.html>

⁵¹ Reg. 2015/847 provides: "This Regulation lays down rules on the information on payers and payees, accompanying transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing, where at least one of the payment service providers involved in the transfer of funds is established in the Union."

R.15.9(b)(iv) – The assessment team found that while in practice this criterion is largely met, there is no technical obligation legally requiring non-VASP financial institutions to meet these obligations. It is recommended that that new directives, or updates to their respective existing AML/CFT directives, be issued by CBC and CySEC (to assure that these obligations apply legally as a requirement, not merely through advisory guidance). In particular it should be explicit that as set forth in Criterion R.15.9(b)(iv), the provisions of Criteria R.15.9(b)(i) and (ii) apply as a matter of law to financial institutions when sending or receiving VA transfers on behalf of a customer, and it should also be clear that these obligations apply to FI that are not required to register as VASPs but conduct VASP activities.

For FI under the CBC, it was observed by the assessment team that this deficiency is more theoretical than an actual deficiency or gap, as none of them have requested permission, to add sending or receiving VA on behalf of a customer to their business activities. It is CBC’s understanding that if CBC were ever to receive such a request and permit it, it could impose conditions. The assessment team recognizes that compliance with these requirements could readily be included among the conditions imposed by CBC. Nevertheless, it is recommended that this be addressed via an update to CBC AML/CFT requirements (for FI including credit institutions, payment institutions, EMI and MVTs) as long as it is a requirement (for full technical compliance) and not merely considered advisory.

The assessment team found the CySEC-supervised CIFs it met with that engage in VASP activities (as permitted under special permission from CySEC under Circular C244) to be well aware of FATF requirements and to have developed their own procedures in place to comply with them. One CySEC-supervised entity engaging in VA activities queried whether it would meet the definition of a VASP.

Failure to meet 15.9 as detailed above represents a significant deficiency in the Cyprus framework. This deficiency should be rectified as a matter of highest priority in the conditions to registration established for VASPs by CySEC and in updates to the CySEC AML/CFT Directive and the CBC AML/CFT Directive. CySEC has indicated its intention to address these deficiencies in legally binding fashion through inclusion of specific legislative text in updated CySEC AML/CFT Directive after enactment of the amendment to the AML/CFT Law.

Criterion R.15.10 is largely met. Moneyval found Cyprus **Largely Compliant** with R.6 and R.7. As VASPs are obliged entities under the amendment to the AML/CFT Law the provisions regarding targeted financial sanctions apply to VASPs. All communication mechanisms, reporting obligations and monitoring referred to in criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d), also apply to VASPs as an obliged entity under the AML/CFT Law. To achieve full compliance with R.15.10 will require CySEC to update its internal written procedures as well as apply express conditions to VASPs.

Moneyval found (c.6.5(d), 7.2(d)) that the required information is circulated to the supervisory authorities, which includes CySEC (as operator of the register for VASPs) and that supervisory authorities circulate this information to obliged entities immediately. It can therefore reasonably be expected that CySEC would similarly send notice of such actions to VASPs by email immediately upon receipt (as VASPs are obliged entities under the amendment to the AML/CFT Law). It is recommended that CySEC update its internal written procedures to ensure this is the case with respect to VASPs. Moneyval also found that large majority of Cyprus obliged entities subscribe to the EU Financial

Sanctions database, and it is recommended that CySEC require subscription to that or comparable database as a condition to or operating requirement of VASP registration in light of the riskiness of VA and the 24/7/365 nature of VA markets, unlike traditional financial markets.

Moneyval observed that international or EU decisions on updated designations for TFS sanctions lists announced after Nicosia business hours on a Friday may not be communicated by supervisors until the next Business Day. Because VA markets, unlike traditional financial markets, are active constantly outside of business hours, and transactions and movements of assets occur 24/7/365 unlike traditional movements of fiat currency, this could be a meaningful gap with regard to VASPs and movement of VA for TF purposes, which could be moved and utilized during these times. Although VASPs as obliged entities should be required to be subscribing directly to databases that also provide these updates independent of the supervisory notification channel, thus mitigating the risk of this gap, a potential gap remains. Practices for supervisory communication of TFS designations, obligations and measures should ensure that there are not gaps over weekend or holiday periods between when MFA is notified and when VASPs are notified through supervisory channel via CySEC or otherwise.

Moneyval found (c.6.5(e), 7.2(e)) that FIs and DNFBPs are required to immediately inform their supervisory authority upon taking any freezing or other measures in compliance with their requirements under the TFS regime (which would include reporting attempted transactions) under the Cyprus Suppression of Terrorism Law (Law No. 110/1/2010), which has been superseded by the Anti-Terror Law and Victim Protection Law of 2019 (Law No. 75(1)(2019)), which transposed EU Directive 2017/541 on Combating Terrorism. This obligation under the new law applies to all obliged entities and will thus apply to VASPs upon registry as VASPs are obliged entities under the AML/CFT Bill. Supervisory authorities are required, in turn, to inform the MFA once they are so informed. It is recommended that the internal written procedures of CySEC should be updated to ensure that CySEC performs these obligations with respect to information provided by VASPs as soon as it commences to operate the VASP registry.

Moneyval enumerated (c.6.6(g)) both EU as well as national level mechanisms for complying with R6.6(g) generally. It is recommended that CySEC should update its written procedures so that its mechanisms for communicating delistings and unfreezings ensure that this information is also communicated to registered VASPs as soon as it commences to operate the VASP registry, including coverage to mitigate potential gaps over evening, weekend or holiday periods.

VASPs (c.7.3) will be subject to the requirements of the Law N. 58 (I) / 2016 and the sanctions thereunder, under the supervision of CySEC, as well as the CySEC AML/CFT Directive.

Moneyval observed EU and national level compliance with criterion (c.7.4(d)) and found that all authorities are required to communicate changes to the entities they supervise. It is recommended that CySEC update its internal written procedures, as operator of registry, to ensure that it communicates this information promptly to all registered VASPs.

Criterion R15.11 is met. Cyprus is able to rapidly provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to VA.

The provisions included in the CySEC Law and AML/CFT Law for exchanging information with CySEC's foreign counterparts, also apply to VASPs as obliged entities under the AML/CFT Law. In addition, the legal basis for exchanging information is already established and in force with bilateral Memorandum of Understanding and Cooperation agreements (MoUs) with CySEC's foreign counterparts.

Glossary of Acronyms

AA	Advisory Authority
Advisory Authority	The Advisory Authority for Combating Money Laundering and Terrorist Financing established under section 56 of the AML/CFT Law
AG	Attorney General
AML/CFT Bill	The Prevention and Suppression of Money Laundering and Terrorist Financing (Amending) Law of 2021
AML/CFT Law	The Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 as subsequently amended
ASL Law	ASP Law
ASP Law	Law Regulating Companies Providing Administrative Services and Related Matters 196(I)/2012
BO	Beneficial Owner
BORIS	Beneficial Ownership Registers Interconnection System
CA	Competent Authority
CBA	Cyprus Bar Association
CBC	Central Bank of Cyprus
CC	Criminal Code
CCD	Crime Combating Department of the Cyprus Police
CCP	Code of Criminal Procedure
CFT	Combating the financing of terrorism
CTO	Counter Terrorism Office of the Cyprus Police CCD
CTR	Currency Transaction Reports
CySEC	Cyprus Securities and Exchange Commission
DCE	Department of Customs and Excise
DEFL	Digital Evidence Forensic Laboratory
DLT	Distributed Ledger Technology
DNFBPS	Designated Non-Financial Business and Professions
DRCOR	The Department of Registrar of Companies and Official Receiver
EC	European Commission
EIOs	European Investigation Orders
EU	European Union

EUSNRA	EU Supra National Risk Assessment
EAWA	European Arrest Warrant Act
FATCA	Foreign Account Tax Compliance Act
FI	Financial Institution
FIU	Financial Intelligence Unit
Fintech	Financial Technology
FT	Financing of Terrorism
FIU	Financial Intelligence Unit
goAML	The FIU's data system
GPO	General Prosecutor's Office
ICCS	Insurance Companies and Control Service
ICPAC	Institute of Certified Public Accountants
ICOs	Initial coin offerings
IFC	International Financial Centre
IMF	International Monetary Fund
IOSCO	International Organization for Securities Commissions
IT	Information Technology
KRIs	Key Risk Indicators
LEA	Law Enforcement Authorities
LoR	Letter of Request
LSI	Law on Societies and Institutions
MECI	Ministry of Energy, Commerce and Industry
MER	Mutual Evaluation Report
MFA	Ministry of Foreign Affairs
MJPO	The Ministry of Justice and Public Order
ML	Money Laundering
MLA	Mutual Legal Assistance
MOF	Ministry of Finance
Mol or MOI	Ministry of Interior
MOKAS	Unit for Combatting Money Laundering / The Cyprus FIU
Moneyval	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe
NBA	National Betting Authority
NRA	National Risk Assessment
OAC	Office of Advisory Council

PF	Proliferation Financing
PPO	Law Office of the Republic's Public Prosecutor Office
PSPs	Payment Service Providers
RBA	Risk-based approach
RBSF	Risk-based Supervisory Framework
REAs	Real estate agents
REs	Reporting entities
RUBO	Register of Ultimate Beneficial Ownership
SAR	Suspicious Activity Report
SDCEC	Sub-Directorate of Combating Economic Crime of the Cyprus Police
SOTL	Suppression of Terrorism Law
SPOC	Single Point of Contact (EU & International Police Cooperation Directorate of the Cyprus Police)
STR	Suspicious Transaction Report
TF	Terrorist Financing
TCSPs	Trust and Company Service Providers
VA	Virtual Asset
VASP	Virtual Asset Service Provider
4th EU AML Directive or 4AMLD	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015
5th EU AML Directive or 5AMLD	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

**Supplemental Annex to
National Risk Assessment with respect to
Virtual Assets and Virtual Asset Service Providers
Republic of Cyprus 2021**

This Supplemental Annex should be read in conjunction with the full 2021 National Risk Assessment (NRA) with respect to Virtual Assets and Virtual Asset Service Providers -- Republic of Cyprus prepared by Bandman Advisors. It is designed to complement the NRA with an overview of certain types of Virtual Assets (VA) and Virtual Asset Service Providers (VASPs) and some key risk attributes and mitigants with respect to ML/TF risks.

Executive Summary

The utilisation, awareness and market capitalisation of VA have grown enormously in recent years. VA have already been adopted for many legitimate purposes, including investment, transactions and payments, as well as to help establish new types of business models as part of “Web 3.0” or the “Internet of Value” in light of their capacity to support secure transfers and holding of natively digital assets, not just information. They hold promise to provide benefits to consumers and society and promote financial inclusion.

Nevertheless, attributes of VA make them vulnerable to abuse by criminals or terrorists for ML/TF, and there have been extensive documented cases and patterns of such abuse. As adoption of or access to VA increases, the significance of these risks and abusive behaviors and the potential responses and mitigants to these threats and vulnerabilities ensures the attention of lawmakers and policymakers and require that a comprehensive regulatory and operational framework be implemented and monitored.

Criminals are often among the earliest adopters of new technologies.⁵² Criminals also were early adopters of automobiles which they used as getaway cars.⁵³ Notwithstanding their early use as getaway cars by criminals, automobiles were not abolished.

VA Types and Risks

This annex identifies multiple taxonomies of VA and the inherent risk of selected VA types and/or subtypes. The following table summarizes the types of VA discussed below and their respective inherent risk:

⁵² See, e.g. Europol, Crime in the age of technology, October 2017, available at https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

⁵³ <https://historydaily.org/getaway-car-history-facts-stories-trivia>

VA Type	Example	Inherent Risk
Anonymous/Privacy VA	Monero, Zcash	Very High
Pseudonymous Payment VA	Bitcoin, Litecoin	High
Platform Tokens	Ethereum, Solana	High
Utility Tokens	Filecoin	Medium
Stablecoins	Tether, USDC	Medium
Security Tokens	Aspen	Low
Trading Platform Token	Binance Coin, HuobiCoin, FTT	Low

VASP Types and Risks

Numerous types of VASPs have emerged and are described by definitions established by FATF, as well as by the Republic of Cyprus in the AML/CFT Law. VASPs are relatively new types of businesses and the industry, services and activities are still evolving. This annex identifies a number of VASP types and their inherent risks. VASPs will be required to register in Cyprus under the AML/CFT Law and the CySEC Registration Directive for Crypto-asset Service Providers (CASPs), both of which entered into force in 2021, however no firms have yet registered, so no data from them is available yet. As described in the NRA a small number of firms regulated by CySEC have been engaging on a limited scale in VASP-type activities, and findings with respect to such activities and risks are described in the main body of the NRA.

Threat Assessment

Threat assessment: these are understood as predicate offenses that generate illegal proceeds that could lead to ML/TF activities. These are addressed in the main body of the NRA in connection with the potential risk of ML/TF associated with VA in the context of predicate offenses as well as other risks previously identified by Moneyval and the 2018 Cyprus NRA.

Vulnerabilities Assessment

Vulnerabilities assessment: these are understood as the potential exposure of a sector (or sub-sector) for ML/TF purposes, as they may be exploited by a threat or may facilitate its activities.

In regard to VA, this may arise from the degree of its relative anonymity; online accessibility and global network reach; ready convertibility; general lack of susceptibility to reversal; and inconsistency of regulatory frameworks.

This annex also considers the vulnerability of selected types of VASP. It should be noted that the vulnerability of Cyprus non-VASPs is addressed in the main body of the NRA, and under current circumstances has been seen to be limited, due primarily to the lack of acceptance or utilization of VAs by FIs or other DNFBPs in Cyprus, as well as to the policies of FIs that prohibit VA transactions or activities by their customers.

Mitigants

Mitigants: this annex discusses available preventive measures by VASPs, which are largely anticipated to be required under CySEC’s amended AML Directive as well as the operational conditions of CASP registration under the CySEC CASP Registration Directive. This annex also reviews mitigating measures for CySEC as VASP supervisor. Mitigating measures for supervisors of other FIs and obliged entities are discussed in the main body of the NRA. Other important mitigating measures – these include the role of MOKAS as the FIU in detection and mitigation of ML/TF relating to VA, the role of the Cyprus Police and the Attorney General of the Republic’s office in prosecution and enforcement, and the role of numerous Cyprus authorities in cooperating with other domestic and international authorities -- are likewise discussed in the main body of the NRA and not repeated here.

1. Types and Risks of Virtual Assets

There are several types of virtual assets with a variety of technological, risk and economic characteristics, as well as use cases. As these technologies are new and still rapidly evolving, there is not a single universally accepted set of definitions or “taxonomy” to describe or categorize VA. That said, there are a number of widely recognized classification methodologies or “taxonomies”.

Perhaps the best known is that described by IOSCO, which divides VA into three basic categories⁵⁴:

- Payment Tokens/Exchange Tokens/Currency Tokens
- Utility Tokens
- Security Tokens

IOSCO categorises tokens into these three types and recognizes that hybrid forms are possible. According to IOSCO:

Payment Tokens, often referred to as [virtual currencies] or cryptocurrencies, typically do not provide rights (as is the case for investment or utility tokens) but are used as a means of exchange (e.g. to enable the buying or selling of a good provided by someone other than the issuer of the token), for speculative purposes or for the storage of value

Utility tokens typically enable access to a specific product or service often provided using a DLT platform. Can only be used in the issuer’s network .

Security tokens typically provide rights (e.g. in the form of ownership rights and/or entitlements similar to dividends). For example, in the context of capital raising, asset tokens may be issued in the context of an Initial Coin Offering (ICO)/Token Generating Event (TGE) that allows

⁵⁴ IOSCO, Investor Education on Crypto-Assets, Final Report, December 2020, available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD668.pdf> at p. 10.

businesses to raise capital for their projects by issuing digital tokens in exchange for fiat money or other crypto-assets..

IOSCO has also made clear that “despite this categorisation, to determine the nature of a digital asset, yet a case-by-case assessment is needed; one must examine the economic reality. Each digital asset must be examined individually according to the specific facts and circumstances and taking into account the domestic legal and regulatory frameworks and approaches in each jurisdiction.”⁵⁵

Another widely recognized taxonomy is that established by Global Digital Finance (GDF).⁵⁶ GDF divides VA into:

- Payment tokens
- Consumer tokens
- Security tokens

According to GDF:

Our taxonomy contains the following three top-level label categories, which are not necessarily mutually exclusive:

- 1. Payment Tokens: Tokens whose intrinsic features are designed to serve as a general purpose store of value, medium of exchange, and/or unit of account.*
- 2. Financial Asset Tokens: Tokens whose intrinsic features are designed to serve as or represent financial assets such as financial instruments and “securities”.*
- 3. Consumer Tokens: Tokens that are inherently consumptive in nature, because their intrinsic features are designed to serve as, or provide access to, a particular set of goods, services or content.*

Stablecoins and hybrid tokens may be assigned to one or more of these categories on a case-by-case basis.

The Blockchain Research Institute has assigned VA into seven categories⁵⁷, these include:

1. Cryptocurrencies
2. Platforms
3. Utility tokens

⁵⁵ Ibid. at 10.

⁵⁶ https://www.gdf.io/wp-content/uploads/2019/08/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf

⁵⁷ <https://www.blockchainresearchinstitute.org/research/>

4. Security tokens
5. Natural asset tokens
6. Crypto collectibles
7. Crypto-fiat currencies and stablecoins

Terminology and use cases are constantly evolving in light of the rapid development of technology and new applications for the technology. For example, the recent growth of decentralized finance, also known as “DeFi”, has seen the growth of so-called “governance tokens”, which some have likened to utility tokens or platform tokens. Such governance tokens are still being assessed by regulators, for example recent discussions with North American securities regulators have suggested that each of these is assessed under a facts and circumstances standard to determine whether and to what extent they should be classified as an offer or sale of securities or as investment contracts. European regulators have not yet broadly expressed views regarding the nature or status of these governance tokens. However, many authorities including the BIS Innovation Hub, ESMA and the U.S. SEC are calling for increasingly close examination of DeFi, including the potential role of governance tokens.

Stablecoins

Stablecoins are also referred to as “so-called Stablecoins” in FATF publications,⁵⁸ though not by the broader public. Stablecoins as introduced to date are far from homogeneous and can have a number of so-called “stability” mechanisms, which may be asset backed, algorithmic or otherwise. The Basel Committee on Banking Supervision has described a number of these potential mechanisms – and the prudential risk weighting implications of same – in a June 2021 consultation entitled Consultative Document Prudential treatment of cryptoasset exposures.⁵⁹ Potential implications and trends relating to stablecoins as private money replacing public money to some degree have also been discussed by the Bank of England in a June 2021 consultation paper on new forms of digital money.⁶⁰ As part of its Digital Finance Package, in September 2020 the European Commission proposed a comprehensive legislative framework for VA and VASPs from a supervisory and regulatory perspective (though not an ML/TF perspective), generally referred to as the proposed Markets in Crypto-assets Regulation or MiCAR.⁶¹ Under this framework stablecoins may be classified, depending on the underlying reference point, as “e-money tokens” or “asset-reference tokens” with some potentially qualifying as “significant”.

Growth in use and market capitalization of stablecoins has been substantial in the 2020-2021 time frame. For example, as of September 2020 the following table⁶² may be considered a baseline for appreciation of rapid subsequent growth.

⁵⁸ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf>

⁵⁹ <https://www.bis.org/bcbs/publ/d519.pdf>

⁶⁰ <https://www.bankofengland.co.uk/paper/2021/new-forms-of-digital-money>

⁶¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

⁶² GDF – Age of Public Digital Currencies, October 2020, as of 20 September 2020, Details as set forth in report











Issuer	Ticker	Mkt. Cap (\$)	% of Stablecoin Market	Backing	Details
Tether	USDT	9,142,785,841	86%	Fiat	Owned by Bitfinex, seen as a way to have exposure to hedge into a more stable asset without leaving the digital universe.
Centre	USDC	740,135,031	7%	Fiat	1:1 USD, ERC20 standard token on Ethereum Network, created by Circle and Coinbase.
Paxos	PAX	251,902,524	2%	Fiat	1:1 USD, based upon the Paxos Standard tokens.
Binance	BUSD	179,423,669	2%	Fiat	1:1 USD, conversion to other coins on Binance (USDT, USDC, TUSD, PAX), ERC20 and BEP-2.
TRUE	TUSD	140,107,753	1%	Fiat	1:1 USD, ERC20 standard token on Ethereum Network.
Huobi	HUSD	121,677,908	1%	Fiat	1:1 USD, run by Paxos, similar structure.
Maker DAO	Dai	10,180,509	0%	Crypto	Collateralized by pooled Ether and multi-collateral Dai that are price stabilized against the USD, using crypto as collateral. Requires over-collateralization and created a debt position of the collateral for creation of the Dai.
Gemini	GUSD	8,653,192	0%	Fiat	Issued by NY Trust Company, strictly pegged to USD 1:1, ERC20 standard token on Ethereum Network.

As of end of January 2021, according to the Block Report on stablecoins published in March 2021, the aggregate supply of stablecoins reached nearly \$40 billion. January 2021 stablecoin transaction volume exceeded more than \$300 billion—surpassing the previous month’s 2020’s all-time high by more than 60%. In 2020, more than \$1 trillion worth of volume was transacted with stablecoins through public blockchain networks in 110 million transactions. By comparison, according to this report, PayPal had \$936 billion of payments volume in 2020 in 15.4 billion transactions. While the total volume is nearly identical, the difference in the use case is apparent from the average payment size, which for the period described was about \$60 for PayPal and more than \$9,000 for stablecoins.

Table: The Block – Stablecoins Report – March 2021 – leading stablecoins by market cap.

NAME	ISSUER	CURRENCY	BACKING	TOKEN	ETH	OTHER	SUPPLY (\$M)
USDT	iFinex	USD	Fiat	✗	☑	☑	\$26,757
USDC	CENTRE	USD	Fiat	✗	☑	☑	\$6,066
Dai	Maker	USD	Crypto	MKR	☑	✗	\$1,651
Binance USD	Paxos	USD	Fiat	✗	☑	☑	\$1,427
PAX	Paxos	USD	Fiat	✗	☑	✗	\$667.7
HUSD	Paxos	USD	Fiat	✗	☑	✗	\$456.5
TrueUSD	TrustToken	USD	Fiat	✗	☑	☑	\$389.1
UST	Terra	USD	Algorithmic	LUNA	✗	☑	\$261.0
sUSD	Synthetix	USD	Crypto	SNX	☑	✗	\$144.6
ESD	Empty Set Dollar	USD	Algorithmic	✗	☑	✗	\$109.1
FRAX	Frax	USD	Algorithmic	FXS	☑	✗	\$82.7
Gemini dollar	Gemini	USD	Fiat	✗	☑	✗	\$78.8











Further explosive growth has continued. By July 2021, market capitalization of the leading stablecoins had grown as follows:⁶³

Name	Price	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ
 Tether USDT	\$1.00	-0.00%	-0.05%	\$61,850,888,549	\$54,022,213,500 53,986,790,642 USDT
 USD Coin USDC	\$1.00	-0.02%	-0.00%	\$26,995,677,437	\$1,980,387,019 1,980,025,768 USDC
 Binance USD BUSD	\$1.00	-0.02%	-0.01%	\$11,715,476,637	\$4,837,487,889 4,836,429,959 BUSD
 Dai DAI	\$1.00	-0.04%	-0.02%	\$5,536,815,108	\$309,985,501 309,622,093 DAI
 TerraUSD UST	\$1.00	-0.10%	-0.16%	\$2,029,213,127	\$21,764,497 21,716,873 UST
 TrueUSD TUSD	\$1.00	-0.01%	-0.03%	\$1,276,129,805	\$64,975,981 64,964,206 TUSD
 Paxos Standard PAX	\$1.00	-0.03%	-0.04%	\$907,410,305	\$93,554,540 93,521,165 PAX
 HUSD HUSD	\$1.00	-0.04%	-0.03%	\$557,717,576	\$346,305,552 346,156,278 HUSD
 Neutrino USD USDN	\$0.9996	-0.16%	-0.09%	\$407,678,012	\$14,313,369 14,323,368 USDN
 Gemini Dollar GUSD	\$0.9993	-0.10%	-0.79%	\$322,145,559	\$9,060,519 9,085,885 GUSD

While stablecoins generally do not have privacy enhanced attributes, the growth of stablecoins may be an indicator of broader adoption or increased activity of VA more generally. In addition, the above table reflects certain stablecoins have a much higher ratio of their 24h volume in proportion to their overall market capitalization, such as USDT, BUSD and HUSD, which suggests greater utilisation for intraday activities such as trading. Stablecoins have also seen utilization in so-called “DeFi” or decentralized finance which may also account for the increased usage and difference in daily ratio of activity. Supervisors should consider these different use cases in monitoring risks and activities, as well as assessing the inherent risk of stablecoins.

The following table sets forth the top ten VA by market cap as of late September 2021⁶⁴:

⁶³ Coinmarketcap.com website visited 24 July, 2021
⁶⁴ Source: Coinmarketcap.com visited 26 September 2021.

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)
☆ 1	 Bitcoin BTC Buy	\$43,241.27	-1.44%	-8.64%	\$815,511,751,079	\$32,410,221,760 748,215 BTC
☆ 2	 Ethereum ETH Buy	\$2,991.84	-2.64%	-10.65%	\$352,837,829,091	\$21,529,530,997 7,180,732 ETH
☆ 3	 Cardano ADA	\$2.26	-5.21%	-3.63%	\$72,672,047,134	\$5,511,256,900 2,428,751,471 ADA
☆ 4	 Tether USDT Buy	\$1.00	-0.05%	-0.03%	\$68,597,006,096	\$78,871,733,336 78,809,633,195 USDT
☆ 5	 Binance Coin BNB Buy	\$344.75	-2.13%	-15.53%	\$58,101,028,597	\$1,862,384,295 5,389,505 BNB
☆ 6	 XRP XRP	\$0.9451	+0.24%	-10.97%	\$44,188,550,571	\$3,457,081,735 3,654,944,547 XRP
☆ 7	 Solana SOL	\$135.68	-2.74%	-15.02%	\$40,432,042,697	\$2,427,202,269 17,846,254 SOL
☆ 8	 USD Coin USDC	\$1.00	-0.03%	-0.04%	\$31,004,738,537	\$3,785,948,278 3,784,391,163 USDC
☆ 9	 Polkadot DOT	\$29.25	-4.62%	-13.31%	\$28,998,463,616	\$2,582,416,620 87,947,461 DOT
☆ 10	 Dogecoin DOGE	\$0.2054	-1.67%	-13.34%	\$27,035,050,658	\$1,502,719,896 7,306,362,025 DOGE

Payment Token VAs

Payment Tokens VAs include several subcategories. The most widely known, encompassing examples like Bitcoin and Litecoin, may be understood as VA with attributes of bearer instruments that are pseudonymous – thus introducing an increased risk of ML/TF – but where the transactions are visible and transparent through the blockchain and can be traced to a specific sender and receiver. The inherent risk of pseudonymous payment token VAs is exacerbated because they do not require the physical presence of the counterparties for a transfer or transaction to occur, which accordingly lowers the barrier for this type of transaction to be carried out, potentially opening the door to increased frequency of high-risk transactions and posing accordingly significant ML/TF risk.

A subcategory of Payment Token VA referred to as “*privacy coins*”⁶⁵, are inherently anonymous, in ways that may obscure the sender, the receiver and/or the amount exchanged. Monero and Zcash are among the best known of these. These have a very high inherent risk. In practice even some of the so-called privacy enhanced or “pseudo anonymous” or “anonymous” VA may come in more than one variant – for example the New York regulator the Department of Financial Services (DFS), one of the leading regulators of VA businesses globally,⁶⁶ as early as 2018 authorized its regulated platforms to offer trading and other services with respect to Zcash, which is widely regarded as a privacy-enhanced VA, but which is also available in an alternate mode with lesser privacy and greater traceability.⁶⁷

The inherent risk of anonymity in VA may be enhanced or facilitated by anonymous crypto wallets and by emerging products, services or tools entering the crypto-assets’ ecosystem, which in effect provide new ML/TF opportunities, including new opportunities for placement, layering and integration of illicit proceeds. Anonymization tools referred to as “Mixers” or “Tumblers”⁶⁸ may be used to allow users to pool, mix and redistribute their crypto-assets, obfuscating the flow of the transaction and/or enabling the mixing of illicit funds with clean VA. However, as discussed further below (with regard to mitigating preventive measures that may be utilised by VASPs such as cryptoasset AML database, forensic and transaction monitoring tools), it is highly possible due to the transparency and visible traceability of the blockchain and the increasing reach of wallet address database identification capabilities for VA to be traced back to addresses that have been identified by such tools as mixers or tumblers. Thus, the use of mixers and tumblers, where associated with a recognized wallet address or addresses, can be widely detected and flagged as an indicator of risk in the transaction history of any particular transfer of VA.

The emergence of decentralised exchanges, decentralized finance (DeFi) and peer to peer transactions, may add further layers of risk, as certain DeFi platforms do not require AML or KYC, and P2P transactions may occur directly between counterparties outside of a participating VASP.

Public perception of the untraceability or anonymity of VA is not necessarily in keeping with the reality of technology and investigative capabilities that mitigate these perceived factors. There is a broad range of public understanding as to the ML/TF riskiness of VA such as bitcoin as well as its traceability. While one of the most pervasive and disruptive forms of criminal activity employing VA is so-called “ransomware”, which exploits cybersecurity weaknesses and then seeks to leverage the availability and convertibility of VA to reap the rewards of such criminal activities, it was disclosed in summer 2021 that U.S. authorities had traced and recovered a high percentage of the ransomware associated with

⁶⁵ See Financial Times, 22 June 2021: “*Monero emerges as crypto of choice for cybercriminals*”. Available at: <https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6>

⁶⁶ https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/regulated_entities

⁶⁷ https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1805141

⁶⁸ See Financial Times, 28 May 2021: “*The rise of crypto laundries: how criminals cash out of bitcoin*”. Available at: <https://www.ft.com/content/4169ea4b-d6d7-4a2e-bc91-480550c2f539>

the widely publicized Colonial Pipeline hack.⁶⁹ Similarly, it has been asserted in the Wall Street Journal that “untraceable bitcoin is a myth”⁷⁰

Stablecoins also provide a Payment Token VA type of function. ML/TF risks are mitigated because there is typically a centralized issuer, such as with USDT and USDC, although Dai has a more decentralized structure. The presence of a centralized issuer may mitigate ML/TF risks, and in fact during summer 2021 in response to the Poly network hack, the operators of USDT were able to freeze USDT Tethers attributed to the attackers. However, the availability of stablecoins may also promote the convertibility of criminal proceeds from a volatile VA to a less volatile stablecoin, which may delay or alleviate the need to convert criminal proceeds into fiat currency.

Utility tokens as described above are intended to provide digital access to an operational application, product or service. Leading examples include Filecoin (FIL) and Basic Attention Token (BAT). While typically utility tokens are designed for use within their respective ecosystems, and transactions are transparent (pseudonymously) on the blockchain, these may also be bought and sold on exchanges and thus can be used in connection with movement of ML/TF proceeds. Accordingly these have medium inherent risk.

Platform Tokens have attributes of Payment Tokens and attributes of Utility tokens. Examples include Ethereum, Solana and Polkadot. They can be used for building applications and deploying smart contracts, however they also share the attributes of Payment Tokens wherein pseudonymous transactions traceable on the blockchain to a specific sender and achiever are readily available, and these may readily be exchanged for fiat or other VA. Accordingly these have high risk.

Security tokens or asset tokens generally have a specific issuer and are issued and traded subject to applicable securities laws, and transfers may be recorded not only on the blockchain but in a CSD in certain conditions, or by a transfer agent in others. While there have been relatively few successful examples of security token issuances to date, the overall inherent risk appears to be low. More data points could in the future indicate whether that rating may warrant adjustment.

One hybrid category that has grown in size are Trading Platform Tokens – examples include BNB (Binance Coin), Huobi Coin and FTT (FTX coin). Their function has attributes of stablecoins, and they also confer discounts or other benefits for users on their respective platforms. As there is a tendency for them to remain within the ecosystem of their platform, and not move across platforms, the relevant platform has high potential visibility into the users and transaction behaviors, including ability to detect suspicious activity on a disclosed basis. A user could convert from one VA to a Trading Platform Token to another VA within the same exchange. The overall inherent risk appears to be low.

⁶⁹ <https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981>

⁷⁰ <https://www.wsj.com/articles/untraceable-bitcoin-is-a-myth-11623860828>

The following table summarizes the Inherent Risk of these types of VA:

VA Type	Example	Inherent Risk
Anonymous/Privacy VA	Monero, Zcash	Very High
Pseudonymous Payment VA	Bitcoin, Litecoin	High
Platform Tokens	Ethereum, Solana	High
Utility Tokens	Filecoin	Medium
Stablecoins	Tether, USDC	Medium
Security Tokens	Aspen	Low
Trading Platform Token	Binance Coin, HuobiCoin, FTT	Low

2. Virtual Asset Service Provider (VASP) – Types of VASPs; Regulatory Status of VASPs in Cyprus

The definition of VASP⁷¹ was introduced by FATF in 2018, and initially included the following types of activities:

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i. exchange between virtual assets and fiat currencies;
- ii. exchange between one or more forms of virtual assets;
- iii. transfer¹ 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.

[1.] 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.

In its consultative guidance released in March 2021, FATF has provided considerable further elaboration of VASP activities yet has not proposed to alter the earlier definition.⁷²

Under the AML Law, Cyprus requires VASPs (which are referred to under applicable statute and regulations as CASPs, or crypto asset service providers) to register with CySEC as the competent authority, and CySEC has issued a registration directive and is completing its application for VASPs as well as updating its AML Directive for its registered entities with respect to VA, including VASPs. As there is no passporting for VASPs either under Cyprus or EU law, achievement of VASP registration (or licensing) in any EU jurisdiction does not result in passporting to other member states.

⁷¹ <https://www.fatf-gafi.org/glossary/u-z/>

⁷² <https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf> at 21-30.

Cyprus's definition of a CASP in the AML/CFT Law is aligned with that set forth by FATF above, with a degree of greater elaboration of the third, fourth and fifth prongs as well as ensuring that initial offerings are covered within the scope of activities:

“Crypto Asset Service Provider” or “CASP” means a person who provides or exercises one or more of the following services or activities to another person or on behalf of another person, which do not fall under the services or activities of the obliged entities mentioned in paragraphs (a) to (h) of article 2A:

- (a) Exchange between crypto assets and fiat currencies;
- (b) Exchange between crypto assets;
- (c) Management, transfer, holding and/or safekeeping, including custody, of crypto assets or cryptographic keys or means which allow the exercise of control over crypto assets;
- (d) Offering and/or sale of crypto assets, including the initial offering; and
- (e) Participation and/or provision of financial services regarding the distribution, offer and/or sale of crypto assets, including the initial offering;

Thus it can reasonably be expected that an initial cohort of VASPs offering VASP services in Cyprus should apply for registration and be registered (or rejected) within the 2021-2022 timeframe.

The overall inherent risk for the VASP sector is high, although individual VASPs may have lesser or greater degrees of risk based on

- Specific products
- Specific activities and services
- Size and scope of operation
- Customer base
- Methods of transmission or delivery
- Risk control framework

Products – the range of VA products that a VASP’s business encompasses will have significant impact – the risks above may have less applicability depending whether for example the VASP’s products include privacy enhanced VA.

Activities and services – there is a wide range of VASP activities as set forth in the FATF and Cyprus definitions above. Typically VASPs operate on a non-face to face basis thus enabling non face to face business relationships. Where VASPs interact with fiat currencies, there are typically greater controls in light of the intersection with the more regulated financial system, and it is believed that the point of intersection or convertibility may tend to expose attempted bad actors. VASPs have also been shown to be susceptible to hacking or cybersecurity weaknesses around the world, and have also been used by operators (such as the operator of the trading platform Quadriga) to exploit customers of the VASPs by stealing and misappropriating their funds. VASPs may also engage in substantial off-chain transactions – that is, they receive and hold customer VA in commingled accounts as a result of which individual transactions and movements are not visible and transparent on the blockchain.

Size and scope of operation – VASPs can range from a small OTC brokerage serving institutional buyers and sellers or a single or small number of VA kiosk “ATMs” to a global exchange or trading platform servicing millions of customers around the world, sending and receiving VA to and from numerous VA addresses, only some of which may be other VASPs. Some exchanges – most recently Binance and FTX – have acquired explosive numbers of customers in relatively short periods.

Customer base – VASP customer bases vary. These tend to be non face to face and involve large numbers of retail customers in multiple jurisdictions, many of which may not have imposed substantial regulation or supervision of VA and VASPs. However other VASPs may have smaller number of more targeted institutional customers. There have been well documented use of VASP exchanges by criminals associated with Silk Road, Liberty Reserve and ransomware, for example.

Method of Transmission and Delivery - VASPs may be exposed to ML/TF risk during the placement, layering or integration steps of ML/TF activities and schemes. Some VASPs may accept payment for VA in fiat currency, and may be exposed to risks associated with transmission of small or substantial amounts of fiat, depending on their policies. Operators of VA kiosks have exposure associated with receiving fiat cash in a physical transmission without staff present. Other VASPs may not accept fiat and may be involved in receiving or sending VA which is being transmitted or converted into other forms of VA. This may allow VA to move across blockchains, potentially obfuscating their path.

Risk control framework – VASPs are a relatively new form of entity and there are limited personnel with training, skills and experience in safeguarding against ML/TF risks. VASPs are subject to a wide range of regulatory frameworks and supervision, and in many jurisdictions the FATF 2019 Guidance and Travel Rule have not yet been implemented.

3. Vulnerabilities of VA and VASPs

Vulnerabilities of VA: VA pose a number of risks that give rise to vulnerabilities. Key vulnerabilities of VA include:

Relative anonymity and pseudo-anonymous nature – users are not able to be easily or immediately identified on the distributed ledger that underpins operation of a VA due to the use of pseudonyms rather than real-world identities, such that users can employ a degree of obfuscation to hide their identity. Identification and monitoring can be further obfuscated through the use of mixers and tumblers, or using privacy-enhanced VA (privacy coins).

Online accessibility and global reach – VA can enable criminals to move funds quickly, at scale, and within a jurisdiction or across international borders at scale. Because these activities occur online, unlike cash, there is no need for a face-to-face relationship or transaction.

Ready convertibility – VA can readily be converted into fiat currencies on numerous exchanges, and from there introduced back into the non-VA economy. These markets operate 24/7/365. While historically the volatility of VA such as bitcoin may have been a concern or deterrent, the emergence

and rise of stablecoins has introduced a far less volatile form of VA that is far more likely to maintain its steady value in relation to its underlying fiat currency or asset, while retaining the other attributes of more volatile forms of VA.

Difficulty of reversal – once VA has been transacted or transferred, the decentralized and distributed nature of most blockchains make it largely infeasible to halt, freeze or reverse a transaction. While this is not always the case – for example the operators of the Tether stablecoin were able to freeze USDTs that had rapidly been attributed to the hackers of the Poly network in summer 2021 – in general where ML/TF activities do proceed it can be difficult to reverse.

Inconsistent regulatory requirements -- Inconsistent regulatory requirements and regulatory arbitrage may also pose vulnerabilities – some jurisdictions have not yet implemented FATF requirements, for example those associated with the Travel Rule or imposing requirements on VASPs or other obliged entities to perform adequate due diligence checks on customers and their transactions.

Availability of multiple ways to hold and transfer VA – There are a multitude of types of way that persons with VA can sell, transfer, exchange, move or hold VA, some of which involve VASPs and others of which do not. These may include P2P transactions, which may occur on non-custodial or decentralized finance (DeFi) platforms that may not perform any KYC and which may assert that they are not subject to ML/TF obligations applicable to VASPs. However, FATF’s analysis published in July 2021 concluded that “*Despite the variation between the companies, the data from all companies is consistent in one sense. The data does not show a clear and consistent shift towards P2P transactions or away from transactions with VASPs. Particularly with the number of transactions, the proportion transacted with and without a VASP has remained largely stable between 2016-2020.*”⁷³ At least one leading DeFi protocol has introduced an institutional version with private pools of liquidity where KYC is required and implemented.⁷⁴

Vulnerabilities of VASPs

Key vulnerabilities of VASPs

Non Face to Face Relationships – a high proportion of VA transactions conducted on or through VASPs involve non face to face business relationships accessed through the internet, enhancing anonymity. The global footprint of VA and internet access increase risk of potential ML/TF activity.

⁷³ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPs.pdf> at 25, paragraph 86.

⁷⁴ <https://uk.finance.yahoo.com/news/aave-debut-institutional-defi-lending-154914554.html>

Scam or crime victims – some customers of VASPs may be victims of scams or ransomware crimes involving VA, and may seek access to VASPs in order to obtain VA to transmit to address such a scenario.

Commingled wallets - VASP transactions may not be registered on blockchain due to exchanges operating a commingled wallet and account structure, thus allowing criminals potentially to evade detection and convert one form of VA into another. This vulnerability is to a degree however mitigated because once the VA leaves the VASP exchange the transaction is transparent outside, and database firms have proven successful at identifying which wallets they are confident they can attribute to a particular VASP exchange's ecosystem. Other forms of off chain transaction may be more difficult to detect, but do not typically involve VASPs.

Absence of CDD: A DeFi or non-custodial VA platform may be particularly vulnerable to ML/TF and anonymity risks because many do not perform CDD. However, as noted in the FATF July 2021 analysis, the proportion transacted with and without VASPs has remained stable over the past five years.

4. Mitigants

Preventive measures by VASPs are critical to responding to the ML/TF risks of VA as well as the VASP sector. The role of VASP supervisors is likewise critical in ensuring that VASPs are applying the controls and measures within their capabilities in proportion to the risks introduced by their activities.

Preventive measures available to VASPs include:

- Customer due diligence proportionate to the risks at all stages of the relationship, including at time of customer onboarding, ongoing due diligence throughout the customer relationship lifecycle and of course transaction monitoring as well as wallet and VA source monitoring utilising the transparency of the blockchain and the availability of professional crypto AML database intelligence and transaction monitoring tools. In monitoring customers, market behaviors and risks, VASPs can avail themselves of the indicators set forth in the FATF Virtual Assets Red Flags report.⁷⁵
- Compliance with the Travel Rule. It should be noted however that in July 2021 FATF issued a Second Twelve Month Review report looking back on the previous year's progress with respect to the Travel Rule and other measures introduced for VA and VASPs under the 2018-2019 revisions to the FATF definitions and guidance in relation to virtual assets.⁷⁶ This report found that the majority of reporting jurisdictions had not yet implemented key provisions of the 2019 amendments, most notably the Travel Rule, nor had they achieved the desired speed of progress in implementing VASP registration or licensing schemes.

⁷⁵ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>

⁷⁶ <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>

- Awareness of regulatory differences or regulatory arbitrage – VASPs should be aware that VASPs in other jurisdictions may be subject to differing or lesser requirements, which may be due to differences in timing of implementation of FATF requirements as noted in the July 2021 FATF Second Twelve Month Review Report cited above. VASPs’ policies and risk assessment of counterparties should take these differences into account.
- Utilization of commercially available technology tools for transaction monitoring, risk scoring and monitoring of wallet addresses and behaviors, and automated application of the FATF red flags per the FATF 2020 Red Flags report and other indicia of suspicious activity. Seven providers of such tools were identified.⁷⁷
- Filing of STRs and SARs is a critical element of VASP ML/TF compliance programs. To date in Cyprus there has been limited MOKAS (FIU) experience with such filings as of the time of the NRA report.
- Cooperation with competent authorities including supervisors, FIU and where applicable Cyprus Police and prosecutors.

Mitigants for Supervisors and Supervision

Mitigating factors to VA and VASP ML/TF risks for supervisors are discussed in the NRA and have been identified pursuant to the 2019 FATF revised Guidance with respect to VA and VASPs. Additional examples and guidance for supervisors with respect to VASPs and VA ML/TF risks have been more recently set forth by FATF in its March 2021 report on Risk-Based Approach for Supervisors.⁷⁸ These include taking steps to develop an understanding of the ML/TF risks posed by VA and VASPs; cooperation with other authorities domestically and internationally; ensuring measures to control market entry by VASPs and restrict market entry by owners or managers who are unfit; oversight and supervision of VASPs; detection through analysis of STRs and SARs; and of course robust prosecution and enforcement.

Supervisors, particularly CySEC, will require sufficient human and technological resources, including information technology systems or tools such as commercially available VA forensic and database tools as well as transaction monitoring tools. The complexity of the underlying technology of VA and VASPs and its rapid ongoing evolution will require such tools and evolving skills for the staff monitoring VA and VASPs.

⁷⁷ To develop market metrics on P2P transactions, the FATF selected seven blockchain analytic companies (Chainalysis, CipherTrace, Coinfirm, Elliptic, Merkle Science, Scorechain, and TRM Labs) based on the outreach and feedback from experts and delegations. See Second Twelve Month Review Report at 24.

⁷⁸ <https://www.fatf-gafi.org/media/fatf/documents/Risk-Based-Approach-Supervisors.pdf> - see especially pp 92-96.